



TRIPWIRE ENTERPRISE 8.7.4

USER GUIDE

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

© 1998-2019 Tripwire, Inc. All rights reserved.

Tripwire is a registered trademark of Tripwire, Inc. Other brand or product names may be trademarks or registered trademarks of their respective companies or organizations.

Contents of this document are subject to change without notice. Both this document and the software described in it are licensed subject to Tripwire's End User License Agreement located at <https://www.tripwire.com/terms>, unless a valid license agreement has been signed by your organization and an authorized representative of Tripwire. This document contains Tripwire confidential information and may be used or copied only in accordance with the terms of such license.

This product may be protected by one or more patents. For further information, please visit: <https://www.tripwire.com/company/patents>.

Tripwire software may contain or be delivered with third-party software components. The license agreements and notices for the third-party components are available at: <https://www.tripwire.com/terms>.

Tripwire, Inc.
308 SW Second Ave, Suite 400
Portland, OR 97204

US Toll-free: 1.800.TRIPWIRE
main: 1.503.276.7500
fax: 1.503.223.0182
<https://www.tripwire.com>
tripwire@tripwire.com

Contents

About This Guide	19
Overview	19
Document List	20
Document Conventions	21
Contact Information	22
Chapter 1. Introduction to Tripwire Enterprise	23
The Tripwire Enterprise Console Interface	24
Tripwire Enterprise Managers and Objects	27
About Groups	29
Chapter 2. Getting Started	31
Using Tripwire Enterprise Fast Track	32
After Fast Track	34
Chapter 3. Terms, Concepts, and Functions	35
How Tripwire Enterprise Detects Change	36
Overview	36
What Does Tripwire Enterprise Monitor?	37
About Baselines	43
About Version Checks	44
Responding to Changes	46
What is Promotion?	47
What is Restoration?	50
About Nodes	51
What are Node Types?	51
How are Nodes Created?	54
About Node Groups and Smart Node Groups	57

Monitoring Virtual Systems with Tripwire Enterprise	59
About Audit Events and Real-Time Monitoring	63
What is Audit Event Collection?	63
How Does an Event Generator Collect Audit Events?	66
How Does Real-Time Monitoring Work?	70
About Selection Methods	73
What is the By-Match Selection Method?	73
What is the By-Reference Selection Method?	76
About Rules	79
What are Rule Types?	79
How Does a File System Rule Work?	83
What is the Adjust Rule Feature?	84
How Does a Windows Registry Rule Work?	85
How Does a Windows RSoP Rule Work?	88
How Does a Database Metadata Rule Work?	89
How Does a Database Query Rule Work?	92
How Does a Directory Rule Work?	93
How Does a Log Transfer Rule Work?	98
How Does a Command Output Capture Rule (COCR) Work?	99
COCR Examples	100
How Does a Command Output Validation Rule (COVR) Work?	103
COVR Examples	104
How Do Regular Expressions Work?	107
About Severity Levels and Severity Ranges	112
What are Severity Levels?	112
What are Severity Ranges?	114
Example: Using Severity Levels and Severity Ranges	115
About Actions	116
What are Actions and Action Types?	116
How Do I Run an Action?	119
How Does an Action Group Work?	120

How Does an E-mail Action Work?	120
How Does an Execution Action Work?	121
How Does the Outside Change Window Action Work?	122
How Does a Restore Action Work?	123
How Does a Run Rule Action Work?	123
How Does a Set Custom Value Action Work?	124
How Does an SNMP Action Work?	124
How Does a Conditional Action Work?	125
About Tasks	127
What are Task Types?	127
How Does a Baseline Rule Task Work?	128
How Does a Check Rule Task Work?	129
How Does the Compact Element Versions Task Work?	130
About Policies and Compliance	131
What are Policy Manager Objects?	131
What are Scopes and Effective Scopes?	133
How Does a Policy Test Work?	135
How Do I Monitor Compliance Statistics?	137
What are Policy Scores?	138
What are Scoring Thresholds?	142
How Do I Review the Results of Policy Tests?	144
What is Policy Test Promotion?	146
Example: Using TE Policies to Enforce PCI Standards	148
About Remediation	151
How Does Automated Remediation Work?	151
Implementing Automated Remediation in Tripwire Enterprise	155
What are Post-Remediation Service Commands?	164
What is Manual Remediation?	165
About Log Messages	166
What are Log Messages?	166
What are TE Log Message Categories?	167

How Does the Archive Log Messages Task Work?	170
About Reports	172
What are Reports and Report Types?	172
Example: Running a Composite Changes Report	179
How Do I Manage Report Output?	181
What are Dashboards?	182
How Do Embedded Report Links Work?	182
Example: Embedding Links in a Change Rate Report	183
What are System Reports and User Reports?	184
How Does a Report Task Work?	186
How Does a Run Report Action Work?	188
About Home Pages	189
What are Home Pages and Widgets?	189
How Do Alert Widgets and Alert Generators Work?	192
Who Can View and Configure a Home Page?	192
About the Settings Manager	194
What are Settings?	194
What are E-mail Servers?	196
What are Global and Local Variables?	196
What are Custom Properties?	197
Example: Using Custom Properties	199
About User Access	202
About Tripwire Enterprise Licenses	202
How Do TE Licenses Work with VI Nodes?	203
What are User Permissions and User Roles?	204
What are User Accounts and User Groups?	206
What is an Effective User Role?	207
What are Login Methods?	207
What are Access Controls?	208
Example: Using Access Controls	211
Linking Tripwire Enterprise Objects	213

What are Links and Linked Objects?	213
How Do Links Work?	214
Example: Creating, Linking, and Unlinking a Node	215
Importing and Exporting Tripwire Enterprise Objects	217
How Do I Import and Export Tripwire Enterprise Objects?	217
Order of Import for Multiple XML Files	219
What are Pre-Configured Rules and Policies?	219
How Do I Manage User Access for Pre-Configured Rules and Policies?	220
How Did Pre-Configured XML Files Change in Tripwire Enterprise 7.1?	221
How Does Tripwire Enterprise Import an XML File?	222
What are Tracking Identifiers?	223
Searching for Tripwire Enterprise Objects	232
How Do I Run a Search?	232
Creating a Saved Search	234
Loading a Saved Search	234
Deleting, Importing, and Exporting Saved Searches	235
Creating a Launch-in-Context URL	235
Using Launch-in-Context URLs	236
Integrating Tripwire Enterprise with Other Applications	237
What is the Tripwire Enterprise AAA Log Monitoring Tool?	237
What is the Command Line Interface?	238

Chapter 4. Home Page Procedures 239

Viewing, Creating, and Deleting Objects in the Home Page Manager	240
Viewing Home Pages and Widgets	240
Creating a Home Page	241
Changing the Properties of a Home Page	242
Duplicating a Home Page	244
Deleting a Home Page	244
Working with Widgets	245
Adding a Widget to a Home Page	245

Working with an Alert Widget	246
Working with a Dashboard Widget	248
Working with a Failing Tests Widget	249
Working with a Log Center Event Widget	251
Working with a Report Widget	251
Working with a Remediation Work Order Widget	253
Deleting a Widget	254
Working with Remediation Work Orders	255
Creating a Remediation Work Order	255
Assigning a Work Order	257
Approving or Denying Remediation Entries in a Work Order	258
Running or Deferring Remediation in a Work Order	259
Closing or Deleting a Work Order	260

Chapter 5. Settings Procedures 261

User Settings	262
Changing User Preference Settings	262
Changing User Difference Settings	265
System Settings	266
Changing System Preferences	266
Changing Log Management Settings	268
Recalculating Database Index Statistics	269
Working with Severity Ranges	270
Working with Global Variables	271
Working with E-mail Servers	272
Working with Approval Templates	273
Configuring Tripwire Enterprise Console Properties	274
Importing Settings	276
Exporting Settings	277
Creating Diagnostic Files for Tripwire Support	278
Upgrading Agents	279

Administration Settings	283
Importing Post-Remediation Service Commands	283
Changing Post-Remediation Service Commands	283
Exporting Post-Remediation Service Commands	284
Deleting Post-Remediation Service Commands	284
Creating a User Account	285
Changing User Account Properties	286
Changing the Password for a User Account	286
Assigning a User Role to a User Account	287
Associating User Accounts with User Groups	287
Unlocking a User Account	288
Deleting User Accounts	288
Working with User Groups	289
Creating a Home Page	290
Duplicating a Home Page	290
Changing the Properties of a Home Page	291
Deleting Home Pages	291
Exporting Home Pages	292
Importing Home Pages	292
Working with User Roles	293
Configuring the Tripwire Enterprise Login Method	294
Adding a License File	297
Deleting Licenses	297
Custom Properties	298
Working with Custom Properties	298
Monitoring Preferences	299
Working with Custom Node Types	299
Creating a Criteria Set for a File System Rule	300
Creating a Criteria Set for a Windows Registry Rule	304
Creating a Criteria Set for a Windows RSoP Rule	306
Creating a Criteria Set for a Database Rule	307

Changing Criteria Set Properties	308
Duplicating Criteria Sets	309
Deleting Criteria Sets	309
Setting File System Preferences	310
Setting LDAP Directory Preferences	311
Setting Active Directory Preferences	311
Chapter 6. Node Procedures	312
Viewing and Changing Objects in the Node Manager	313
Viewing Nodes, Node Groups, and Elements	313
Monitoring the Health of Nodes and Resolving Errors	317
Viewing Changed Nodes	320
Filtering Elements in the Node Manager	320
Changing the Properties of a Node	321
Changing the Properties of a Node Group	325
Changing the Properties of an Element	326
Changing the Properties of an Element Version	327
Defining Values for Custom Properties	328
Working with Node Access Controls	333
Working with Policy Test Results in a Node Properties Dialog	335
Classifying Nodes with Tags	339
Getting Started with Tags	339
Tagging Best Practices	342
Using the Asset View Tab	346
Viewing Specific Nodes or Groups in Asset View	351
Working with Tags and Tag Sets	352
Working with Saved Filters	353
Working with Tagging Profiles	354
Searching for Nodes, Elements, and Versions	355
Searching for Nodes	355
Searching for Elements	361

Searching for Element Versions	364
Creating and Deleting Objects in the Node Manager	368
Creating a Node Group	368
Creating a Custom Node	368
Creating a Directory Server Node	369
Creating a Database Node	370
Creating a Network Device Node	374
Creating a VI Management Node	375
Duplicating Nodes	376
Deleting Nodes and Node Groups	377
Deleting Elements	378
Moving, Linking, and Unlinking Objects in the Node Manager	379
Moving Nodes and Node Groups	379
Linking Nodes and Node Groups	380
Unlinking Nodes and Node Groups	381
Baselining and Version Checking Monitored Objects	382
Initial Baselining of Monitored Objects	382
Re-baselining Monitored Systems	383
Re-baselining Specific Monitored Objects	384
Version Checking Monitored Systems	385
Version Checking Specific Monitored Objects	386
Temporarily Disabling Checks and Baselines on a Node	387
Comparing Element Versions	388
Comparing a Current Change Version with the Current Baseline	388
Comparing an Element Version with the Current Baseline	389
Comparing Any Two Versions of the Same Element	390
Comparing Any Two Versions of Different Elements	391
Clearing Mark for Compare Selections	392
Promoting Element Versions	393
Promoting a Specific Element Version	393
Promoting All Current Versions for a Node or Node Group	395

Promoting by Match	396
Promoting by Reference	397
Changing Rules with the Adjust Rule Feature	398
Adding a Start Point with the Adjust Rule Feature	398
Editing a Start Point with the Adjust Rule Feature	399
Adding a Stop Point with the Adjust Rule Feature	400
Deleting a Stop Point with the Adjust Rule Feature	401
Using the Run Actions Feature	402
Running Actions for Specific Elements	402
Running Actions for a Node or Node Group	403
Restoring a Changed File with the Run Actions Feature	404
Restoring Multiple Files with the Run Actions Feature	405
Exporting and Importing Objects in the Node Manager	406
Exporting Nodes and Node Groups	406
Importing Nodes and Node Groups	407
Exporting, Importing, and Cloning Element Versions	408
Exporting the Content of an Element Version	408
Importing Element Version Content	409
Cloning an Element Version	410
Managing Agent Nodes	411
Assigning a Delegated Agent to a Node	411
Restarting Tripwire Enterprise Agents	412
Upgrading Agents	413
Changing TE Agent Configuration Properties	417
Managing Licenses for Nodes	418
Configuring SSL for Database, Directory Server, and Virtual Nodes	419
Configuring Audit Event Collection and Real-Time Monitoring for Multiple Systems	422
Downloading Agent Log Files	423
Restricting Commands on Agent Nodes with Whitelists	424
Restricting Queries on Database Nodes with Whitelists	429

Chapter 7. Rule Procedures 431

Viewing and Changing Objects in the Rule Manager	432
Viewing Rules and Rule Groups	432
Searching for Rules	434
Changing the Properties of a Rule	437
Changing the Properties of a Rule Group	440
Changing the List of Monitored Objects in a File Rule or Configuration File Rule	441
Changing Filter or Search-and-Replace Criteria for a COVR or COCR	442
Working with Rule Access Controls	443
Creating and Deleting Objects in the Rule Manager	445
Creating a Rule Group	445
Creating a Command Output Capture Rule	445
Creating a Command Output Hypervisor Rule	446
Creating a Command Output Validation Rule	446
Creating a Configuration File Rule	447
Creating a Database Metadata Rule	448
Creating a Database Query Rule	449
Creating a Directory Rule	450
Creating a File Rule	451
Creating a Log Transfer Rule	451
Creating a Status Check Rule	452
Creating a VI Hypervisor Rule	453
Creating a Virtual Machine Configuration Rule	453
Creating a Virtual Switch Configuration Rule	454
Creating a Distributed Virtual Switch Configuration Rule	455
Creating a File System Rule	455
Creating a Windows Registry Rule	457
Creating a Windows RSoP Rule	458
Duplicating Rules	459
Deleting Rules and Rule Groups	459
Working with Start Points, Stop Points, Queries, and RSoP Specifiers	461
About Start Points and Stop Points	461

Adding a Start Point to a Rule	462
Changing or Deleting Start Points	466
Adding a Stop Point to a Rule	467
Changing or Deleting Stop Points	469
Adding a Query to a Database Query Rule	470
Changing or Deleting Queries in a Database Query Rule	471
Adding a Specifier to a Windows RSoP Rule	472
Changing or Deleting Specifiers in a Windows RSoP Rule	472
Moving, Linking, and Unlinking Objects in the Rule Manager	473
Moving Rules and Rule Groups	473
Linking Rules and Rule Groups	473
Unlinking Rules and Rule Groups	474
Exporting and Importing Objects in the Rule Manager	475
Exporting Rules and Rule Groups	475
Importing Rules and Rule Groups	476

Chapter 8. Action Procedures 477

Viewing and Changing Objects in the Action Manager	478
Viewing Actions and Action Groups	478
Searching for Actions	480
Changing the Properties of an Action	482
Changing the Properties of an Action Group	487
Ordering Actions in an Action Group	488
Working with Action Access Controls	489
Creating and Deleting Objects in the Action Manager	491
Creating an Action Group	491
Creating a Conditional Action	491
Creating an E-mail Action	492
Creating an Execution Action	493
Creating a Promote Action	495
Creating a Restore Action	496

Creating a Run Command Action	497
Creating a Run Report Action	497
Creating a Run Rule Action	498
Creating a Run Task Action	498
Creating a Set Custom Value Action	499
Creating a Severity Override Action	499
Creating an SNMP Action	500
Creating a Syslog Action	500
Duplicating Actions	501
Deleting Actions and Action Groups	502
Moving, Linking, and Unlinking Objects in the Action Manager	503
Moving Actions and Action Groups	503
Linking Actions and Action Groups	503
Unlinking Actions and Action Groups	504
Exporting and Importing Objects in the Action Manager	505
Exporting Actions and Action Groups	505
Importing Actions and Action Groups	506

Chapter 9. Task Procedures 507

Viewing and Changing Objects in the Task Manager	508
Viewing Tasks and Task Groups	508
Searching for Tasks	510
Changing the Properties of a Task	512
Changing the Properties of a Task Group	514
Working with Task Access Controls	515
Creating and Deleting Objects in the Task Manager	517
Creating a Baseline Rule Task	517
Creating a Check Rule Task	518
Creating a Report Task	519
Creating a Task Group	519
Duplicating Tasks	520

Deleting Tasks and Task Groups	521
Working with Objects in the Task Manager	522
Creating Current Baselines for a Check Rule Task	522
Running Tasks and Task Groups Manually	523
Stopping Tasks and Task Groups Manually	523
Enabling Tasks	523
Disabling Tasks	524
Moving, Linking, and Unlinking Objects in the Task Manager	525
Moving Tasks and Task Groups	525
Linking Tasks and Task Groups	525
Unlinking Tasks and Task Groups	526
Exporting and Importing Objects in the Task Manager	527
Exporting Tasks and Task Groups	527
Importing Tasks and Task Groups	528

Chapter 10. Policy Procedures 529

Viewing and Changing Objects in the Tests Tab	530
Viewing Policy Manager Objects in the Tests Tab	530
Searching for Policy Tests	532
Changing the Properties of a TE Policy	534
Changing the Properties of a Policy Test	536
Changing the Properties of a Policy Test Group	538
Changing the Properties of Multiple Policy Tests	539
Working with Policy Access Controls	541
Creating and Deleting Objects in the Policy Manager	543
Creating a TE Policy	543
Creating a Policy Test	545
Creating a Policy Test Group	547
Duplicating Policy Tests	548
Deleting Policy Manager Objects	549
Viewing Results in the Compliance Tab	550

Viewing Policy Manager Objects in the Compliance Tab	550
Viewing Policy Test Results from the Compliance Tab	554
Working with Scoring Thresholds	555
Filtering Compliance Statistics in the Policy Manager	557
Searching for Policy Test Results	559
Running, Promoting, and Waiving Policy Tests	561
Running Policy Tests Manually	561
Promoting Policy Test Results	562
Creating a Waiver	564
Changing the Properties of a Waiver	566
Searching for Waivers	567
Closing Waivers	569
Deleting Waivers	569
Moving, Linking, and Unlinking Objects in the Policy Manager	570
Moving Policy Manager Objects	570
Linking Policy Manager Objects	571
Unlinking Policy Manager Objects	572
Exporting and Importing Policy Manager Objects	573
Exporting Policy Manager Objects	573
Importing Policy Manager Objects	574
Chapter 11. Log Message Procedures	575
Viewing, Sorting, and Filtering TE Log Messages	576
Viewing TE Log Messages in the Log Manager	576
Viewing the Properties of a Log Message	577
Filtering Log Messages	578
Searching for TE Log Messages	579
Searching for TLC Log Messages	581
Exporting and Deleting Log Messages	582
Exporting Log Messages	582
Deleting TE Log Messages	583

Chapter 12. Report Procedures	584
Viewing and Changing Objects in the Report Manager	585
Viewing Reports, Report Groups, and Dashboards	585
Searching for Reports	587
Changing the Properties of a Report	589
Changing the Properties of a Report Group	590
Changing the Properties of a Dashboard	591
Creating and Deleting Objects in the Report Manager	592
Creating a Report	592
Creating a Report Group	593
Creating a Dashboard	594
Duplicating Reports and Dashboards	595
Deleting Reports, Report Groups, and Dashboards	596
Moving, Linking, and Unlinking Objects in the Report Manager	597
Moving Reports, Report Groups, and Dashboards	597
Linking Reports, Report Groups, and Dashboards	597
Unlinking Reports, Report Groups, and Dashboards	598
Exporting and Importing Objects in the Report Manager	599
Exporting Reports, Report Groups, and Dashboards	599
Importing Reports, Report Groups, and Dashboards	600
Working with the Output of Reports and Dashboards	601
Running a Report Manually	601
Running a Dashboard	607
Archiving Report Output	607
Working with Archived Report Output	608
Deleting Archived Report Output	609
 Appendices	 610
Appendix I: Definitions of User Permissions	611
 Index	 617

About This Guide

Overview

The *Tripwire Enterprise User Guide* includes the following chapters:

- [Chapter 1: Introduction to Tripwire Enterprise \(on page 23\)](#) introduces the components of Tripwire Enterprise and the user interface.
- [Chapter 2: Getting Started \(on page 31\)](#) outlines the steps involved in preparing TE for change auditing and configuration assessment.
- [Chapter 3: Terms, Concepts, and Functions \(on page 35\)](#) presents a discussion of all TE objects, features, and processes.
- [Chapter 4: Home Page Procedures \(on page 239\)](#) shows how to create, configure, and use Tripwire Enterprise home pages.
- [Chapter 5: Settings Procedures \(on page 261\)](#) explains how to create TE objects and adjust application parameters in the Settings Manager.
- [Chapter 6: Node Procedures \(on page 312\)](#) provides instructions for managing and monitoring systems on your network.
- [Chapter 7: Rule Procedures \(on page 431\)](#) outlines the procedures involved in creating and administering rules.
- [Chapter 8: Action Procedures \(on page 477\)](#) describes how to create, modify, and enable actions.
- [Chapter 9: Task Procedures \(on page 507\)](#) explains how to create, schedule, and run tasks.
- [Chapter 10: Policy Procedures \(on page 529\)](#) describes how to create, change, and manage TE policies and policy tests.
- [Chapter 11: Log Message Procedures \(on page 575\)](#) includes directions for reviewing and maintaining log messages.
- [Chapter 12: Report Procedures \(on page 584\)](#) outlines procedures for creating, managing, and running both reports and dashboards.
- The [Appendices \(on page 610\)](#) describe each TE user permission and identify the permissions required for each procedure in this guide.

Document List

The *Tripwire Enterprise Installation & Maintenance Guide* provides installation and upgrade instructions for Tripwire Enterprise software. In addition, this guide includes procedures for the maintenance of your Tripwire Enterprise software and database.

The *Tripwire Enterprise User Guide* provides a detailed overview of Tripwire Enterprise functionality, along with related concepts and procedures.

The *Tripwire Enterprise Reference Guide* contains supplemental information for the operation of Tripwire Enterprise software and associated applications.

PDF versions of these documents are available:

- on the Downloads page of the Tripwire Customer Center (<https://tripwireinc.force.com/customers>)
- in the docs directory of the Tripwire Enterprise installation DVD
- in the TE Console download archive

In addition, **online help** may be accessed from the Tripwire Enterprise interface. The online help includes the content of all documents cited above.

Document Conventions

Convention	Description
Bolding	Indicates: <ul style="list-style-type: none">• The labels of buttons, menus, fields, drop-downs, and check boxes.• Options selected from a drop-down list or menu.• Keystrokes and menu paths.• Introductory sentences for procedures.• The first reference of a term. Examples: <ul style="list-style-type: none">• In the Monitor dialog, select the Activate check box.• Press CTRL+DELETE.
<i>Italics</i>	Indicates cross references to sections and chapters in this book, as well as the titles of other books. Example: "For more information, see <i>Creating a Node</i> ."
Sans Serif	Indicates: <ul style="list-style-type: none">• URLs and e-mail addresses• Directory paths and file names• Command-line entries Examples: <ul style="list-style-type: none">• <code>www.tripwire.com</code>• <code>C:\Program Files\</code>
Brackets	Indicates a set of possible user-entered options; individual options are separated by the pipe () character. Example: [1 2 3]
Angle brackets	Indicates placeholders for user-entered values. Example: <a_variable>

Contact Information

Tripwire, Inc.

308 SW Second Ave, Suite 400
Portland, OR 97204
Web site: <https://www.tripwire.com>
Main: 503.276.7500
Fax: 503.223.0182
US Toll-free: 1.800.TRIPWIRE (1.800.874.7947)

Tripwire Sales

Domestic: sales@tripwire.com
Government: govt@tripwire.com
EMEA: emeasales@tripwire.com
APAC: apacsales@tripwire.com
Japan: info@tripwire.co.jp

Tripwire Technical Support

Online support: <https://tripwireinc.force.com/customers>
Support policies: <https://www.tripwire.com/customers/support-policy/>
Contact: <https://tripwireinc.force.com/customers/contact>

Tripwire Professional Services

Tripwire Professional Services provides a wide range of services, including Tripwire Quickstarts, Turnkey Implementations, Change Auditing, and Process Improvement. For more information, please visit <https://www.tripwire.com/services> or contact your Tripwire sales representative.

Tripwire Educational Services

Tripwire Educational Services provides hands-on technical training for the installation, configuration, and maintenance of your Tripwire software. All courses are taught by Tripwire Certified Instructors. For more information, please contact your Tripwire sales representative or visit <https://www.tripwire.com/services/training>.

Product Alerts and Notifications

The Tripwire Forums provide an online community where you can ask questions, get help from other Tripwire users, and find the latest product updates and alerts. Subscribe to the product-alert channels to receive notifications about important product issues that may affect your environment. To subscribe, visit <https://forums.tripwire.com>.

Chapter 1. Introduction to Tripwire Enterprise

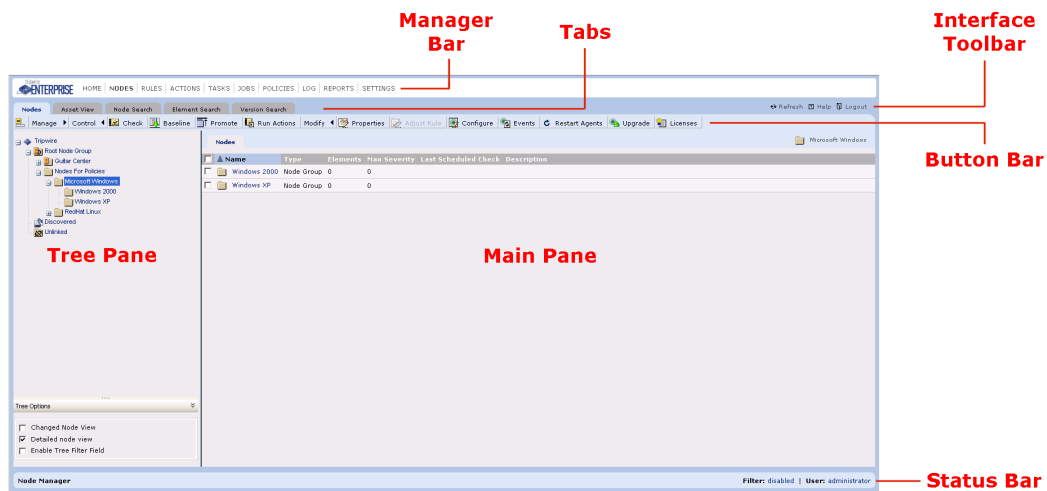
The Tripwire Enterprise Console Interface

The **TE Console interface** is a Web-based GUI that allows an unlimited number of users to simultaneously use Tripwire Enterprise. [Figure 1](#) shows the main components of the interface, which are described in greater detail in this section.

Notes When working in the TE Console interface, do **not** use your Web browser's **Forward**, **Back**, or **Refresh** buttons.

The Home Page Manager has a different interface. For more information, see [Viewing Home Pages and Widgets on page 240](#).

Figure 1. The TE Console interface



Manager Bar and Tabs

Use the Manager bar ([Figure 2 below](#)) to select the component of Tripwire Enterprise that you want to use. Each Manager in Tripwire Enterprise controls a different component of the software. For example, the Node Manager is used to view, create, and perform other actions on nodes. For a description of the objects that each Manager controls, see [Tripwire Enterprise Managers and Objects on page 27](#).

Based on the permissions assigned to your user account, some Managers may not be accessible from the Manager bar.

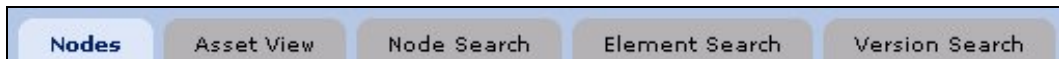
Figure 2. The Manager Bar



Tip Click the Tripwire Enterprise logo on the left side of the button bar to see the Tripwire Enterprise version and build number that you are using.

When you select a Manager in the Manager bar, TE displays a unique set of tabs (Figure 3) along the top of the interface. Each tab contains a sub-set of functions and data for the selected Manager.


Figure 3. Tabs for the Node Manager



Button Bar

The **button bar** (Figure 4) consists of buttons that initiate TE functions. The actual buttons in the bar depend on which Manager is selected in the Manager bar, and which tab is selected in the Manager. Some Managers have many buttons grouped in expandable **button sets**. To expand or retract a button set, click the corresponding button.

Some buttons in the button bar may be disabled until you select an appropriate object for that action. And as with the Manager bar, some buttons may be permanently disabled, based on the permissions for your user account.

The label button  at the left end of the button bar toggles the display of text labels through three states:




- Show all labels in a Manager's button bar.
- Hide all labels in a Manager's button bar.
- Show the label of a button only when you move your cursor over the button.

Figure 4. The Button bar (with the Control button set expanded)



Interface Toolbar

The interface toolbar, in the upper right section of the Console, consists of the following buttons:

-  **Refresh** updates displayed data with the latest information. Do **not** use your Web browser's Refresh button to refresh data in the Tripwire Enterprise interface.
-  **Help** opens the TE online help system.
-  **Logout** ends the current user session.

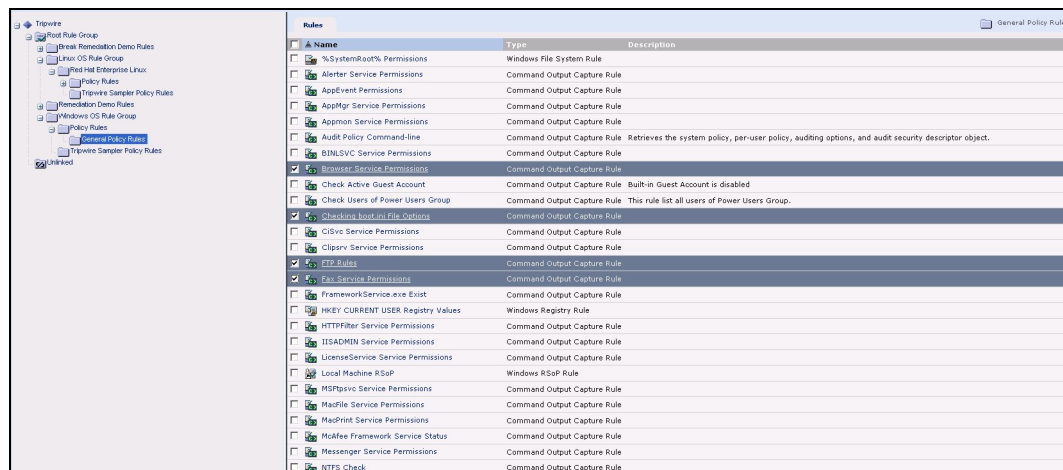
Tree Pane and Main Pane

In most Managers, the tree pane displays the hierarchy of groups used to organize the objects in that Manager. If you select an object in the tree pane, information about that object is displayed in the main pane. For example, if you select a group, all of the objects and groups descended from that group are displayed.

To execute an action on an **object** in TE, you first select the object's parent group in the tree pane, then select the object in the main pane. To execute an action on a **group**, you first select the group's parent group in the tree pane, then select the group in the main pane. To execute an action on **all of the objects in a Manager**, select the Root group for that Manager in the tree pane, then select all of the descendant objects in the main pane.

In [Figure 5](#), the General Policy Rules group is selected in the tree pane, and a number of rules in that group are selected in the main pane.

Figure 5. The Tree pane and Main pane



Status Bar

The status bar displays the following information:

- The Manager that is currently open.
- The name of the current user. Click the user name in the status bar to view and edit the settings for that user account.
- The last time that the TE Console updated the audit event and real-time monitoring configuration for all Tripwire Axon Agents (Axon Agents). Individual Axon Agents may have been updated more recently. Click **Last Axon Agent config** to open the Task Manager, where you can manually run the Configure Axon Agents task. For more information, see [What is Audit Event Collection? \(on page 63\)](#) and [How Does Real-Time Monitoring Work? \(on page 70\)](#).

Tripwire Enterprise Managers and Objects

The Tripwire Enterprise UI consists of a number of **Managers**. You use each Manager to control different types of **Tripwire Enterprise objects**. [Table 1 \(below\)](#) identifies each TE Manager and the objects available in each Manager. To open a Manager, click the Manager's link in the **Manager bar** (see [The Manager Bar on page 24](#)).

Table 1. Types of Tripwire Enterprise objects in each TE Manager

Manager Bar Link	Manager Name	Tripwire Enterprise Object Types
HOME	Home Page Manager	A home page is a TE interface page in which users can run specific reports and dashboards, or review alerts about TE system events. For more information, see What are Home Pages and Widgets? on page 189 .
NODES	Node Manager	<ul style="list-style-type: none"> A node represents a monitored system, which is a file server, directory server, network device, database, or virtual infrastructure (VI) component audited by Tripwire Enterprise. For more information, see What are Node Types? on page 51. An element represents a monitored object, which is a component or property of a monitored system that has been audited by TE. For instance, an element might represent a file or the availability of a monitored system. For further details, see What Does Tripwire Enterprise Monitor? on page 37. An element version is a record of a monitored object's state at a specific point in time. The element versions created for a monitored object provide a historical archive of changes made to the object. For further details, see How Tripwire Enterprise Detects Change on page 36.
RULES	Rule Manager	A rule identifies one or more monitored objects. For an introduction to rules, see What are Rule Types? on page 79 .
ACTIONS	Action Manager	An action initiates a response to changes detected by Tripwire Enterprise or failures generated by policy tests. For example, if TE detects an unauthorized change, an action could send an e-mail notification to appropriate personnel. For further details, see What are Actions and Action Types? on page 116 .
TASKS	Task Manager	A task runs a Tripwire Enterprise operation on a manual or scheduled basis. For more information, see What are Task Types? on page 127 .
POLICIES	Policy Manager	<ul style="list-style-type: none"> A TE policy measures the degree to which the configurations of monitored systems are in compliance with a policy, such as an industry or corporate standard. A policy test determines if monitored systems comply with a specific requirement of a policy. For more information, see What are Policy Manager Objects? on page 131.
LOG	Log Manager	A log message is a record of network or user activity created by Tripwire Enterprise or Tripwire Log Center (TLC). For more information, see What are Log Messages? on page 166 .

Manager Bar Link	Manager Name	Tripwire Enterprise Object Types
REPORTS	Report Manager	<ul style="list-style-type: none"> • A report compiles current data about systems monitored by Tripwire Enterprise. With reports, you can easily review and assess the current state of your network. For an overview of Tripwire Enterprise's reporting capabilities, see What are Reports and Report Types? on page 172. • A dashboard is a user-defined collection of reports that may be run and viewed at the same time. By adding reports to a dashboard, you can review the latest output for all of the reports in a single window. For more information, see What are Dashboards? on page 182.
SETTINGS	Settings Manager	Tripwire Enterprise settings consist of a variety of TE objects, system parameters, and monitoring preferences. For more information, see What are Settings? on page 194 .

About Groups

A **group** is a collection of one or more Tripwire Enterprise objects in a Manager. [Table 2 \(on the next page\)](#) describes the groups that are created by default when TE is installed. Default groups cannot be deleted.

Note In addition to regular groups, the Node Manager can also contain smart node groups, which reflect tags and other elements in the Asset View tab. For more information, see [About Node Groups and Smart Node Groups on page 57](#). The Node Manager also has additional default groups.

In the Root Group of a Manager, you can create additional groups to organize the TE objects in the Manager. For example, in the Node Manager, you might create a node group that contains a collection of nodes and/or other node groups.

Typically, a user-created group consists of TE objects that share a common trait. For instance, a node group may contain nodes with similar geographic locations or functions. When you check a node group for changes, the operation runs on all applicable nodes within the group.

To create groups in TE Managers, see:

- [Creating a Node Group \(on page 368\)](#)
- [Creating a Rule Group \(on page 445\)](#)
- [Creating an Action Group \(on page 491\)](#)
- [Creating a Task Group \(on page 519\)](#)
- [Creating a Policy Test Group \(on page 547\)](#)
- [Creating a Report Group \(on page 593\)](#)

Note TE policies and VI management nodes are similar to groups since they contain other TE objects. For more information, see:

- [What are Policy Manager Objects? \(on page 131\)](#)
- [Monitoring Virtual Systems with Tripwire Enterprise \(on page 59\)](#)

Table 2. Default groups

Default Group	Description
Root Group	<p>In a Manager, all user-created groups are created within the Manager's Root Group. As needed, you may create new TE objects within the Root Group itself, or any sub-group of the Root Group.</p> <ul style="list-style-type: none">• To add an existing TE object (including another group) to a group, you can move the object from another group or create a link. For more information, see What are Links and Linked Objects? on page 213.• In the Root Group of the Node Manager, the VI node discovery process creates node groups that represent virtual infrastructure objects. For more information, see Monitoring Virtual Systems with Tripwire Enterprise on page 59.
Unlinked Group	<p>When a TE object is unlinked from all groups in a Manager, Tripwire Enterprise moves the object to the Manager's Unlinked Group. For more information, see How Do Links Work? on page 214.</p>

Chapter 2. Getting Started

Using Tripwire Enterprise Fast Track

Fast Track will help you to configure Tripwire Enterprise for Change Auditing, Policy Management, or an integrated Security Configuration Management (SCM) solution. It only takes a few minutes to complete the setup questionnaire. After you do, Fast Track will use your answers to install the components that you need.

For new installations of Tripwire Enterprise Console, Fast Track launches automatically after you log into the software and configure the default administrator user account. You cannot use Fast Track to configure an upgraded installation of Tripwire Enterprise.

Note Do not use your browser's **Forward** or **Back** buttons while using Fast Track.

Step 1. Add your Tripwire Enterprise License

In order to use Tripwire Enterprise, you must first add a license file. Tripwire Enterprise license files include `twenterprise.cert` in the file name.

Step 2. Configure Change Auditing and/or Policy Management

Change Auditing protects your enterprise by checking monitored systems for change. **Policy Management** ensures that monitored systems are in compliance with external or internal policies.

Available Policies lists common policies that Fast Track can install. You can add additional policies later from the Tripwire Enterprise Console.

Step 3. Specify the Platforms to Monitor

If you select a platform from the **Available Platforms** list, Fast Track will automatically install the components that Tripwire Enterprise needs to monitor that platform. You can always configure the software to monitor additional platforms later.

Step 4. Set up a Schedule for Running Checks and Reports

In this section, you can schedule the frequency with which Tripwire Enterprise checks monitored systems for change or compliance. You can also schedule times when the software generates reports on the state of your systems.

Some guidelines when scheduling checks and reports:

- If you are scheduling both checks and reports, we recommend that you stagger the start times by at least 3 hours to ensure that reports always have the most recent information.
- If you are scheduling both Change Auditing and Policy Management checks, allow enough time for the Change Auditing checks to finish before starting Policy Management checks.

If you need to change the schedule that you specify here, it's easy to adjust the start times later in the Tripwire Enterprise Console.

Step 5. Configure an E-mail Server for Sending Reports and Alerts

Tripwire Enterprise can use e-mail to inform users about changes to monitored systems. You can specify the e-mail server that Tripwire Enterprise should use now, or do it later.

Step 6. Create an Administrator Account for Tripwire Enterprise Console

The user account that you create here will have administrative permissions in Tripwire Enterprise. Make sure to create a strong password and manage it appropriately.

Next Steps

After Fast Track is complete, you will be logged into Tripwire Enterprise Console using the account you just created. To finish the initial configuration of Tripwire Enterprise, see [After Fast Track on the next page](#).

After Fast Track

After Fast Track is finished, you need to perform a few more tasks to begin using Tripwire Enterprise.

Tip For information on administering the configuration created by Fast Track, see https://tripwireinc.force.com/customers/CommunitySiteLogin?startURL=/articles/Standard_Operations/Information-about-Fast-Track-Results

- **Install Tripwire Enterprise Agent and/or Tripwire Axon Agent software.** You need to install this software on each server that you want to monitor. For more information, see *Installing Tripwire Enterprise Agent* and *Installing Tripwire Axon Agent* in the *Tripwire Enterprise Installation & Maintenance Guide*
- **Enable tasks to run checks and reports.** If you didn't enable the check and reporting tasks you created in the Fast Track interface, you should do so after you install Agent software. For more information, see [Enabling Tasks on page 523](#).
- **Create tags and tagging profiles to automatically classify your assets.** You can use tags to automatically organize the assets you monitor by operating system, location, organizational unit, or any other criteria you choose. For more information, see [Getting Started with Tags on page 339](#).

Chapter 3. Terms, Concepts, and Functions

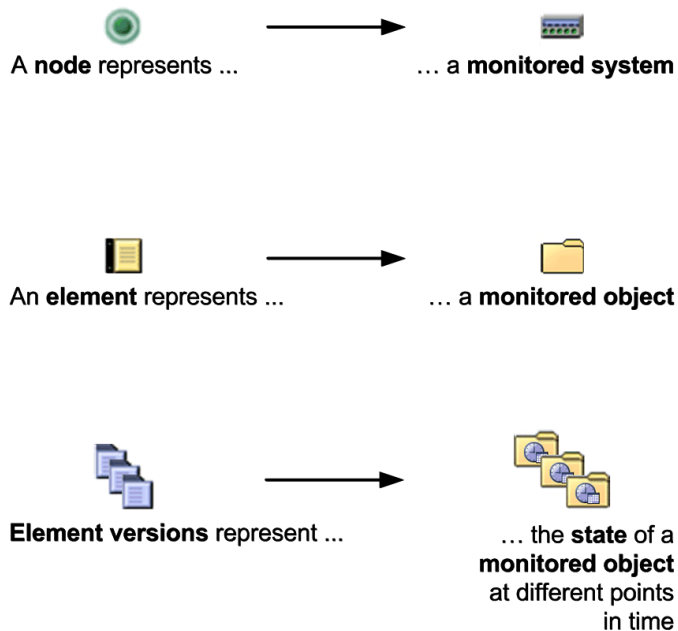
How Tripwire Enterprise Detects Change

Overview

Tripwire Enterprise uses a few basic components to detect change:

- A **node** represents a system on your network, such as a server or a network device, that you want to monitor for change. For a list of nodes you can create in TE, see [What are Node Types? on page 51](#).
- A **rule** identifies a component of a node that you want to monitor, known as a **monitored object**. Often a rule specifies a file or directory in a file system and the attributes of that object (content, permissions, hashes, etc.) that you want to monitor. However, rules can also be used to monitor other aspects of a system, such as its availability, or the output that it returns when Tripwire Enterprise runs a specific command. For a list of rules you can create in TE, see [What are Rule Types? on page 79](#).
- When Tripwire Enterprise applies a rule to a node, it generates an **element**. An element represents a single monitored object on a single node. Because monitored objects can change over time, Tripwire Enterprise creates multiple **element versions** for each element. Each element version represents the state of a monitored object at a specific point in time. For a list of monitored objects in TE, see [What Does Tripwire Enterprise Monitor? on the next page](#).

Figure 6. Items represented by a node, element, and element version



The first time that you check a node with a rule (known as a **version check**), Tripwire Enterprise creates an element for each monitored object on each node checked. The initial version of an element that is created during this process is called the **baseline version**, and usually represents a monitored object in a known good state.

The next time a version check runs, Tripwire Enterprise compares the current state of a monitored object against the baseline version. If the monitored object hasn't changed, nothing happens. If TE detects a change to the monitored object, it creates a new element version for the element, which is called a **change version**.

For changes that represent an unwanted change to a monitored object, Tripwire Enterprise can be configured to run **actions**, automated responses that range from sending an e-mail notification to executing a series of commands. For more information, see [What are Actions and Action Types? on page 116](#).

If a change version represents an approved change, you can promote the change version in Tripwire Enterprise, making it the new baseline version. For more information, see [What is Promotion? on page 47](#).

What Does Tripwire Enterprise Monitor?

Components of nodes that you want to monitor are known as **monitored objects**. Monitored objects are often files or directories in a file system, but can also represent other aspects of a system, such as its availability, or the output that it returns when Tripwire Enterprise runs a specific command. Each monitored object on a node is represented by an **element**, and an **attribute** is a specific property of a monitored object that TE can audit for changes. For instance, an element may be created for a configuration file (the monitored object), and file size is an attribute of the file that can be monitored by TE.

The following tables list the types of elements that TE can create for each type of node:

- Directory server nodes ([Table 3 on the next page](#))
- Database nodes ([Table 4 on the next page](#))
- Network device nodes ([Table 5 on the next page](#))
- File server nodes ([Table 6 on page 39](#))
- Virtual infrastructure nodes ([Table 7 on page 39](#))

Table 3. Types of elements for directory server nodes

Element Type	Description and Attributes
entries	An entry is a record in a directory. Tripwire Enterprise creates a single element for each monitored entry, and each of the entry's attributes can be monitored for change. Binary attributes are stored as a hash (MD5 or SHA-1).

Table 4. Types of elements for database nodes

Element Type	Description and Attributes
database objects	<p>Tripwire Enterprise can monitor the objects in a database; for example, tables, views, indices, or stored procedures. For each database object, Tripwire Enterprise creates a single element consisting of the database definition language (DDL) statements that define the object. A hash (MD5, SHA-1, SHA-256, and/or SHA-512) of DDL statements is the only attribute that can be monitored for change.</p> <p>Note: For PostgreSQL databases, the element's content may not include the complete DDL for any given database object. Database elements should NOT be used to remediate or recreate any database objects in PostgreSQL databases.</p>
configuration parameters	A hash (MD5, SHA-1, SHA-256, and/or SHA-512) is the only attribute of a database configuration parameter that can be monitored for change. The hash is a digest of a string that identifies the parameter's name, description, and value.
query results	<p>To check the content of a database for changes, you can run a SQL query on one or more tables and/or views. Tripwire Enterprise compares the query results with previous results to identify any changes in content.</p> <p>TE creates a single element for each defined query run on a database. A hash (MD5, SHA-1, SHA-256, and/or SHA-512) of query results is the only attribute that can be monitored for change.</p>

Table 5. Types of elements for network device nodes

Element Type	Description and Attributes
availability	Availability is the network connectivity status of a network device. This element indicates whether or not the Tripwire Enterprise Server can access the device.
configuration files	An MD5 hash of file content is the only attribute of a configuration file that can be monitored for change.
command output	<p>To check the settings or parameters of a network device for changes, you can run a command on the device to generate and capture output. Tripwire Enterprise then compares the output with previous output to identify any variances. For example, you could run a command to generate the routing tables for a router or the active rules of a firewall.</p> <p>A hash of command-output content is the only attribute of command output that can be checked for changes.</p>

Table 6. Types of elements for file server nodes

Element Type	Description and Attributes
command output	<p>To check the settings or parameters of a file server for changes, you can run a command on the server to generate and capture output. TE then compares the output with previous output to identify any variances. For example, you could run a command to generate a list of service packs that are currently installed for a file server's operating system.</p> <p>For this type of element, attributes include a hash of command-output content and the exit code (or return code) that results from running the command.</p>
files and directories	<p>TE can monitor the files and directories in a file system.</p> <ul style="list-style-type: none"> • For a list of attributes that may be monitored on UNIX file systems, see Table 76 on page 301. • For a list of attributes that may be monitored on Windows file systems, see Table 77 on page 302.
registry keys and entries	<p>On a Windows file server, TE can monitor the keys and entries in the server's registry. For a list of registry attributes that may be monitored, see Table 78 on page 304.</p>
Resultant Set of Policy (RSoP)	<p>To monitor the Resultant Set of Policy (RSoP) for a Windows user, you can run a query of the file server's RSoP plug-in. The query retrieves a report of the plug-in's RSoP calculations for the user. To identify any changes, TE compares the new RSoP report with a previous version of the report.</p> <p>TE creates a single element for each monitored RSoP. A hash (MD5 and/or SHA-1) of an RSoP report is the only attribute that can be monitored for change.</p>

Table 7. Types of elements for virtual infrastructure nodes

Element Type	Description and Attributes
configuration files	<p>Tripwire Enterprise can monitor the content of a hypervisor's configuration files in the file system of a host machine.</p>
configuration parameters	<p>Tripwire Enterprise can monitor the values of configuration parameters assigned to hypervisors, virtual machines, virtual switches, and distributed virtual switches.</p>
command output	<p>To check the settings of an operating system on a hypervisor's host machine, you can run a command to generate and capture output. Tripwire Enterprise then compares the output with previous output to identify any variances. For example, you could run a command to generate a list of permissions for specified files and directories.</p>

Element Differences Between TE Agent and the Axon Agent

If you migrate a monitored system from TE Agent to Axon Agent, all of the element data collected by the TE Agent will be preserved and can still be viewed after Axon Agent is installed. After migrating, you may see minor differences between existing elements collected by the TE Agent and elements collected by the Axon Agent. These differences are expected due to more accurate data collection by the Axon Agent. Specific differences between the two Agents are listed in this section.

Command Output Capture Rules (COCRs)

1. A TE Agent will reject a request to run a version check using a COCR rule if the rule is currently being used in another check. The Axon Agent will queue the request and run another version check with the COCR rule when the current check is complete.
2. The Axon Agent uses PCRE regular expressions, which provide some advantages over the Java regular expressions used by the TE Agent. Because of this, a COCR rule authored on a TE Agent will function correctly on an Axon Agent. However, a rule authored on an Axon Agent may not work on a TE Agent.
3. The Axon Agent properly hashes files on Windows systems that have been 'exclusively locked'. Existing elements of this type that were created with a TE Agent will show a Modification when they are first checked using an Axon Agent.
4. The Axon Agent properly hashes files on Windows systems that have the 'Encrypt contents to secure data' option enabled. Existing elements of this type that were created with a TE Agent will show a Modification when they are first checked using an Axon Agent.
5. The Axon Agent properly hashes files that are under four bytes in size. Existing elements of this type that were created with a TE Agent will show a Modification when they are first checked using an Axon Agent.
6. When an Axon Agent uses a COCR in a baseline or version check and the content collected exceeds the **Maximum size of archived content** setting in the Settings Manager (under **Monitoring > File Systems**), the Agent will archive content **up to** the specified limit. TE Agents do not archive **any** content in this case. This difference in behavior will cause Modifications to existing elements created by a TE Agent with the same rule.
7. When an Axon Agent uses a COCR in a baseline or version check and the time required to collect content exceeds the **Timeout** value in the rule, the Agent will return content collected **up to** the timeout. TE Agents do not return **any** content in this case. This difference in behavior will cause Modifications to existing elements created by a TE Agent with the same rule.
8. The working directory differs between Axon Agents and TE Agents. If you used a relative path in a COCR rule for TE Agents, you will need to modify the rule to make it work correctly with Axon Agents.
9. Pay attention to the PATH environment variable with COCR rules. This variable may have a different value on Axon Agents and TE Agents.

Attributes & Content

The Axon Agent differentiates between files, junctions, and symbolic links on Windows file systems. The TE Agent reports all of these types as File in an element's Element Type attribute. Because the Axon Agent does not collect file attributes for junctions and symbolic links, existing elements of this type that were created with a TE Agent will show a Modification when they are first checked using an Axon Agent.

Log Manager Messages

The Axon Agent generates a message in the TE Console Log Manager when it initiates a baseline operation or version check, and when it completes the operation. Both messages include a time stamp specifying when the scan was initiated (for example, Scan initiated 7/24/15 10:36:28 AM). This time stamp can be used to match a completion log message with its initiation log message.

SACL/DACL Attributes

The Axon Agent will show the Inheritance flag as set on the SACL attribute for a file whose parent's SACL was deleted. Existing file elements with this attribute that were created with a TE Agent will show a Modification when they are first checked using an Axon Agent.

Forward Slashes in Windows Start Points

Forward slashes used in the start points of Windows file system rules will be replaced with backslashes in the resulting element generated by an Axon Agent. This will cause the Axon Agent to generate a different element from the TE Agent when it uses these rules.

Changing a Criteria Set on a Rule

Modifying the criteria set on a pre-existing rule will cause Modifications to existing elements created by that rule when they are scanned by an Axon Agent.

'Maximum Size of Archived Content' Setting

When an Axon Agent uses a file system rule that archives content and the content exceeds the **Maximum size of archived content** setting in the Settings Manager (under **Monitoring > File Systems**), the Agent will archive content up to the specified limit. TE Agents do not archive any content in this case. This difference in behavior will cause Modifications to existing elements created by TE Agent with the same rule.

Data Collection Errors

The Axon Agent will return an error when a requested attribute cannot be collected. In these situations the Agent will return as much requested data as possible. Any attributes that the Agent was not able to harvest will be missing. This difference in behavior will cause Modifications to existing elements created by TE Agents with the same rule.

Grouped Rules

If an Axon Agent attempts a baseline operation or version check using a group of rules, and one of the rules does not have any start points, the Agent will stop the operation and generate an error message identifying the rule(s) with missing start points. A TE Agent will simply ignore any rules in the group that do not have start points.

Differences in 'Baseline - New elements only' Behavior

If pre-existing elements from a file system or registry rule are deleted and the rule used to generate those elements is used again with the **Baseline - New elements only** option, the Axon Agent will not return any elements if no new elements are in scope. After deleting elements in the TE Console, we strongly recommend that the **Baseline - All elements** option is used instead.

RSOP Rules

1. On the Axon Agent, elements generated by Windows RSoP rules are limited by the **Maximum size of archived content** setting in the Settings Manager (under **Monitoring > File Systems**).
2. The Axon Agent gathers Event Log attributes in cases where the TE Agent was not able to gather this data.
3. The Axon Agent gathers additional settings that appear in the Security Options of the Local Security Policy if they have been configured through Group Policy.
4. The Axon Agent also gathers additional per-user audit policy security attributes. This can result in up to four `acl_` attributes: Audit Policy DACL, Audit Policy SACL, Global File SACL, and Global Key SACL.

File Encoding

Agents will attempt to determine the content encoding of a monitored file. If the encoding cannot be determined by inspecting the contents of the file, each Agent will report a different encoding. A TE Agent will use the default encoding of the JRE on the Agent system. The Axon Agent will not provide an encoding and the content may be saved in the wrong format by the TE Console.

Monitoring Linux Virtual Files

On Linux systems, virtual files in `/proc` are reported by the operating system as 0 bytes in size, but actually can contain a large amount of information. When an Axon Agent monitors a virtual file for content, the file's content will be recorded even if the size of that virtual file is reported as 0 bytes. This is a difference from the TE Agent, which will not record the file's content if the size of that file is reported as 0 bytes.

About Baselines

Baselining is the act of creating an element that reflects the current state of a monitored object. This element is known as the **current baseline**. If an object already has a baseline, you can update the object's current baseline at any time by running another baseline operation. When a node is re-baselined, TE saves the former baseline as an **historic baseline**.

In Tripwire Enterprise, a baseline operation may be run with the following methods:

- **Node Manager baseline operations** can only be run on a manual basis from the Node Manager.
- A **baseline rule task** is created in the Task Manager, and can be run on a manual or scheduled basis. For more information, see [How Does a Baseline Rule Task Work? on page 128](#).

With either method, you must specify the nodes and rules involved (see [Table 8](#)).

Table 8. Tripwire Enterprise objects used in a baseline operation

Tripwire Enterprise Object	Description
nodes	To identify the monitored systems to be baselined, at least one node must be selected. <ul style="list-style-type: none">• With a Node Manager baseline operation, you may select multiple nodes and/or node groups.• With a baseline rule task, you can only select a single node or node group.
rules	To indicate which monitored objects will be baselined, a single rule or rule group must be selected. For more information, see What are Rule Types? on page 79 . Note: Tripwire Enterprise creates a different element for each rule applied to a single monitored object. Therefore, multiple elements may represent the same monitored object. For example, if two baseline operations use two different rules to baseline the same configuration file on a router, Tripwire Enterprise creates two elements for the file.

About Version Checks

After you have created nodes and rules, you can run a **version check** to check monitored objects for changes. During a version check, Tripwire Enterprise compares the current state of a monitored object against the object's most recently recorded state to see if there are any changes.

- **If the monitored object has not been baselined** (that is, it doesn't have any element versions because TE hasn't checked the object with this rule), TE creates a baseline version for that object.
- **If TE detects a change to the monitored object**, it creates a new element version for the element, called a change version.
- **If the monitored object hasn't changed**, nothing happens.

You can initiate a version check in the following ways:

- **Node Manager version checks** are initiated from the Node Manager, and can only be run on a manual basis.
- A **check rule task** is created in the Task Manager, and may be run on a manual or scheduled basis. For more information, see [How Does a Check Rule Task Work? on page 129](#).

With either method, you must specify the Tripwire Enterprise objects to be used in the version check. [Table 9 below](#) lists each Tripwire Enterprise object involved in a version check.

Table 9. Tripwire Enterprise objects used in a version check

Tripwire Enterprise Object	Required?	Description
nodes	Yes	To identify the monitored systems to be version checked, at least one node or node group must be selected. <ul style="list-style-type: none">• With a Node Manager version check, you may select multiple nodes and/or node groups.• With a check rule task, you can only select a single node or node group. Note: Node Manager version checks can also be run on specific elements of TE Agent nodes. This functionality is not supported on Tripwire Axon Agents.
rules	Yes	To indicate which monitored objects will be checked for changes, a single rule or rule group must be selected. For more information, see What are Rule Types? on page 79 . Note: Tripwire Enterprise creates a different element for each rule applied to a single monitored object. Therefore, multiple elements may represent the same monitored object. For example, if two baseline operations use two different rules to baseline the same configuration file on a router, Tripwire Enterprise creates two elements for the file.

Tripwire Enterprise Object	Required?	Description
actions	No	<p>If desired, you can direct Tripwire Enterprise to respond to a change detected by a version check. To do so, you assign one or more actions to the version check (see What are Actions and Action Types? on page 116).</p> <ul style="list-style-type: none"> • With a Node Manager version check, actions can only be assigned to individual rules. • With a check rule task, actions can be assigned to individual rules and/or the task itself. <p>Note: Since restore and promote are opposite actions, only one of these action types may be associated with a single rule or rule task.</p>

Responding to Changes

Tripwire Enterprise provides a number of ways to evaluate and respond to detected changes.

To evaluate changes across your enterprise, TE includes a wide range of reports that you can customize to your specific needs. For more information, see [What are Reports and Report Types?](#) on page 172.

To evaluate changes to specific monitored objects, you can use the Node Manager's **Difference Viewer**. With the Difference Viewer, you can compare the attributes and contents (if available) of any pair of element versions.

- To assess a change reflected in a new change version, you may compare the version with the element's current baseline. For instructions, see [Comparing a Current Change Version with the Current Baseline](#) on page 388.
- To compare an element's current baseline with any previous version of the element, see [Comparing an Element Version with the Current Baseline](#) on page 389.
- To compare any two versions of the same element, see [Comparing Any Two Versions of the Same Element](#) on page 390.
- To compare a version of one element with a version of another element, see [Comparing Any Two Versions of Different Elements](#) on page 391. By comparing versions from different elements, you can investigate and assess common network anomalies, such as patterns in configuration errors.

<p>Note To use the Difference Viewer to evaluate changes on a node, a Change Audit license must be installed on that node. For more information, see About Tripwire Enterprise Licenses on page 202.</p>

If you configure actions for rules or tasks, the actions run automatically whenever TE detects a change using that rule or task. For more information on the actions available in TE, see [What are Actions and Action Types?](#) on page 116.

If TE detects a change that is approved, you can promote the change version in Tripwire Enterprise, making it the new baseline version. For more information, see [What is Promotion?](#) on the next page.

What is Promotion?

Promotion creates a new current baseline that is an exact copy of the most recent change version. You can promote element versions for a variety of reasons; for example, if you approve of the changes reflected in the latest change version of a file, you can promote the change version to the baseline.

Notes If the element version that is promoted is **not** the most recent change version, the promotion operation will **not** create a new baseline version from the historical version. Instead, the promoted version's **Approval ID** and **Comment** fields will be updated to reflect that it was promoted.

The term 'promotion' also refers to the act of designating the value in a failed policy test result as a valid value for future runs of the test. For more information, see [What is Policy Test Promotion?](#) on page 146.

In TE, you can manually promote a specific element version **or** all current change versions for a specified node or node group. For instructions, see:

- [Promoting a Specific Element Version](#) (on page 393)
- [Promoting All Current Versions for a Node or Node Group](#) (on page 395)

In addition, you can run a promote operation with a selection method. A **selection method** automates the process of determining which element versions are involved in a TE operation. For more information, see:

- [What is the By-Match Selection Method?](#) (on page 73)
- [What is the By-Reference Selection Method?](#) (on page 76)

To use a selection method in a manual promote operation, see:

- [Promoting by Match](#) (on page 396)
- [Promoting by Reference](#) (on page 397)

Note With a **promote action** or the default **Promote to Baseline Action**, Tripwire Enterprise runs a promote operation in response to a change detected by a version check. For more information, see [What are Actions and Action Types?](#) on page 116.

Tips You can limit promotions run on file server elements to specific software-installation packages. For more information, see [Promotion and Software-Installation Packages](#) below.

Before manually promoting element versions for a system that Tripwire Enterprise is monitoring in real time, Tripwire recommends that you first disable real-time monitoring for the node (see [Changing the Properties of a Node](#) on page 321).

If the **Allow promotion approval identifier** setting is enabled (see [Changing System Preferences](#) on page 266), users can enter an approval ID when they run a promote operation (for example, a change-request ticket number). If an approval ID is specified, Tripwire Enterprise saves the approval ID in each baseline version created by the operation **and** in each existing version of the element created since the last baseline version or version with an approval ID. To quickly identify authorized changes, you can search for versions that have specific approval IDs in the Version Search tab (see [Searching for Element Versions](#) on page 364).

Promotion and Software-Installation Packages

For an overview of how Tripwire Enterprise acquires and processes software-installation package data from file servers, see [What is Software-Installation Package Data? on the next page](#).

When you run a promote operation, you can specify one or more packages to limit the promotion to element versions that are **‘associated’** with those packages.

- TE considers an **element** to be associated with a package if the element’s name matches the full path of a package object saved in the TE Console database.
- TE considers an **element version** to be associated with a package if 1) its element is associated with the package, and 2) it has a unique identifier that matches the unique identifier of the corresponding package object in the TE Console database.

If you attempt to promote an element version and specify one or more packages, the promotion’s **Strict Package Match** setting determines if TE promotes the version.

- If this setting is **disabled**, TE will promote the version if its element is associated with one of the specified packages.
- If this setting is **enabled**, TE will only promote the version if the version itself is associated with one of the specified packages.

What is Software-Installation Package Data?

A **package object** is a file or directory in a software-installation package on a file server, and a **unique identifier** is a hash that identifies a package object. On a monitored system, each package includes an installation database that contains the full path and unique identifier for each file or directory installed by default with the package.

If you select the **Enable installation package association** check box in the Settings Manager (see [Setting File System Preferences on page 310](#)) and then baseline a monitored system, TE completes the following steps:

1. TE scans the system for installed packages.
2. From the installation database of each identified package, TE collects the full path and unique identifier of each related package object. TE then saves this information in the TE Console database.
3. TE baselines each package object identified by a file system rule or Windows registry rule. If a rule's criteria set has the **Package Data** attribute enabled, TE saves the object's unique identifier in the properties of the baseline version. If the Package Data attribute remains enabled, TE will save the unique identifier in the properties of each element version created for the package object in the future.

For further details about baselining, see [About Baselines on page 43](#).

How is Package Data used in Tripwire Enterprise?

In addition to promotions run in the Node Manager, package data from file servers may be referenced or used in a number of other TE features, including:

- **Promote actions.** If a promote action is run with a version check, you can limit resulting promotions to change versions with unique identifiers associated with specified packages (see [What are Actions and Action Types? on page 116](#)).
- **Package conditional actions.** If a package conditional action is run with a version check, the version's unique identifier may determine the action's response (see [How Does a Conditional Action Work? on page 125](#)).
- **Packages report criterion.** By specifying one or more packages in the Packages criterion of a report, you can limit report output to versions that have unique identifiers associated with the specified packages. For more information, see [What are Reports and Report Types? \(on page 172\)](#).

What is Restoration?

Restoration is the act of overwriting the content of a changed file on a network device with the content of the file's current baseline. In Tripwire Enterprise, files on some network devices can be restored with a **restore action** (see [How Does a Restore Action Work? on page 123](#)).

By using a restore action in a version check, you can automatically restore changed files detected by the check. With the Run Actions feature, you can manually restore changed elements displayed in the Node Manager.

- To restore a single file to its current baseline state, see [Restoring a Changed File with the Run Actions Feature on page 404](#).
- To restore all changed files on one or more monitored systems, see [Restoring Multiple Files with the Run Actions Feature on page 405](#).

Note Files on monitored file servers can only be restored with **execution actions** (see [How Does an Execution Action Work? on page 121](#)).

Files on directory servers, database servers, Nokia network devices, and HP ProCurve XL network devices cannot be restored. In addition, you cannot restore files in new network devices (or network device operating systems) that have been introduced since TE 5.5. In such cases, you should use an appropriate configuration tool to restore the device.

About Nodes

What are Node Types?

To monitor a physical or virtual system with Tripwire Enterprise, you must first create a node. A **node** is a Tripwire Enterprise object that represents a system on your network. A **monitored system** is a database, directory server, file server, network device, or virtual infrastructure (VI) system represented by a node.

- [Table 10 on the next page](#) defines the types of nodes that may be created in Tripwire Enterprise.

Note A directory server node or file server node can represent either a physical or virtual machine. Similarly, a database node can represent a database hosted by a physical or virtual machine. For an introduction to virtual machines, see [Monitoring Virtual Systems with Tripwire Enterprise on page 59](#).

- For a current list of databases, directory services, file server platforms, network devices, and virtual infrastructure platforms that can be monitored by Tripwire Enterprise, visit the Tripwire Web site:

[https://www.tripwire.com/products/tripwire-enterprise/
tripwire-enterprise-platform-and-device-support-register](https://www.tripwire.com/products/tripwire-enterprise/tripwire-enterprise-platform-and-device-support-register)

- To learn how nodes are created, see [How are Nodes Created? on page 54](#).

Table 10. Types of nodes

Type	Description
<p>database</p>	<p>A database server is a physical server or virtual machine configured to host a database application in a client/server environment. A database node represents a single database on a database server. In Tripwire Enterprise, you may create the following types of database nodes:</p> <ul style="list-style-type: none"> • A DB2 database node represents a DB2 database. • A Microsoft SQL Server database node represents a Microsoft SQL Server database. • An Oracle database node represents an Oracle database. • A PostgreSQL database node represents a PostgreSQL database. <p>For more information about databases, see:</p> <ul style="list-style-type: none"> • How Does a Database Metadata Rule Work? (on page 89) • How Does a Database Query Rule Work? (on page 92)
<p>directory server</p>	<p>A directory is a centrally managed information store that enables users to search for data saved in a variety of locations on a network. A directory server is a physical server or virtual machine that hosts a directory, and a directory protocol is a communication standard used to access information with a directory.</p> <p>A directory server node represents a directory server. In Tripwire Enterprise, you may create the following types of directory server nodes:</p> <ul style="list-style-type: none"> • An LDAP directory node represents any directory server that uses LDAP as the directory protocol. LDAP (Lightweight Directory Access Protocol) is a standard, vendor-independent directory protocol. • An Active Directory node represents a Windows system that supports Active Directory, an LDAP-compliant Microsoft directory included with some Windows platforms. <p>For more information about directories, see How Does a Directory Rule Work? on page 93.</p>
<p>file server</p>	<p>A file system, or file management system, is software used to organize and store files on a computer. A file server is a physical server or virtual machine that hosts a file system. A file server node represents a file server running a Windows, UNIX, or Linux operating system.</p> <p>Note: For an introduction to virtual machines, see Monitoring Virtual Systems with Tripwire Enterprise on page 59.</p>
<p>network device</p>	<p>A network device node is a node that represents a physical router, switch, firewall, load balancer, or UNIX system.</p> <p>Notes: VMware ESX is a hypervisor created by VMware, Inc. The VMware ESX 'network device' node represents a physical server on which VMware ESX is installed. For more information about hypervisors, see Monitoring Virtual Systems with Tripwire Enterprise on page 59.</p> <p>A UNIX system is any system running a POSIX-compliant, UNIX-based operating system.</p> <p>If Tripwire Enterprise does not include a node type for a network device you wish to monitor, you can create a custom node type in the Settings Manager (see Working with Custom Node Types on page 299).</p>

Type	Description
virtual infrastructure	<p>For an introduction to virtual infrastructure (VI) terms and concepts, see Monitoring Virtual Systems with Tripwire Enterprise on page 59.</p> <p>A VI node represents a VI or a component of a VI. With the following types of VI nodes, you can monitor the configuration files and parameters of a VI:</p> <ul style="list-style-type: none"> • A VI management node represents an entire VI defined by a single installation of VI management software. As a 'container' object similar to a group (see About Groups on page 29), a VI management node contains node groups and other nodes that represent specific components of the VI. • A VI hypervisor node represents a hypervisor installed on a VI host machine. • A virtual machine template node represents a template in VI management software used to create virtual machines. • A virtual machine node represents a virtual machine. • A virtual switch node represents a virtual switch. • A distributed virtual switch node represents a distributed virtual switch. <p>To learn more about the creation of VI nodes, see Monitoring Virtual Systems with Tripwire Enterprise on page 59.</p> <p>Notes: The hierarchy of nodes and node groups descended from a VI management node can not be directly modified in the Node Manager. For example, you cannot move a VI node descended from a VI management node, link an external node to a group under a VI management node, or create a new node or node group under a VI management node.</p> <p>To monitor a database, directory, or file system hosted by a virtual machine, you must create a database, directory server, or file server node (see How are Nodes Created? on the next page).</p>

How are Nodes Created?

Tripwire Enterprise supports two methods for the creation of a node:

- To create a **file server node**, you install Tripwire Enterprise Agent or Tripwire Axon Agent software on a file server. For more information, see [Creating a Node by Installing Agent Software \(below\)](#).
- To create any other type of node, you complete the New Node Wizard in the Node Manager. For further details, see [Creating a Node Manually \(on page 56\)](#).

To enable Tripwire Enterprise features for a node, you must apply a license to the node. For more information on the functionality available with each type of license, see [About Tripwire Enterprise Licenses on page 202](#).

Creating a Node by Installing Agent Software

To create a file server node, you install one of the following types of **Agent software** on the system to be monitored:

- **Tripwire Enterprise Agent (TE Agent)** is a remote-execution environment that enables TE Console to monitor a file server.
- **Tripwire Axon Agent (Axon Agent)** is Tripwire's new generation of agent technology, and does not require Java to be installed on the monitored system.

Only one type of Agent software can be installed on a system to be monitored. Both types of Agent software perform a similar function, monitoring the files and directories on a file server (referred to as an **Agent system**). If a change is detected, the Agent software reports the change to the TE Console. By performing some operations locally, the TE Agent and Axon Agent software minimize the network traffic generated by a Tripwire Enterprise implementation.

Note The Axon Agent utilizes significantly less network bandwidth by virtue of its messaging and compression methods.

In general, nodes with Axon Agent installed behave like those with TE Agent installed. Differences in behavior and performance between the two types of nodes are described in [Differences Between Axon Agent and Tripwire Enterprise Agent on the next page](#).

When Agent software is installed and started, it immediately notifies the TE Console of its availability. If the TE Console has a valid license, it automatically creates a node for the Agent's host system in the Discovered node group. If smart node groups are enabled, nodes added to the Discovered group are automatically moved and linked to one or more smart node groups, depending on the characteristics of the monitored system and any tags that are automatically applied to it. For more information, see [About Node Groups and Smart Node Groups on page 57](#).

For TE Agent installation instructions, see *Installing Tripwire Enterprise Agent* in the *Tripwire Enterprise Installation & Maintenance Guide*. For Axon Agent installation instructions, see *Installing Tripwire Axon Agent* in the *Tripwire Enterprise Installation & Maintenance Guide*.

Differences Between Axon Agent and Tripwire Enterprise Agent

- Compared with TE Agent, the Axon Agent demonstrates greatly improved performance and lower resource utilization on monitored systems.
- Axon Agent is implemented using C++, so Java is not required on monitored systems.
- The Axon Agent is much more resilient than the TE Agent, and is able to self-heal from many errors that would require manual intervention on a TE Agent.
- Version 8.5.0 or later of TE Console must be installed for use with Axon Agents. Earlier versions of TE Console are not supported.
- Axon Agents cannot be used as the delegated Agent used to support monitoring of a database, directory server, or virtual infrastructure node.
- Rules cannot be authored on a TE Console by browsing the file system or Windows registry on nodes where Axon Agent is installed. As a workaround, create rules by browsing on a similar system that has TE Agent installed, and then use those rules on the system with Axon Agent installed.
- Axon Agents do not cause tasks to “time out” in the same way that TE Agents do. Axon Agent nodes that do not complete a check are assigned the Task Timeout tag in the Asset View tab and logged with a Task Stop error in the Log Manager, but they do not cause the associated task to have a status of “Timed Out”.
- Axon Agents do not support running version checks on specific elements. Instead, the whole rule used to monitor the element should be re-run.
- The Axon Agent cannot use log transfer rules, which provide one way to integrate Tripwire Enterprise and Tripwire Log Center.
- Automated Remediation using remediation scripts is not supported on Axon Agents.
- Execution actions can be used with Axon Agents, but the %f variable (which generates a Detailed Changes Report) is not supported on the Axon Agent.
- The Axon Agent is not automatically installed with TE Console. Instead, a TE Agent is installed. The TE Console software can only be upgraded if TE Agent is installed on the TE Console system. For this reason, Tripwire strongly recommends that you **not** replace TE Agent on the system where TE Console is installed.
- Custom functionality that leverages JAR downloading capabilities provided by the TE Agent is not supported on Axon Agents. For information on compatibility with custom implementations, please contact Tripwire Professional Services.

When existing TE Agent nodes are upgraded to Axon Agent, the element data history collected by TE Agent will be preserved and can still be viewed after Axon Agent is installed. However, there may be slight differences in how element data is collected. For more information, see [Element Differences Between TE Agent and the Axon Agent on page 40](#).

Creating a Node Manually

To create a database node, directory server node, network device node (including custom nodes), or VI management node, you complete the New Node Wizard in the Node Manager. In the wizard, you enter information that enables your Tripwire Enterprise Server to communicate with the monitored system. These **node properties** may include:

- An IP address or resolvable hostname for the monitored system
- A communication protocol
- Valid login credentials (username and password) with which TE can access the system

When you create a database node, directory server node, or VI management node, you also specify a delegated Agent for the node. A **delegated Agent** is a system with Tripwire Enterprise Agent software installed that processes some Tripwire Enterprise functions for the node. For more information, see [Creating a Node by Installing Agent Software on page 54](#).

Note Only nodes with Tripwire Enterprise Agent installed can be a delegated Agent for a database, directory server, or VI management node. Tripwire strongly recommends that you install TE Agent on these nodes and use that Agent both to monitor that system's file system, and as the delegated Agent for the database, directory server, or VI management system itself.

Nodes with Axon Agent installed cannot be used as a delegated Agent.

VI management nodes are the only type of VI node that can be created directly with the New Node Wizard. Tripwire Enterprise creates all other VI node types as part of the **VI node discovery** process, which TE automatically initiates when a VI management node is created. For further details, see [Monitoring Virtual Systems with Tripwire Enterprise on page 59](#).

To create a node with the New Node Wizard, see:

- [Creating a Database Node \(on page 370\)](#)
- [Creating a Directory Server Node \(on page 369\)](#)
- [Creating a Network Device Node \(on page 374\)](#)
- [Creating a VI Management Node \(on page 375\)](#)

Tip To create a custom node, you must first create a **custom node type** in the Settings Manager (see [Working with Custom Node Types on page 299](#)).

About Node Groups and Smart Node Groups

Like the other Managers in Tripwire Enterprise, the Node Manager uses groups for organization. The Node Manager has all of the default groups described in [About Groups on page 29](#), and also a number of special groups which are listed in [Table 11 \(on the next page\)](#).

In addition to standard groups, the Node Manager also uses **smart node groups** to organize nodes. Each smart node group corresponds to a tag set or saved filter in the Asset View tab of the Node Manager. For more information on these objects, see [Getting Started with Tags on page 339](#). When you add a new node to TE, the software automatically links the node into one or more smart node groups, depending on the characteristics of the monitored system and any tags that are automatically applied to it.

Tip To learn about best practices for using tags and smart node groups, see [Tagging Best Practices on page 342](#).

Note Smart node groups are enabled by default in new installations of Tripwire Enterprise. If your Tripwire Enterprise installation was upgraded from an earlier version, click **Smart Node Groups: disabled** at the bottom of the Node Manager to enable them.

You can also enable smart node groups in the System Preferences section of the Settings Manager. For more information, see [Changing System Preferences on page 266](#).

Like standard node group, smart node groups can be used to scope version checks, reports, and other operations. However, smart node groups differ from standard node groups in several important ways:

- you can only create, delete, or rename a smart node group by manipulating the corresponding tag sets or saved filters in the Asset View tab
- you can only link a node to or unlink a node from a smart node group by changing the tags associated with the node, or by changing the saved filter in the Asset View tab
- you can't create a standard node group anywhere in the smart node group hierarchy
- you can't move a smart node group or move nodes into a smart node group
- you can't link a smart node group to, or unlink it from, any other group
- you can't import smart node groups with standard node groups. For more information, see [Importing Nodes and Node Groups on page 407](#).

For more information on working with the objects in smart node groups, see [Using the Asset View Tab on page 346](#).

Table 11. Node Manager groups

Node Manager Group	Description
Automatically Linked	<p>If Tripwire Enterprise Agent is installed on a file server hosted by a virtual machine, and the Tripwire Enterprise Server has a valid Change Audit license, Tripwire Enterprise creates a new file server node.</p> <ul style="list-style-type: none"> • If the Node Manager contains a VI management node with a virtual machine node that has the same IP address as the new file server node, TE creates the new node in the Automatically Linked Group. • Otherwise, TE creates the new node in the Discovered node group. <p>Note: When TE creates a new file server node in the Automatically Linked Group, it also replaces the corresponding virtual machine (VM) node with a new node group bearing the name of the VM node. TE then moves the VM node under the new group, and links the new file server node to the group. As a result, the new group contains two nodes for the virtual machine: the VM node and the new file server node.</p>
Discovered	<p>Tripwire Enterprise creates a new file server node in the Discovered node group when Tripwire Enterprise Agent or Axon Agent is installed on a file server. To monitor the file server with TE, the node should be moved from the Discovered node group to the Root Node Group. For instructions, see Moving Nodes and Node Groups on page 379.</p> <p>If smart node groups are enabled, nodes added to the Discovered group are automatically moved and linked to one or more smart node groups, depending on the characteristics of the monitored system and any tags that are automatically applied to it.</p> <p>Note: Tripwire Enterprise Console includes an embedded Tripwire Enterprise Agent. Therefore, when you first install TE Console software, a node for the Tripwire Enterprise Server is added to the Discovered node group.</p>
Smart Node Groups	<p>This node group is created automatically if smart node groups are enabled. This group always contains the Operational Tag Sets, Saved Filters, System Tag Sets, and Tag Sets sub-groups. For more information about these types of objects, see Getting Started with Tags on page 339.</p> <p>Note: When you add a new node to TE, the node is automatically linked into one or more of these groups, depending on the tags associated with it.</p>

Monitoring Virtual Systems with Tripwire Enterprise

Virtualization is a software technology that enables multiple operating systems to share the physical resources of a single computer at the same time. By running multiple operating systems on the same hardware, virtualization consolidates IT resources on fewer machines.

A **hypervisor** (e.g. VMware ESXi) is virtualization software that manages the physical resources of a single computer — for instance, the computer’s hard disk, random access memory (RAM), and central processing unit (CPU). A **virtual infrastructure (VI) host machine** is a computer on which virtualization software (such as a hypervisor) has been installed, and a **virtual system** is a simulated computer or switch created by a hypervisor.

A **virtual infrastructure (VI)** is an IT environment containing one or more virtual systems. A VI consists of both physical and virtual components, including virtual systems, VI host machines, network hardware, hypervisors, and other virtualization software.

VI node discovery is an automated process in which Tripwire Enterprise creates nodes and node groups that represent the virtual objects defined in VI management software. VI node discovery involves the following steps.

1. In the Node Manager, you complete the New Node Wizard for a VI management node (e.g. a vCenter node; see [Creating a VI Management Node on page 375](#)).
2. When you click **Finish** in the New Node Wizard, Tripwire Enterprise queries the specified installation of VI management software to identify the properties of each of the software’s virtual objects. The query also determines the hierarchy of virtual objects defined by the software.
3. In the Node Manager, TE creates the VI management node. Under the VI management node, TE creates a node or node group for each virtual object identified by the query. The hierarchy of Node Manager objects mirrors the hierarchy defined by the VI management software.

Once a VI management node has been created, you can **synchronize** the node’s contents with the VI management software at any time. When a VI management node is synchronized, Tripwire Enterprise updates the node’s descendant objects in the Node Manager to reflect the current contents and hierarchy of the VI management software. For example, if a user creates a new virtual machine in the VI management software, synchronization will create a corresponding virtual machine node under the VI management node.

- To synchronize a VI management node manually, click the **Synchronize** button in the node’s properties dialog (see [Changing the Properties of a Node on page 321](#)).
- To schedule synchronization, configure the Synchronization tab in the node’s properties dialog (see [Changing the Properties of a Node on page 321](#)).

Note If you install TE Agent on a new virtual machine for which a node has yet to be created via discovery or synchronization, TE creates a new Agent node in the Node Manager’s Discovered node group. When the next synchronization identifies the virtual machine, TE moves the Agent node to the appropriate location in the hierarchy of the associated VI management node.

Discovering and Synchronizing a VMware Virtual Infrastructure

vSphere is a VI platform developed by VMware, Inc. With vSphere Client, this platform's VI management console, administrators can manage the physical and virtual components of their virtual infrastructure. In vSphere Client, **inventory views** provide administrators with alternative perspectives on their inventory objects. An **inventory object** is any system or object in an inventory view; for instance, a virtual machine, cluster, or datacenter.

Inventory views include:

- **Hosts & Clusters**
- **Virtual Machines & Templates**
- **Networking**
- **Datastores**

[Table 12 \(on page 62\)](#) indicates which inventory object types appear in each inventory view.

In Tripwire Enterprise, a **VMware vCenter node** is a VI management node that can either represent a vCenter or a VirtualCenter. When you complete the New Node Wizard for a VMware vCenter node, TE 'discovers' the specified vCenter/VirtualCenter and creates the vCenter node in the Node Manager. Directly beneath the new vCenter node, TE creates a node group for each inventory view of the vCenter/VirtualCenter.

As shown in [Figure 7 on the next page](#), the hierarchy of objects in these node groups matches the object hierarchy in the inventory views of vSphere Client. For example, the **Hosts & Clusters node group** contains nodes and node groups that represent the inventory objects in the Hosts & Clusters inventory view, while the **VMs & Templates node group** presents the contents of the VMs & Templates view.

Note All objects in vCenter must have **Full Access** rights in order for TE to synchronize with vCenter. Any object in vCenter with limited rights such as **No Access** will cause the synchronization process to fail.

For each type of inventory object, [Table 12 \(on page 62\)](#) indicates the type of Node Manager object created by the VI node discovery process. In addition, the VI node discovery process creates:

- **Host groups.** A host group consists of nodes that represent the components of a single VI host machine. At minimum, a host group contains a VI hypervisor node.
- **Template node groups.** In the Hosts & Clusters node group, TE automatically adds a 'Templates' node group to each datacenter node group. This group contains all virtual machine template nodes for a datacenter.
- **A Deleted Nodes group.** If the vCenter node contains an inventory object that is subsequently deleted from vCenter/VirtualCenter, TE moves the object's node to the Deleted Nodes group.

Once a VMware vCenter node has been created in the Node Manager, Tripwire Enterprise can synchronize the node with any future changes made in the vCenter/VirtualCenter. If TE synchronizes the node and detects any of the following changes, TE automatically makes corresponding changes to the nodes and node groups under the VMware vCenter node:

- A change in the properties of an inventory object
- A change in the hierarchy of inventory objects in an inventory view

Figure 7. A VMware vCenter node in the Node Manager

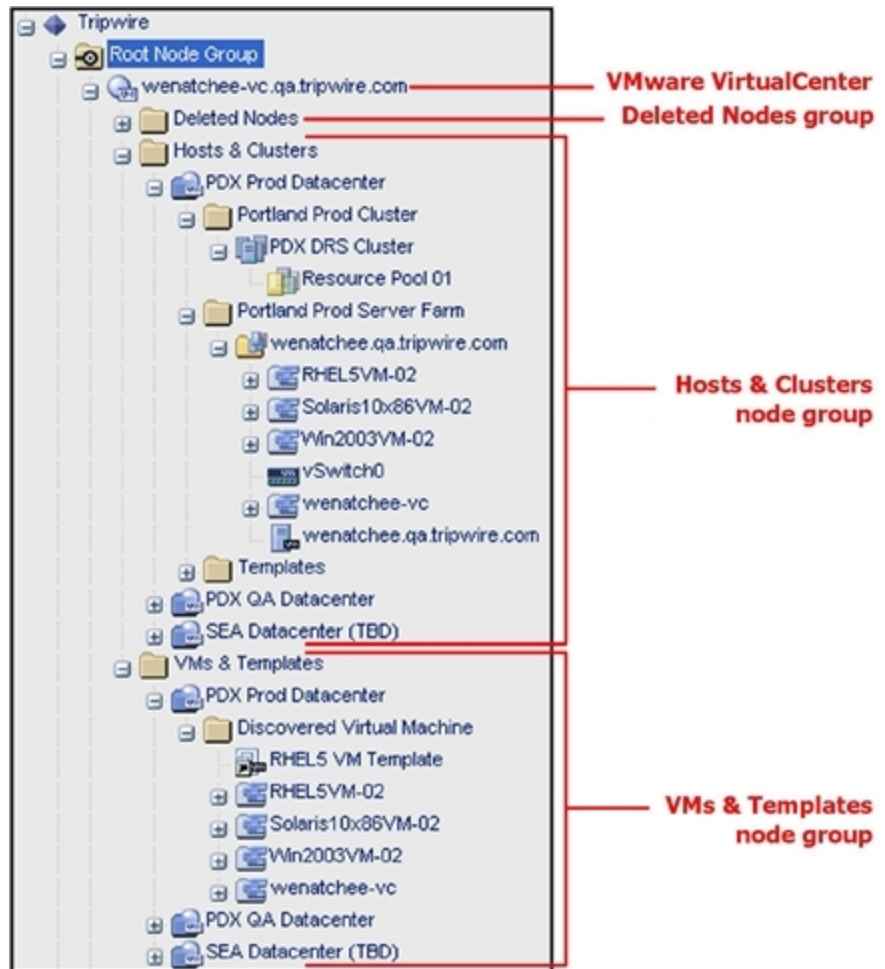


Table 12. Inventory objects and equivalent TE objects

Inventory Object	Displayed in Hosts & Clusters View?	Displayed in Virtual Machines & Templates View?	Displayed in Networking View?	Displayed in Datastores View?	In TE, this inventory object is represented by ...
Clusters	Yes	No	No	No	... a static node group ^A
Datacenters	Yes	Yes	No	Yes	... a static node group ^A
Datastores	No	No	No	Yes	... a node group
Distributed virtual port groups	No	No	Yes	No	... an element of a distributed virtual switch
Distributed virtual switches	No	No	Yes	No	... a node
Folders	Yes	Yes	Yes	Yes	... a node group
Host machines	Yes	No	Yes	Yes	... a node
Networks	No	No	Yes	No	... a node group
Resource pools	Yes	No	No	No	... a static node ^A
Virtual applications	Yes	Yes	No	No	... a node group
Virtual machine templates	No	Yes	Yes	Yes	... a node
Virtual machines	Yes	Yes	Yes	Yes	... a node ^B
Virtual switches	Yes	No	No	No	... a node

A A static node or node group is a Node Manager object for which a properties dialog cannot be opened by selecting the object in the main pane of the Node Manager.

B If a TE Agent has been installed on a virtual machine, Tripwire Enterprise creates a node group that contains both the Agent node and virtual machine node.

About Audit Events and Real-Time Monitoring

What is Audit Event Collection?

Tripwire Enterprise can collect audit events from the types of monitored systems identified in [Table 13 below](#). Audit events provide valuable information about what caused a change and specifically who made that change.

If audit event collection is enabled for a node, and a baseline operation or version check is run on the monitored system, Tripwire Enterprise harvests audit events from one of the sources identified in that table.

Table 13. Audit event sources for monitored systems

Monitored System	TE Agent audit event sources	Axon Agent audit event sources
UNIX file server	Audit log or TE Event Generator	TE Event Generator
Windows file server	Security event log or TE Event Generator	TE Event Generator
Database server	Database audit log	N/A - Axon Agents can't be used to monitor database nodes
Active Directory server	Security event log	N/A - Axon Agents can't be used to monitor Active Directory nodes

If a TE Event Generator is installed on a system with TE Agent or Axon Agent, audit event collection is enabled automatically for that node and the TE Event Generator is used as the source for audit events. To manually enable audit event collection on a node, see [Manually Configuring Audit Event Collection on the next page](#).

If a version check creates a new version of an element for which one or more audit events indicate a change:

- TE creates a log message for each of the audit events (Category = Audit Event), and
- In the properties of the version, TE saves links to the associated log messages.

Notes

Axon Agent nodes only collect audit events from rules that are part of an enabled task. Audit events associated with these rules will be collected whether the task runs on a schedule, or is run manually.

TE Agents collect audit events for rules that are part of tasks and rules that are run manually, even if the rules are not part of a task.

To collect audit events on a node, a Change Audit license must be installed on that node. For more information on the functionality available with each type of license, see [About Tripwire Enterprise Licenses on page 202](#).

Manually Configuring Audit Event Collection

Notes To configure audit event settings for **directory** nodes, see [Setting Active Directory Preferences on page 311](#) and [Setting LDAP Directory Preferences on page 311](#).

To configure audit event collection for **multiple** Agent systems at the same time, see [Configuring Audit Event Collection and Real-Time Monitoring for Multiple Systems on page 422](#).

To manually enable audit event collection on Agent or database nodes:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the node group containing the node.
3. In the main pane, select the node in the **Name** column.
4. Click the node's **Events** tab.

Notes This tab does not contain any options for Axon Agent nodes that do not have a TE Event Generator installed.

Audit event collection is not supported on PostgreSQL database nodes.

5. Select **Collect audit-event information** and select the **Event source** for audit events.

Notes Axon Agents only support the TE Event Generator as an **Event source**, and Tripwire recommends that the Event Generator is used to collect audit events on all systems that support it, due to its greater accuracy and lower impact on the monitored system.

To collect information from a native operating-system audit log, logging must be enabled on the monitored system.

6. Click **OK**.

When you enable audit-event collection on a node, the node starts to collect audit events for a rule the first time that rule is used in a baseline operation or version check on the system.

Tips Remember that Axon Agents only collect audit events from rules that are part of an enabled task, whether the task runs manually or automatically.

The Configure Axon Agents task pushes any updates to audit event and RTM configurations out to all Axon Agent nodes. This task runs daily at midnight by default, so any changes to audit event and RTM configurations on Axon Agent nodes will take effect at that time. **You should also run this task manually any time you make changes to rules or any components of rules (start and stop points, global variables, etc) that are used for audit event collection or real-time monitoring.** For a complete list, see [Activities that May Change Audit Event or RTM Configurations on Axon Agents on the next page](#).

Activities that May Change Audit Event or RTM Configurations on Axon Agents

Any of the activities below may change the rules that Agents use for audit event collection or real-time monitoring. To ensure that Axon Agents have the latest configuration, manually run the Configure Axon Agents task after making any of these changes. For more information, see [Running Tasks and Task Groups Manually on page 523](#). This task also runs daily at midnight by default.

The TE Console status bar displays the last time that the Configure Axon Agents task ran (either manually or as a scheduled task).

Rules

- Delete
- Move
- Link/unlink
- Modify name
- Modify realtime setting
- Add/delete start points

Start points/stop points

- Modify

Criteria sets

- Add/delete attributes

Nodes

- Move
- Link/unlink
- Add/modify/delete local variables

Tasks

- Create
- Delete
- Modify

Global variables

- Create
- Modify

Settings Manager settings

- Monitoring > File Systems > "Maximum size of archived content" setting

How Does an Event Generator Collect Audit Events?

A **TE Event Generator** is an auditing utility that can be installed with Tripwire Enterprise Agent or Axon Agent on some Windows and UNIX file servers. For system requirements and installation instructions, see the following sections in the *Tripwire Enterprise Installation & Maintenance Guide*:

- *Requirements for a Tripwire Enterprise Agent System*
- *Installing and Configuring Axon Agent*
- *Managing the Event Generator Service*

If a TE Event Generator is installed on a system with TE Agent or Axon Agent, audit event collection (but not real-time monitoring) is enabled automatically for that node and the Event Generator is used as the source for audit events. For information on manually configuring audit event collection, see [What is Audit Event Collection? on page 63](#).

Once configured, TE collects audit events from the Agent system as follows:

1. The Event Generator monitors the Agent's operating system (and registry, if the Agent is a Windows server). If the Event Generator detects an event involving a monitored object identified by a file system rule or Windows registry rule that has been used to baseline the Agent, it creates an audit event. For descriptions of the types of audit events created by Event Generators on supported Agent systems, refer to the following tables:
 - For Windows systems, see [Table 14 on page 68](#).
 - For UNIX systems, see [Table 15 on page 69](#).

The Event Generator does not create audit events for the following OS events:

- A change in the **Access** attribute of a file or directory. (The Access attribute indicates the last time a file or directory was accessed by a user.)
- Any OS event in a mounted Windows file system.

To audit objects in the HKEY_CURRENT_USER hive of an Agent's registry, the Event Generator must run as the same user as the Agent.

2. The **coalescence period** determines how frequently the Event Generator sends collected audit events to the Agent. When the coalescence period expires, all audit events are transferred from the Event Generator to the Agent. If multiple events involve changes made to the same monitored object by the same user, and those changes occur within the same coalescence period, the Event Generator only creates a single audit event to reflect the changes.

Note To change the coalescence period, see Changing the Coalescence Period for an Event Generator on the next page .

3. The Agent accumulates audit events until the next baseline operation or version check. At that time, the Agent sends the collected audit events to TE Console.

Restarting an Event Generator

To restart an Event Generator, see *Managing the Event Generator Service* in the *Tripwire Enterprise Installation & Maintenance Guide*.

When an Event Generator is restarted on an Agent system, Tripwire Enterprise:

- creates an Error message in the Log Manager indicating that the EG went down
- overlays the Agent's icon with an error emblem in the Node Manager

In addition, the Event Generator stops collecting audit events. To resume audit event collection on a TE Agent, you must restart and refresh the Event Generator's Agent (see [Restarting Tripwire Enterprise Agents on page 412](#)). Axon Agents automatically recover when an Event Generator restarts, and do not need to be manually restarted.

Changing the Coalescence Period for an Event Generator

The duration of the coalescence period on an Agent is defined by a property in the Agent's configuration file. The value of this property is 30000ms (30 seconds) by default.

On TE Agents, the coalescence period is defined (in milliseconds) by the Event Generator Transfer Interval property in a TE Agent's configuration file. To change this setting, see [Changing TE Agent Configuration Properties on page 417](#).

On Axon Agents, the coalescence period is defined (in milliseconds) by the `tesvc.coalesce.interval` property in the Axon Agent's `twfim.conf` file.

To change this setting on Axon Agents:

1. Open one of the following files on the Axon Agent system:

Linux: `/etc/tripwire/twfim.conf`

Windows: `%PROGRAMDATA%\Tripwire\agent\config\twfim.conf`

If the file doesn't already exist, create a new text file in that location.

2. Add or edit the following line in the file:

```
tesvc.coalesce.interval=<value_in_milliseconds>
```

3. Save the file, then restart the Axon Agent service:

Linux:

```
/sbin/service tripwire-axon-agent stop
/sbin/service tripwire-axon-agent start
(/usr/sbin/service on Debain or Ubuntu systems)
```

Windows:

```
net stop TripwireAxonAgent
net start TripwireAxonAgent
```

Table 14. Types of audit events created by Event Generators on supported Windows systems

Type	Applies to ...	This type of audit event indicates ...
Create	... file systems	... the creation of a file or directory.
Create Key	... Windows registries	... the creation of a registry key or entry.
Create Stream	... file systems	... the creation of an alternate data stream on a file or directory.
Delete	... file systems	... the deletion of a file or directory.
Delete Key	... Windows registries	... the deletion of a registry key or entry.
Delete Stream	... file systems	... the deletion of an alternate data stream on a file or directory.
Delete Value	... Windows registries	... the deletion of a value in a registry entry.
Rename From or Rename To	... file systems	... a change in the name of a file or directory.
Set Info	... file systems	... a change in any of the following attributes for a file or directory: Write, Create, Archive, Offline, Temp, Hidden, System, Compressed, and Read-Only. For attribute descriptions, see Table 77 on page 302 .
Set Key	... Windows registries	... a change in the write time attribute for a registry key. For attribute descriptions, see Table 78 on page 304 .
Set Key Security	... Windows registries	... a change in any of the following attributes for a registry key: DACL, SACL, Owner, and Group. For attribute descriptions, see Table 78 on page 304 .
Set Security	... file systems	... a change in any of the following attributes for a file or directory: DACL, SACL, Owner, and Group. For attribute descriptions, see Table 77 on page 302 .
Write	... file systems	... a change in the content of a file.
Write Stream	... file systems	... a change in the content of an alternate data stream on a file or directory.
Write Value	... Windows registries	... a change in a value of a registry entry.

Table 15. Types of audit events created by Event Generators on supported UNIX systems

Type	Applies to ...	This type of audit event indicates ...
Chgrp	... file systems	... a change of the user group that owns a file.
Chmod	... file systems	... a change in the access mode of a file.
Chown	... file systems	... a change in the owner of a file.
Create	... file systems	... the creation of a file.
Link	... file systems	... the creation of a link to a file.
Mount or Umount	... file systems	... that file has been attached or removed to/from an existing directory.
Rename From or Rename To	... file systems	... a change in the name of a file.
Truncate	... file systems	... a shortening of a file's length.
Utime	... file systems	... a change in the Last Modified time for a file or directory.
Write	... file systems	... a change in the content of a file.
Xattr	... file systems	... a change in the attributes of a file.
Unlink	... file systems	... the deletion of a file.

How Does Real-Time Monitoring Work?

If a TE Event Generator is installed on an Agent system, Tripwire Enterprise can monitor the system for changes made in real time. With **real-time monitoring (RTM)**, the Agent continuously reports any detected changes to TE Console. For an introduction to the TE Event Generator, see [How Does an Event Generator Collect Audit Events? on page 66](#).

To enable real-time monitoring on an Agent system, see [Enabling Real-Time Monitoring on an Agent System on the next page](#)

Note To use real-time monitoring on a node, a Change Audit license must be installed on that node. For more information on the functionality available with each type of license, see [About Tripwire Enterprise Licenses on page 202](#).

Tripwire Enterprise uses the following process to monitor an Agent system in real time:

1. As described in [How Does an Event Generator Collect Audit Events? \(on page 66\)](#), the Event Generator monitors the Agent and creates audit events. At the end of each coalescence period, the Event Generator sends all new audit events to the Agent.
2. At a regular interval, the Agent automatically runs a version check of the monitored objects for which the current collection of audit events indicates a change(s).

Notes On TE Agents, the length of the interval between version checks is defined by the **Real Time Monitoring (RTM) Interval** property in the TE Agent's configuration file. For more information, see [Tripwire Enterprise Agent Configuration Properties](#) in the [Tripwire Enterprise Reference Guide](#).

In a single interval, the TE Agent creates a single change version for each changed object, even if the collected audit events indicate that multiple changes were made to the object.

3. At the end of the version check, the Agent automatically forwards the audit events and all new change versions to the TE Console.

Tips Use Asset View to track errors associated with real-time monitoring. Systems with RTM errors will be tagged with the Health:Event Generator Errors tag. For more information, see [Monitoring the Health of Nodes and Resolving Errors on page 317](#).

If you restart a system that is being monitored in real-time by TE, you should run a manual version check of the Agent node with all applicable RTM-enabled rules.

The **Real-Time Action Interval** determines the frequency with which actions are run in response to change versions created by RTM-enabled rules. At the end of this interval, TE runs all actions associated with the rules used to create change versions within that period of time. However, if TE creates a 2nd change version for the same monitored object in the same interval, TE will automatically run the associated actions and reset the interval timer. In this case, the 2nd change version is assigned to the new interval.

Enabling Real-Time Monitoring on an Agent System

Note With the Events button in the Node Manager, you can configure real-time monitoring for multiple Agent systems at the same time (see [Configuring Audit Event Collection and Real-Time Monitoring for Multiple Systems](#) on page 422).

To enable real-time monitoring on an Agent system:

1. Open the properties dialog for the Agent node (see [Changing the Properties of a Node](#) on page 321). In the **Events** tab:
 - a. If not already selected, select **Collect audit-event information** and select **TE Event Generator** as the **Event source**.
 - b. Select **Enable real-time monitoring**.
 - c. Click **OK**.

Note This tab does not contain any options for Axon Agent nodes that do not have a TE Event Generator installed.

2. To monitor the Agent system in real time, create new RTM-enabled rules and/or enable existing rules for RTM.
 - To create a new rule, see [Creating a File System Rule](#) (on page 455) or [Creating a Windows Registry Rule](#) (on page 457). Make sure that **Enable real-time monitoring** is selected when creating rules.
 - To enable RTM for an existing rule, configure the settings in the rule's **Real-Time** tab (see [Changing the Properties of a Rule](#) on page 437).
3. Run a version check using all of the rules you added or modified in step 2 on all of the TE Agent and Axon Agent nodes that you want to monitor in real time. For details, see [Version Checking Monitored Systems](#) on page 385.
4. **For Axon Agents only**, manually run the Configure Axon Agents task. For details, see [Running Tasks and Task Groups Manually](#) on page 523.

The Configure Axon Agents task pushes any updates to audit event and RTM configurations out to all Axon Agent nodes. This task runs daily at midnight by default, so any changes to audit event and RTM configurations on Axon Agent nodes will take effect at that time. **You should also run this task any time you make changes to rules or any components of rules (start and stop points, global variables, etc) that are used for audit event collection or real-time monitoring.** For a complete list of activities that affect audit event and RTM configurations, see [Activities that May Change Audit Event or RTM Configurations on Axon Agents](#) on page 65.

A TE Agent node registers a rule's real-time status the first time it uses the rule for a baseline or version check. After this connection is established, updates to the rule are applied immediately and automatically.

Guidelines for Event Generators on Linux Systems

When installing an Event Generator on a supported Linux file server, these guidelines apply:

- Agents installed on Linux systems can detect changes to mounted filesystems on that system. However, an Event Generator only collects audit events and triggers real-time monitoring on a mounted filesystem if the change is made from the system where the Event Generator is installed. A change made to a mounted filesystem from another system will be detected by a version check, but the Event Generator will not generate audit events or trigger real-time monitoring for that change. For this reason, Tripwire recommends that you monitor filesystems locally whenever possible.
- To detect changes on an NFS-exported UNIX file server, you should select the **Enable real-time monitoring** option in the Events tab of each node that represents a client of the file server (see [Changing the Properties of a Node on page 321](#)).
- On a UNIX system, multiple hard links can refer to the same file. If a change is made to the content of a UNIX file via a hard link, Tripwire Enterprise real-time monitoring will only detect the change if a file system rule identifies the link. Therefore, to monitor a UNIX file with a file system rule, the rule should specify each of the file's hard links.
- To enable real-time monitoring on a Linux system, the `auditd` auditing subsystem must be installed on that system. However, Tripwire recommends that you disable the auditing subsystem to avoid potential conflicts.
- The Event Generator cannot report changes made via the `mmap()` family of syscall functions. If a syscall function is responsible for a change, it can only be detected with a version check.

Guidelines for Event Generators on AIX Systems

On AIX systems, the operating system disables the generation of Audit events for some privileged programs, including password maintenance tools like the `useradd` command. Because TE Agents on AIX systems depend on the native AIX audit system to generate audit data, changes made by these programs will not be detected by real-time monitoring. Any changes made by privileged programs will be detected by a standard TE version check, however.

About Selection Methods

A **selection method** specifies criteria that may be used to identify the element versions on which some promotions and some conditional actions will run. For further details, see:

- [What is the By-Match Selection Method? \(below\)](#)
- [What is the By-Reference Selection Method? \(on page 76\)](#)

What is the By-Match Selection Method?

With the **by-match** method, Tripwire Enterprise limits an operation to current change versions that meet criteria specified by a matching strategy. If an element’s current version fails to satisfy the criteria, TE omits the version from the operation.

To run a by-match operation, you specify the type of **matching strategy**, and provide the name and path of the source file containing the approved match criteria (known as a **match file**). [Table 16](#) describes each matching strategy, along with the content of associated match files.

Table 16. Matching strategies and match file contents

Matching Strategy	Match file contains a list of ...	An operation runs if ...
Element name	... element names	... a current version represents an element with a name that matches an entry in the match file.
Element name and hash value	... element names and associated hash values	... a current version represents an element with a name, change type, and hash value (optional) that matches an entry in the match file.
Rule name	... rule names	... a current version represents a monitored object that was identified by a rule listed in the match file.

A match file can either be a **UTF-8 encoded text file** or an **XML file** containing the output of a Detailed Changes Report.

- For information about Detailed Changes Reports and report XML files, see [What are Reports and Report Types? on page 172](#)
- For guidance in creating a text file, see *Creating a Text-Match File* in the *Tripwire Enterprise Reference Guide*.

Table 17 describes how the by-match method works with each applicable Tripwire Enterprise feature. When Tripwire Enterprise completes a **promotion** with the by-match method, the application reports the following data:

- The total number of current change versions that were successfully promoted.
- The total number of discrepancies. For descriptions, see [Table 18 on the next page](#).

Table 17. TE features that support the by-match method

TE Feature	With this feature, the by-match method determines ...
Node Manager promotions and promote actions	<p>... which current change versions will be promoted. For example, if you run a promote operation with the element-name strategy, Tripwire Enterprise only promotes a current change version if the match file contains the name of the version's element. If the file excludes the element's name, TE will not promote the version.</p> <p>Promote-by-match operations can be run manually in the Node Manager, or with a promote action. For more information, see:</p> <ul style="list-style-type: none"> • Promoting by Match (on page 396) • What are Actions and Action Types? (on page 116) • Creating a Promote Action (on page 495) <p>Note: As with all promotions, the scope of a promote-by-match can be limited to specific software-installation packages. For more information, see Promotion and Software-Installation Packages (on page 48).</p>
By-match conditional actions	<p>... which response is initiated by the conditional action. If a new change version satisfies the match criteria, the action runs its conditional response. For more information, see How Does a Conditional Action Work? (on page 125).</p>

Table 18. Discrepancies reported by a promote operation run with the by-match selection method

Type of Discrepancy	Applicable Matching Strategies	This discrepancy type indicates ...
At baseline	All	... an existing element in TE that 1) is specified by the match file, and 2) has a current baseline as its current version.
Mismatch	Element name and hash value	... an existing element in TE that 1) is specified by the match file, and 2) has a current version with a hash or change type that differs from the hash or change type specified by the match file.
Missing element	Element name Element name and hash value	... an element specified by the match file but lacking a corresponding element in TE.
Missing rule	Rule name	... a rule specified by the match file but lacking a corresponding TE rule.
Promote failed	All	... an existing element in TE that 1) is specified by the match file, and 2) that experienced a failure during the promote operation (for example, a failure due to a TE Console database error or an Agent communication failure).
Unexpected change	All	... an existing element in TE that 1) is <i>not</i> specified by the match file, and 2) has a change version as its current version.

What is the By-Reference Selection Method?

The **by-reference** selection method limits an operation to current versions that have a corresponding baseline version associated with another node (known as the **reference node**). To run an operation with this selection method, you specify the following objects:

- The reference node
- One or more **target nodes** (to indicate the systems on which the operation will run)
- (Optional) A rule or rule group to limit the operation to specific monitored objects. If a rule or rule group is not specified, the operation is not limited to specific objects.

A **target element** represents a monitored object of a target node. When you run a by-reference operation, Tripwire Enterprise performs the following steps for **each target element** (see [Figure 8 on page 78](#)):

1. Determines if the current version of the target element is a **change version**.
 - If so, the operation continues with [step 2](#).
 - If not, no further action is taken.
2. Determines if the target element is identical to one of the reference node's elements (known as the **reference element**).
 - If so, the operation continues with [step 3](#).
 - If not, no further action is taken.
3. To determine if the **change version is identical to any baseline version** of the reference element, TE compares a hash of the change version with each of the reference element's baselines.
 - If a match exists, TE runs the operation on the change version.
 - Otherwise, no action is taken.

Notes

If you run a promote-by-reference with the **Current baselines only** option, Tripwire Enterprise only compares the change version with the reference element's current baseline.

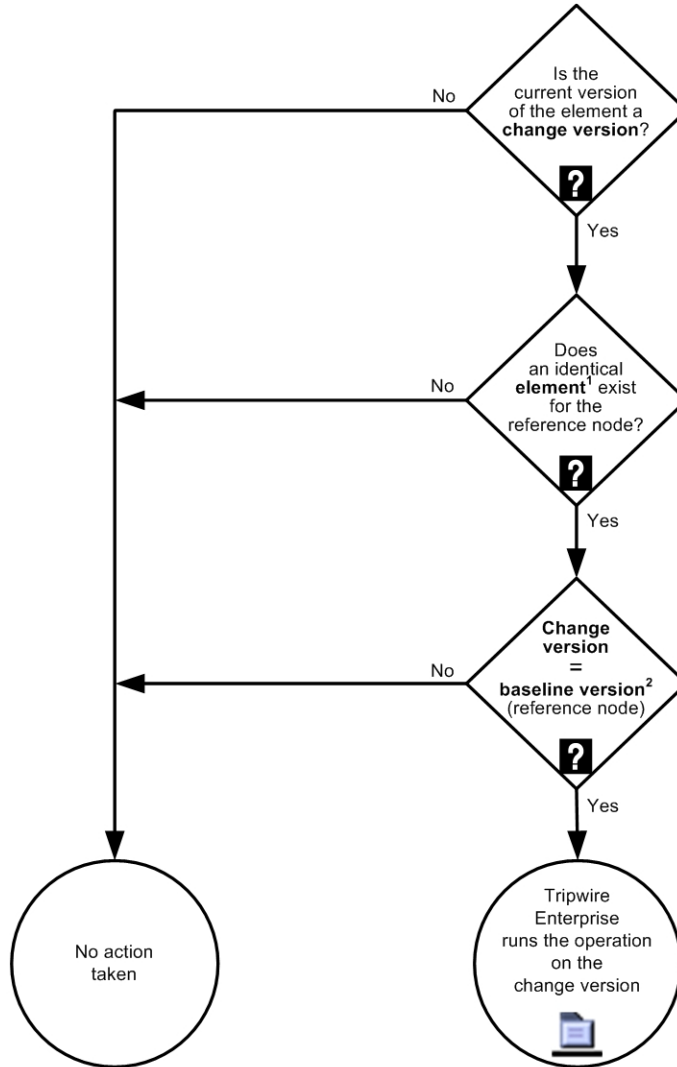
To run a by-reference operation, you specify the hash to be used (either MD5, SHA-1, SHA-256, or SHA-512). If the reference element's baselines lack the specified hash, TE runs the operation on the change version.

[Table 19 on the next page](#) describes how the by-reference method works with each applicable Tripwire Enterprise feature.

Table 19. TE features that support the by-reference method

TE Feature	With this feature, the by-reference method determines ...
Node Manager promotions and promote actions	<p>... which current change versions will be promoted. If a change version satisfies the by-reference criteria, TE promotes the version.</p> <p>By-reference promotions can be run manually in the Node Manager, or with a promote action. For more information, see:</p> <ul style="list-style-type: none">• Promoting by Reference (on page 397)• What are Actions and Action Types? (on page 116)• Creating a Promote Action (on page 495) <p>Note: As with all promotions, the scope of a promote-by-reference can be limited to specific software-installation packages. For more information, see Promotion and Software-Installation Packages (on page 48).</p>
By-reference conditional actions	<p>... which response is initiated by the conditional action. If a new change version satisfies the by-reference criteria, the action runs its conditional response. For more information, see How Does a Conditional Action Work? (on page 125).</p>

Figure 8. Process flow for a by-reference operation



1 To determine if the reference and target elements are identical, TE compares the names of the elements and the rules used to create the elements. If the names and rules match, the application considers the two elements to be identical.

2 If you run a by-reference operation with the **Current baselines only** option, TE only compares the change version with the reference element's current baseline.

About Rules

What are Rule Types?

A **rule** is a Tripwire Enterprise object that identifies one or more monitored objects. For each type of monitored system, TE provides a unique set of rules:

- **Database rules** (see [Table 20 below](#))
- **Network device rules** (see [Table 21 on the next page](#))
- **Directory rules** (see [Table 22 on the next page](#))
- **File server rules** (see [Table 23 on page 81](#))
- **Virtual infrastructure rules** (see [Table 24 on page 82](#))

Each of these rule types can only identify objects for the corresponding type of monitored system. For example, file server rules can only be used to identify monitored objects for file servers.

Tripwire Enterprise uses rules to:

- Baseline a monitored system ([About Baselines on page 43](#))
- Version check a monitored system ([About Version Checks on page 44](#))
- Refine the scope of a policy test (see [How Does a Policy Test Work? on page 135](#))

Tip In the Root Group of the Rule Manager, you can create rule groups to organize the rules in your TE implementation. For more information, see [About Groups on page 29](#).

Table 20. Types of database rules

Rule Type	Definition
Database metadata rules	A metadata rule specifies database configuration parameters and/or database objects. For further details, see How Does a Database Metadata Rule Work? on page 89 . Note: This version of Tripwire Enterprise can monitor Oracle, Microsoft SQL Server, PostgreSQL, and DB2 databases.
Database query rules	A query rule defines one or more SQL queries to retrieve content from monitored databases. For more information, see How Does a Database Query Rule Work? on page 92 .

Table 21. Types of network device rules

Rule Type	Definition
Command output validation rules (COVRs)	A COVR runs a command on a network device to generate output. To identify changes, Tripwire Enterprise compares the output with previous output from the system. For more information, see How Does a Command Output Validation Rule (COVR) Work? on page 103 .
Configuration file rules	A configuration file rule (or configuration rule) specifies configuration files on a specific type of network device produced by a single vendor. For example, a Cisco IOS configuration file rule can only identify configuration files on Cisco IOS routers. For more information, see Creating a Configuration File Rule on page 447 .
File rules	<p>A file rule specifies files on a network device to be checked for changes in content. Unlike configuration file rules, file rules can identify any type of file.</p> <ul style="list-style-type: none"> • A custom file rule identifies files on a network device represented by a custom node (see Creating a Custom Node on page 368). • A UNIX file rule identifies files on a UNIX system. A UNIX system is any system running a POSIX-compliant, UNIX-based operating system. <p>For more information, see Creating a File Rule on page 451.</p> <p>Note: VMware ESX file rules have been replaced by virtual infrastructure rules. For more information, see Table 24 on page 82.</p>
Status check rules	A status check rule determines the availability of a network device; in other words, whether or not the Tripwire Enterprise Server can access and communicate with the system. To create a status check rule, see Creating a Status Check Rule on page 452 .

Table 22. Types of directory rules

Rule Type	Definition
Active Directory rules	<p>An Active Directory rule specifies entries in an Active Directory.</p> <p>Note: For more information about directory rules, see How Does a Directory Rule Work? on page 93.</p>
LDAP rules	An LDAP rule specifies entries in any directory that uses LDAP as the directory protocol. LDAP (Lightweight Directory Access Protocol) is a standard, vendor-independent protocol.

Table 23. Types of file server rules

Rule Type	Definition
Command output capture rules (COCRs)	A command output capture rule (COCR) runs a command on a file server to generate output. To identify changes, Tripwire Enterprise compares the output with previous output from the server. For more information, see How Does a Command Output Capture Rule (COCR) Work? on page 99 .
Log transfer rules	<p>Unlike other rules, log transfer rules do <i>not</i> identify monitored objects.</p> <p>A log transfer rule runs a command on a TE Agent system to generate output which is then transferred to Tripwire Log Center (TLC). In TLC, the output is then converted into TLC log messages (see What are Log Messages? on page 166). For more information, see How Does a Log Transfer Rule Work? on page 98.</p> <p>Note: Log transfer rules cannot be used with Axon Agents.</p>
UNIX file system rules	A UNIX file system rule identifies directories and files in the file system of a UNIX operating system. For further details, see How Does a File System Rule Work? on page 83 .
Windows file system rules	A Windows file system rule identifies directories and files in the file system of a Windows operating system. For further details, see How Does a File System Rule Work? on page 83 .
Windows registry rules	A Windows registry rule identifies keys and entries in the registry of a Windows operating system. For further details, see How Does a Windows Registry Rule Work? on page 85 .
Windows RSoP rules	A Windows RSoP rule defines one or more queries to retrieve reports on the Resultant Set of Policy (RSoP) for specified Windows users. For more information, see How Does a Windows RSoP Rule Work? on page 88 .

Table 24. Types of virtual infrastructure rules

Rule Type	Definition															
VI hypervisor rules^{A,B}	<p>This rule type identifies configuration files and parameters for a hypervisor. For example, a VMware ESXi rule identifies:</p> <ul style="list-style-type: none"> • All VMware ESXi configuration files on a VI host machine. • All configuration parameters specified by the VMware application program interface (API). <p>For more information, see Creating a VI Hypervisor Rule on page 453.</p>															
Virtual machine configuration rules^B	<p>This type of rule identifies the configuration parameters for virtual machines managed by a hypervisor. For example, a VMware VM rule identifies all configuration parameters for a virtual machine managed by a VMware ESXi host. For more information, see Creating a Virtual Machine Configuration Rule on page 453.</p>															
Virtual switch configuration rules^B	<p>This type of rule identifies the configuration parameters for virtual switches managed by a hypervisor. For example, a VMware vSwitch rule identifies all configuration parameters for a virtual switch managed by a VMware ESXi host. For more information, see Creating a Virtual Switch Configuration Rule on page 454.</p>															
Distributed virtual switch rules	<p>This type of rule identifies the configuration parameters for distributed virtual switches managed by a hypervisor. For example, a VMware vNetwork Distributed Switch rule identifies all configuration parameters for a virtual switch managed by a vCenter server. For more information, see Creating a Virtual Switch Configuration Rule on page 454.</p>															
Command output hypervisor rules (COHRs)	<p>This type of rule runs a command on a hypervisor's host machine to generate output. In Tripwire Enterprise, the output is represented by a single element that adopts a name specified in the properties of the rule. When a COHR results in the creation of an element version, TE saves the output's content in the version's properties, along with an MD5 hash of the content. For more information, see Creating a Command Output Hypervisor Rule on page 446.</p> <p>Note: A COHR can only generate output for host machines that grant remote users access via SSH.</p>															
<p>A A VI hypervisor rule (e.g. a VMware ESXi rule) identifies the following configuration files on an ESXi host:</p> <table border="0" data-bbox="418 1457 1243 1612"> <tr> <td>esx.conf</td> <td>penwsman.conf</td> <td>syslog.conf</td> </tr> <tr> <td>hostAgentConfig.xml</td> <td>proxy.xml</td> <td>vmware_config</td> </tr> <tr> <td>hosts</td> <td>snmp.xml</td> <td>vmware_configrules</td> </tr> <tr> <td>license.cfg</td> <td>ssl_cert</td> <td>vmware.lic</td> </tr> <tr> <td>motd</td> <td>ssl_key</td> <td>vpxa.cfg</td> </tr> </table> <p>B VMware's Managed Object Browser (MOB) is a Web-based server application installed on all VMware ESXi hosts and vCenter servers. In the MOB, you can review all parameters for ESXi hosts, virtual machines, and vSwitches.</p>		esx.conf	penwsman.conf	syslog.conf	hostAgentConfig.xml	proxy.xml	vmware_config	hosts	snmp.xml	vmware_configrules	license.cfg	ssl_cert	vmware.lic	motd	ssl_key	vpxa.cfg
esx.conf	penwsman.conf	syslog.conf														
hostAgentConfig.xml	proxy.xml	vmware_config														
hosts	snmp.xml	vmware_configrules														
license.cfg	ssl_cert	vmware.lic														
motd	ssl_key	vpxa.cfg														

How Does a File System Rule Work?

A **UNIX file system rule** or **Windows file system rule** identifies files and directories in a file system. [Table 25](#) defines the components that may be assigned to a UNIX or Windows file system rule.

To create a new file system rule, see [Creating a File System Rule on page 455](#).

Tip To optimize system performance, you should avoid using a single file system rule to monitor an entire file system. Instead, Tripwire recommends the use of multiple file system rules that identify different monitored objects. By using multiple file system rules (as opposed to a single rule), you can significantly reduce the amount of bandwidth and memory required to baseline or version check the file system.

Table 25. Components of a UNIX or Windows file system rule

Component	Description
start points	A start point specifies a file or directory for the rule.
stop points	A stop point specifies a file or directory to be excluded from operations run with the rule. If a stop point specifies a directory, you can also exclude the directory's contents.
criteria sets	<p>In a file system rule, a criteria set specifies attributes of files and directories. When a new element version is created for a file or directory identified by the rule, TE saves the object's values for the specified attributes in the new version.</p> <ul style="list-style-type: none">• To create a criteria set for a file system rule, see Creating a Criteria Set for a File System Rule on page 300.• For a list of attributes that may be added to a criteria set for a UNIX file system rule, see Table 76 on page 301.• For a list of attributes that may be added to a criteria set for a Windows file system rule, see Table 77 on page 302.
actions	An action initiates a response if the rule identifies a monitored object for which a change version is created. For more information, see What are Actions and Action Types? on page 116 .

What is the Adjust Rule Feature?

With the **Adjust Rule** feature, you can quickly modify the following rule types from a variety of locations in the TE interface:

- File system rules
- Windows registry rules
- Database rules
- Directory rules

Specifically, you can make the following changes to a rule:

- Add a start point for a monitored object (such as a directory or registry key)
- Edit an existing start point for a monitored object
- Add a stop point for a monitored object
- Delete a single stop point

The available options depend upon whether or not start points and stop points exist for a specified monitored object. For example, if a Windows file system rule includes a start point for a file, you cannot create another start point for the same file.

You can access the Adjust Rule feature from any part of the TE interface containing a list of elements. For example, you can access the Adjust Rule feature from:

- The **Node Manager** when elements are displayed in the Node Manager table (see [Viewing Nodes, Node Groups, and Elements on page 313](#))
- The **Elements tab** in a node properties dialog (see [Changing the Properties of a Node on page 321](#))

To modify a rule with the Adjust Rule feature, see:

- [Adding a Start Point with the Adjust Rule Feature \(on page 398\)](#)
- [Editing a Start Point with the Adjust Rule Feature \(on page 399\)](#)
- [Adding a Stop Point with the Adjust Rule Feature \(on page 400\)](#)
- [Deleting a Stop Point with the Adjust Rule Feature \(on page 401\)](#)

How Does a Windows Registry Rule Work?

What is a Registry?

A **registry** is a database in which a Windows operating system stores configuration information. The information in a registry is organized hierarchically in a collection of keys, entries, and values.

- A **key** is an object containing related registry information.
- The keys at the highest level of a registry hierarchy are known as **root keys** or **hives**. Although root keys vary between operating systems, [Table 26](#) defines those that are most common.
- Each key may contain a number of named **entries**. Each entry has one or more **values**, including a single, unnamed **default value**. With the exception of some default values, each value consists of data in numeric, text, or binary format.

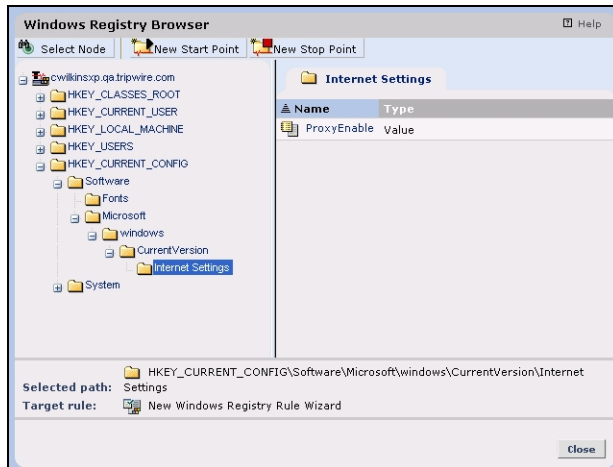
Table 26. Common root keys in a Windows registry

Root Key Name	Contains ...
HKEY_CLASSES_ROOT	... object linking and embedding (OLE) information, along with file associations (the application with which each file type is associated by default).
HKEY_CURRENT_USER	... all preference settings for the current user.
HKEY_USERS	... all preference settings for all users of the system.
HKEY_LOCAL_MACHINE	... settings for the operating system, system hardware, and installed applications.
HKEY_CURRENT_CONFIG	... configuration data for the current hardware profile.

[Figure 9 on the next page](#) shows an example of a Windows registry hierarchy in a Tripwire Enterprise dialog known as the Windows Registry Browser. In this example, the registry tree is expanded to display the keys within the **HKEY_CURRENT_CONFIG** root key. The displayed keys include **System** and **Software**, along with the keys descended from the Software key (Fonts, Microsoft, windows, CurrentVersion, and Internet Settings). In addition, the ProxyEnable entry is displayed in the right-hand pane of [Figure 9](#).

Note In the Windows Registry Browser, you may select registry keys and entries to be used as start points and stop points for a Windows registry rule.

Figure 9. Registry contents in the Windows Registry Browser



About Windows Registry Rules

A **Windows registry rule** identifies registry keys and entries on a Windows system. [Table 27 \(on the next page\)](#) defines the components of a Windows registry rule. For more information, see:

- [Naming Requirements for Monitored Objects Identified by Start Points and Stop Points in a Windows Registry Rule \(on the next page\)](#)
- [Creating a Windows Registry Rule \(on page 457\)](#)

Tip To optimize system performance, avoid using a single Windows registry rule to monitor all registry keys and entries on a Windows system. Instead, Tripwire recommends using multiple Windows registry rules that identify different keys and entries. By using multiple Windows registry rules (as opposed to a single rule), you can significantly reduce the amount of bandwidth and memory required to baseline or version check a Windows system.

Table 27. Components of a Windows registry rule

Component	Description
start points	A start point specifies a registry key or entry for the rule.
stop points	A stop point specifies a key or entry to be excluded from operations run with the rule. If a stop point specifies a key, you can also omit the key's descendant objects.
criteria sets	<p>In a Windows registry rule, a criteria set specifies attributes of keys and entries. When a new element version is created for a key or entry identified by the rule, TE saves the object's values for the specified attributes in the new version.</p> <ul style="list-style-type: none">• To create a criteria set for a Windows registry rule, see Creating a Criteria Set for a Windows Registry Rule on page 304.• For a list of attributes that may be added to a criteria set for a Windows registry rule, see Table 78 on page 304.
actions	An action initiates a response if the rule identifies a monitored object for which a change version is created. For more information, see What are Actions and Action Types? on page 116 .

Naming Requirements for Monitored Objects Identified by Start Points and Stop Points in a Windows Registry Rule

In order to create a start point or stop point in a Windows registry rule (see [Table 27 above](#)), the name of the corresponding registry key or entry (in the registry of the monitored system) must satisfy the following requirements:

- If the name involves a path containing multiple keys, a **backward slash (\)** must appear after each key in the path.
- If the name identifies an entry (rather than a key), the **pipe symbol (|)** must appear between the last key and the entry.

If the registry object's name fails to meet these requirements, you cannot create a start point or stop point for the object. For example, for the EnableAutodial entry shown in [Figure 9 on the previous page](#), the entry's name must be:

```
HKEY_CURRENT_CONFIG\Software\Microsoft\windows\  
CurrentVersion\Internet Settings|EnableAutodial
```

For a key's default value, the pipe symbol must appear at the end of the key's path, as in the following example:

```
HKEY_CURRENT_CONFIG\Software\Microsoft\windows\  
CurrentVersion\Internet Settings|
```

How Does a Windows RSoP Rule Work?

In a Windows environment, a **Group Policy Object (GPO)** stores policy settings for users and computers. For instance, a GPO could define the following settings:

- Windows Registry permissions
- Audit and security policies
- Login/logout scripts

Each Windows system stores a single **local Group Policy Object**. In an Active Directory environment, a local GPO has a subset of the settings stored in a **non-local Group Policy Object**. Stored on a domain controller, a non-local GPO is linked to an Active Directory site, domain, or organizational unit. (For a discussion of directory terms and concepts, see [How Does a Directory Rule Work? on page 93](#)).

If the settings in a local GPO conflict with those of a single non-local GPO, the non-local GPO takes precedence. However, multiple non-local GPOs can apply to the same user or computer. In this case, a **Resultant Set of Policy plug-in** calculates the cumulative effect of multiple GPO settings for each user on the local system. A **Resultant Set of Policy (RSoP)** is the group of policy settings that are actually in effect for a specific user.

To monitor the RSoP of a Windows user for changes, you can use a **Windows RSoP rule**. A Windows RSoP rule defines one or more queries, and each query retrieves a report on the RSoP of a specified Windows user. To identify any changes, Tripwire Enterprise compares the following attributes with a previous version of the report:

- A static set of attributes that indicate the values of common Group Policy settings. For a list of these settings, see *Windows RSoP Attributes* in the *Tripwire Enterprise Reference Guide*.
- The MD5 and/or SHA-1 hash of the RSoP report's content. These hashes are specified by the criteria set assigned to the rule.

For more information, see:

- [Creating a Windows RSoP Rule \(on page 458\)](#)
- [Creating a Criteria Set for a Windows RSoP Rule \(on page 306\)](#)

How Does a Database Metadata Rule Work?

About Database Metadata Rules

A **database metadata rule** identifies configuration parameters and/or database objects (such as tables or views). Tripwire Enterprise creates a single element for each monitored object that is baselined by a metadata rule.

- For a **configuration parameter**, each element version consists of a hash of a string that identifies the parameter's name and value. For an Oracle parameter, the string also includes a description.
- For a **database object**, each element version consists of a hash of all database definition language (DDL) statements used to define the object.

Table 28 defines the components that may be assigned to a database metadata rule.

Table 28. Components of a database metadata rule

Component	Description
start points	A start point specifies a configuration parameter or database object for the rule. For further details, see Database Metadata Rules and Monitored Objects below.
stop points	A stop point specifies a configuration parameter or database object to be excluded from operations run with the rule. Tip: A stop point is useful for excluding a type of database object, such as all tables or views. To exclude specific objects, you can also use the include and exclude filters in a start point (see Creating a Database Metadata Rule on page 448).
criteria sets	A criteria set determines the format of hashes (MD5, SHA-1, SHA-256, and/or SHA-512) in element versions created for monitored objects identified by the rule. To create a criteria set, see Creating a Criteria Set for a Database Rule on page 307.
actions	An action initiates a response if the rule identifies a monitored object for which a change version is created. For more information, see What are Actions and Action Types? on page 116.

Database Metadata Rules and Monitored Objects

In a **Microsoft SQL Server metadata rule**, a start point can identify a configuration parameter, login, server role, database, or one of the following types of database objects:

Database roles	Tables
DML triggers	Users
Functions	User-defined types
Indices	Views
Stored procedures	

In a **DB2 metadata rule**, a start point can identify any configuration parameter, login, server role, database, or one of the following types of database objects:

Alias	Security Label Component
Audit Policy	Sequence
Bufferpool	Service Class
Configuration Parameter	Table
Database Partition Group	Tablespace
Event Monitor	Threshold
Function	Trigger
Group	User
Histogram Template	User Defined Type
Index	Variable
Package	View
Procedure	Work Action Set
Role	Work Class Set
Schema	Workload

The following DB2 objects **cannot** be monitored by a database metadata rule: Function Mapping, Index Extension, Method, Nickname, Security Label, Security Policy, Server, Transform, Trusted Context, Type Mapping, User Mapping and Wrapper.

In an **Oracle metadata rule**, a start point can identify a database configuration parameter or one of the following types of database objects:

Clusters	Profiles	Tables
Database links	Procedures	Tablespaces
Directories	Roles	Triggers
Functions	Schemas	Users
Indices	Sequences	User defined types
Libraries	Stored outlines	Views
Packages	Synonyms	

The following Oracle objects **cannot** be monitored by a database metadata rule: Java objects, rollback segments, operators, and materialized views and logs. In addition, Tripwire Enterprise *cannot* detect changes in some options associated with Oracle database **tables** and **indices**. For further details, see [Table 29 \(below\)](#).

Table 29. Unmonitored options for Oracle tables and indices

Database Object	Tripwire Enterprise cannot monitor ...
Indices	<ul style="list-style-type: none"> • Hash partitions on LOBs and VARRAYs • Local composite list partitions, including subpartitions
Tables	<ul style="list-style-type: none"> • Object properties for object and XML tables • OID index clauses for object and XML tables • LOB partition storage • Composite partitioning

In a **PostgreSQL metadata rule**, a start point can identify one of the following types of database objects:

Extensions	Schemas
Indices	Sequences
Functions	Tables
Roles	Views

To create a database metadata rule, see [Creating a Database Metadata Rule on page 448](#).

How Does a Database Query Rule Work?

A database query rule defines one or more **SQL queries** to retrieve content from specified tables and/or views in monitored databases. In a query rule, each query is defined with a SELECT statement (or with a SELECT or SHOW statement for PostgreSQL databases). When a query rule baselines a database, Tripwire Enterprise creates a single element for each query in the rule.

Notes Since a query can only be defined with a SELECT or SHOW statement, database contents are unaffected when the query runs.

If you have implemented query whitelists on Tripwire Enterprise Agents, each query specified in a database query rule must exactly match a query in a query whitelist file. For more information, see [Restricting Queries on Database Nodes with Whitelists on page 429](#).

A database query rule **cannot** retrieve content from the following types of Oracle database columns:

BINARY FLOAT	RAW
BINARY DOUBLE	TIMESTAMP WITH TIME ZONE
INTERVAL DAY TO SECOND	USER DEFINED TYPE
INTERVAL YEAR TO MONTH	XMLTYPE
LONG RAW	

To create a query rule, see [Creating a Database Query Rule on page 449](#).

How Does a Directory Rule Work?

What are Directory Entries and Attributes?

Note For an introduction to directories and directory servers, see *What are Node Types?* on page 51.

A **directory** is a centrally-managed, hierarchical repository of data. The data in a directory can be drawn from a variety of systems, applications, and databases on a network.

Any type of data can be stored in a directory. However, directories are typically used to store information that remains relatively constant over time. For example, directories commonly store:

- Personal information (such as people’s names, e-mail addresses, and phone numbers)
- User account credentials (such as user names and passwords)
- Network resources (such as the configurations of computers and other devices on a network)

An **entry** is a record within a directory, and an **attribute** is a property of an entry. For example, the entries in a directory may represent user accounts. For each of those entries, the associated attributes may consist of the user’s name, phone number, and e-mail address.

Each attribute consists of two components:

- The **attribute name** is a label for the attribute.
- The **attribute value** is the actual data being stored by the attribute. The attribute value may consist of either text or binary data, and a single attribute can have one or more values.

For example, `cn=Monica Combs` is an attribute name/value pair, where:

`cn` is the attribute name, and

`Monica Combs` is the attribute value.

Table 30 (below) identifies some common attribute names used in directories.

Table 30. Common attribute names

Attribute Name	Used for ...
cn	... common names of entities
ou	... organizational units that reflect the structure of a network or organization
dc	... components of a domain name (domain components)

What are Object Classes and Schemas?

Each attribute in an entry is either required or optional. However, the **objectClass** attribute is a special attribute that is required for all entries. The **objectClass** attribute identifies the object classes that apply to each entry. An **object class** is a collection of definitions that applies to one or more entries; for example:

- Definitions dictating the required and optional attributes for each entry in the object class
- Definitions determining the directory location(s) in which the object class' entries may be created

The available object classes are defined in the directory's **schema**. When an entry is added to a directory, the system checks the entry against the definitions associated with the entry's object class. If the entry does not satisfy all of the definitions for the object class, the addition will fail. For instance, if the entry lacks a required attribute, the entry is incomplete and, therefore, disallowed by the schema.

How are Directories Organized?

Four types of entries comprise a directory:

- The **root DSE** (Directory Systems Agent Specific Entry) is a special entry that defines the capabilities of the directory server itself. For example, the root DSE identifies the directory protocols that are compatible with the directory.
- A **container entry** is an entry used to organize other entries in parent/child relationships. As with a folder in a file system, a container can have entries and/or other containers as children, but a child entry can only have a single container as a parent. An entry becomes a container when other entries (children) are placed under it.
- Listed in the root DSE, a **naming context** is a container entry that has no parent entry.
- Under a naming context, a **leaf entry** is an entry that does *not* contain other entries.

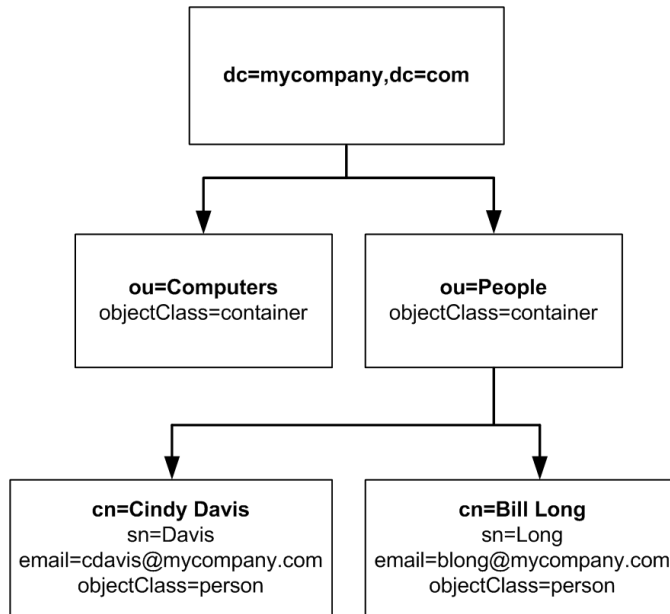
Figure 10 on the next page provides an example of a simplified directory.

- `dc=mycompany,dc=com` is the naming context for the directory hierarchy.
- Directly beneath that, two container entries have been created: `ou=Computers` and `ou=People`.
- In one of the container entries (`ou=People`), two leaf entries exist. The leaf entries are records for two people (Cindy Davis and Bill Long).
- The **objectClass** (`person`) identifies two required attributes (`sn` and `email`) that must be associated with each leaf entry.

Note The root DSE is not depicted in Figure 10.

In a directory, each entry is uniquely identified by a **distinguished name (DN)**. A DN refers to a specific entry in a directory, and clearly indicates the location of the entry.

Figure 10. Example of a directory hierarchy



Each distinguished name is an ordered list of attribute-value pairs that are read from right to left. To identify an entry, a DN adds a unique attribute to the DN of the entry's parent. In our example (Figure 10), the DN for the Bill Long entry is:

`cn=Bill Long,ou=People,dc=mycompany,dc=com`

Among the children of the parent entry (`ou=People`), the `cn` attribute (`cn=Bill Long`) is unique. The other components of the DN (`ou=People`, `dc=mycompany`, and `dc=com`) represent attribute-value pairs positioned above the `cn` attribute in the directory hierarchy.

For more information about directory servers, see:

LDAP Directories Explained, Brian Arkills (Addison-Wesley, 2003)

About Directory Rules

In Tripwire Enterprise, a **directory rule** identifies entries and attributes in a directory (see [Table 22 on page 80](#) for a list of directory rule types). [Table 31](#) defines the components that may be assigned to a directory rule. Start points and stop points determine exactly which entries and attributes are identified by a directory rule.

Table 31. Components of a directory rule

Component	Description
start points	A start point specifies an entry, as well as one or more attributes of the entry to be monitored by the rule. If a start point specifies a container entry, the entry's children will also be identified by the rule. Note: The <code>objectClass</code> attribute determines which attributes are available with each entry (see How are Directories Organized? on page 94).
stop points	A stop point specifies an entry to be excluded from operations run with the rule. If a stop point specifies a container entry, you can also exclude the entry's children.
actions	An action initiates a response if the rule identifies a monitored object for which a change version is created. For more information, see What are Actions and Action Types? on page 116 .

To create a new directory rule, see [Creating a Directory Rule on page 450](#).

Tips For your convenience, Tripwire provides a collection of default directory rules on the Tripwire Web site. For more information, see [What are Pre-Configured Rules and Policies? on page 219](#).

For a list of directory products officially supported by Tripwire Enterprise, see:

<https://www.tripwire.com/products/tripwire-enterprise/tripwire-enterprise-platform-and-device-support-register>

To optimize system performance, you should avoid using a single directory rule to monitor all entries in a directory. Instead, Tripwire recommends the use of multiple directory rules that identify different entries and attributes. By using multiple directory rules (as opposed to a single rule), you can significantly reduce the amount of bandwidth and memory required to baseline or version check the directory.

What are Binary Attributes and Security Attributes?

In a directory, attributes can be saved in a variety of formats. As appropriate, you can define the formats of specific attributes in the Settings Manager. By defining the formats of attributes, you explicitly instruct Tripwire Enterprise to process and save the data in a specific manner.

- When an attribute is defined as a **binary attribute**, Tripwire Enterprise treats the attribute's value as binary data. As a result, the application saves the attribute's value as an MD5 hash in new element versions.
- (Active Directory only) If you designate an attribute as a **security attribute**, Tripwire Enterprise will interpret the attribute's value as a Windows security descriptor. As a result, new element versions will save the attribute's value as four related attributes: a DACL, a SACL, an owner, and a group.

<p>Note In an Active Directory, a Windows security descriptor is a binary data structure that identifies the users who have access to an entry. In addition, a Windows security descriptor defines the permissions granted to each user.</p>
--

For further instructions, see:

- [Setting LDAP Directory Preferences \(on page 311\)](#)
- [Setting Active Directory Preferences \(on page 311\)](#)

How Does a Log Transfer Rule Work?

Unlike other rules, log transfer rules do *not* identify monitored objects. Instead, a **log transfer rule** defines a command to query the contents of one or more files on TE Agents. When a log transfer rule is used in a baseline operation or version check run on a TE Agent, TE executes the command and saves the output in a single G-zipped temporary file on the Agent. The TE Agent then sends the file to your Tripwire Log Center (TLC) File Collector via SFTP, and TLC creates a **TLC log message** for each line in the file.

Note Log transfer rules cannot be used with Axon Agents.

In the properties of a log transfer rule, you define the command to be run on TE Agents. The command can query all content in a file or just specified content. With the search-and-replace feature, you can use regular expressions to replace every instance of a string in command output with another string. For instance, you might conceal passwords in command output by replacing them with other text. For more information, see:

- [How Do Regular Expressions Work? \(on page 107\)](#)
- [Advanced Search-and-Replace with Variables \(on page 109\)](#)
- [Creating a Log Transfer Rule \(on page 451\)](#)

Note If you have implemented whitelists on Agent systems, the command specified in a log transfer rule must exactly match a command in a whitelist file. For more information, see [Restricting Commands on Agent Nodes with Whitelists on page 424](#).

For more information about TLC, see the Tripwire Log Center documentation:

<http://tlcdocumentation.tripwire.com/>

How Does a Command Output Capture Rule (COCR) Work?

A command output capture rule (COCR) runs a command or script on a **file server** to generate and capture output. In Tripwire Enterprise, the output is represented by a single element that adopts a name specified in the properties of the COCR. To identify changes, TE compares generated command output with a baseline version of the output.

In the properties of a COCR, you define the command or script to be run on targeted file servers. In addition, you can configure the features described in [Table 32](#). These features are configured with regular expressions. For more information about regular expressions in Tripwire Enterprise, see [How Do Regular Expressions Work? on page 107](#).

Note If you have implemented whitelists on Agents, the command specified in a COCR must exactly match a command in a whitelist file. For more information, see [Restricting Commands on Agent Nodes with Whitelists on page 424](#).

Table 32. Command output capture rule (COCR) features

Feature	Description
Filtering command output	Filtering is the process of excluding content from command output monitored by Tripwire Enterprise. For example, you could instruct TE to remove all instances of a password from command output.
Search-and-replace	With the search-and-replace feature, you can replace every instance of a string in command output with another string. For instance, you could conceal passwords in command output by replacing them with other text. For more information, see Advanced Search-and-Replace with Variables on page 109 .

If a COCR generates output for a new element version created by a baseline operation or version check, TE saves the output's content in the version, along with the following attributes:

- An MD5 hash of the content. To calculate this hash, TE excludes any filtered output and includes any replacement strings (see [Table 32](#)).
- The return code (or exit code) of the command.

To create a COCR, see [Creating a Command Output Capture Rule on page 445](#).

For examples of how COCRs can be used, see [COCR Examples on the next page](#)

COCR Examples

COCR Example #1: Determining the Physical Memory Capacity of Windows File Servers

As the system administrator for his company, Ron has been tasked with determining the physical memory capacity of each Windows file server on the company's network. In this example, Ron will create a COCR to retrieve this information from each server's Windows Management Instrumentation (WMI) service.

To create and test the new COCR, Ron completes the following steps:

1. First, Ron creates the COCR (see [Creating a Command Output Capture Rule on page 445](#)). In the New Rule Wizard, he enters the following command in the **Command Line** field:

```
wmic /node:localhost memphysical get Caption, MaxCapacity, MemoryDevices
```

In the **Element Name** field, Ron enters the following descriptive name for elements created by the COCR:

```
ram-max-cap
```

2. In the Task Manager, Ron creates a check rule task, and assigns the Windows file server node and the new COCR to the task (see [Creating a Check Rule Task on page 518](#)).

In the last page of the New Task Wizard, he selects the **Initialize baselines now** check box. With this setting, Tripwire Enterprise automatically creates a current baseline by applying the new COCR to the Windows file server node.

3. In the Node Manager, Ron selects the current baseline to open the element version properties dialog (see [Changing the Properties of an Element Version on page 327](#)). The **Content** tab should indicate the physical memory capacity for the Windows system.

COCR Example #2: Monitoring the Processes Running on an Agent Using a Script

This example demonstrates how scripts can be used in COCRs to capture more advanced output. Specifically, the COCRs below gather a list of running processes on Linux and Windows nodes.

Tip For more information on using scripts in COCRs, click **Help** in any COCR's Command tab.

Linux:

For a COCR targeted to run on **Linux** systems, the **Command Line** field (on the rule's Command tab) would contain the following line, which launches a script:

```
$(ScriptFile.sh)
```

The **Script** field on the Content tab would include the following script:

```
declare -a arrPaths
declare -a arrElements
declare -a arrElementDirs
regex="^[0-9]+$"
exe=exe;
for processDirFull in `ls -d /proc/*/*`; do
    match=0
    processDir=${processDirFull:6}
    len=${#processDir}
    processDir=${processDir:0:$len-1}
    if [[ $processDir =~ $regex ]]; then
        processEXE=${processDirFull}$exe
        processPath=`readlink $processEXE`
        lenProcessPath=${#processPath}
        if (($lenProcessPath > 1)); then
            for acc in "${arrPaths[@]}"; do
                if [[ $acc = "$processPath" ]]; then
                    match=1
                    break
                fi
            done
            if [[ $match = 0 ]]; then
                arrPaths+=("$processPath")
                echo $processPath
            fi
        fi
    fi
done
```

The **Element Name** field would contain a descriptive name for the output of the rule, like:

```
Current Running Processes
```

Each time TE runs this rule on a Linux system, the script generates a list of processes running on the system. Each time the rule detects a change to that list, TE will create a new version of the Current Running Processes element. You can view the list of processes from the element version's Content tab.

Windows:

For a COCR targeted to run on **Windows** systems, the **Command Line** field (on the rule's Command tab) would contain the following line:

```
move $(ScriptFile) $(ScriptFile).vbs && cscript /nologo $(ScriptFile).vbs &&
del $(ScriptFile).vbs
```

This command enables the same script to be used on both TE Agent and Axon Agent systems. Because Axon Agents don't support VBS scripts by default, this command renames the script, runs it, and then deletes the script after it has run.

Tip For more information on using scripts in COCRs, click **Help** in any COCR's Command tab.

The **Script** field on the Content tab would include the following script:

```
Dim runningProcs()
Set objWMIService = GetObject("winmgmts:{impersonationLevel=impersonate}!\\.\root\cimv2")
Set colProcesses = objWMIService.ExecQuery("Select * from Win32_Process", , 48)
intSize=0
For Each objProcess in colProcesses
    If not isnull(objProcess.ExecutablePath) Then
        If InStr (objProcess.CommandLine, WScript.ScriptName) = 0 Then
            runningProcBool=false
            filename=objProcess.ExecutablePath
            procCheck=Filter(runningProcs,LCASE(filename))
            for each p in procCheck
                runningProcBool=true
            Next
            If runningProcBool = false Then
                ReDim Preserve runningProcs(intSize)
                runningProcs(intSize)=LCASE(filename)
                intSize = intSize + 1
                wscript.echo filename
            End If
        End If
    End If
Next
```

The **Element Name** field would contain a descriptive name for the output of the rule, like:

```
Current Running Processes
```

Each time TE runs this rule on a Windows system, the script generates a list of processes running on the system. Each time the rule detects a change to that list, TE will create a new version of the Current Running Processes element. You can view the list of processes from the element version's Content tab.

How Does a Command Output Validation Rule (COVR) Work?

A command output validation rule (COVR) runs one or more commands on a **network device** to generate and capture output. As with COCRs, Tripwire Enterprise creates a single element to represent the output generated by a COVR. TE assigns the element a name specified in the properties of the COVR. To identify changes, TE compares generated command output with a baseline version of the output.

COVRs have several features that provide users with significant flexibility. [Table 33 \(below\)](#) defines the primary features associated with COVRs.

Selection and **filter** criteria are entered with regular expressions. For more information about regular expressions in Tripwire Enterprise, see [How Do Regular Expressions Work? on page 107](#).

For greater control, you can apply both selection and filter criteria to a COVR. In this case, Tripwire Enterprise first selects specified lines from generated output, and then filters undesired content from those lines.

- For examples of how COVR features might be used in practice, see [COVR Examples on the next page](#).
- To create a COVR, see [Creating a Command Output Validation Rule on page 446](#).

Table 33. Command output validation rule (COVR) features

Feature	Description
Command execution	In addition to output-generation commands, a COVR may include commands to be executed before (pre-commands) or after (post-commands) the generation of output. For instance, you could enter a command to change directories before executing a directory-listing command.
Selecting command output	Selecting is the process of specifying lines in command output to be monitored by Tripwire Enterprise. For instance, you could instruct TE to monitor lines that include a particular word, while ignoring all other lines.
Filtering command output	Filtering is the process of excluding content from command output generated by the rule. For example, you could instruct Tripwire Enterprise to remove all instances of a password from command output.
Search-and-replace	With the search-and-replace feature, you can replace every instance of a string in command output with another string. For instance, you could conceal passwords in command output by replacing them with other text. For more information, see Advanced Search-and-Replace with Variables on page 109 .
Asserting a baseline	With this feature, you can define baseline content for a COVR. When you baseline a monitored system with the COVR, the new baseline version adopts the baseline content defined by the COVR. When the same system is version checked with the COVR, Tripwire Enterprise compares the snapshot with the baseline defined by the COVR. Note: For an overview of version checking, see About Version Checks on page 44 .

COVR Examples

COVR Example #1: Monitoring Network Devices Outside a Firewall

In some environments, your Tripwire Enterprise Server may be unable to retrieve configuration information from a monitored network device. For instance, if a firewall separates the TE Server from a switch, the server may be unable to retrieve configuration information from the switch via TFTP. In such cases, a COVR may be used as an alternative to a configuration file rule. With a COVR, the TE Server establishes a connection with the switch, and retrieves configuration information via the connection.

In the following example, Julie, a system administrator, creates a COVR to monitor configuration information on a Cisco IOS device.

To create and test the new COVR, Julie completes the following steps:

1. First, Julie creates the COVR (see [Creating a Command Output Validation Rule on page 446](#)). In the New Rule Wizard, she enters the following command in the **Commands to capture** field:

```
show running-config
```

In the **Element name** field, Julie enters the following descriptive name for elements created by the COVR:

```
Cisco IOS config
```

2. In the Task Manager, Julie creates a check rule task, and associates the Cisco IOS device and the new COVR with the task (see [Creating a Check Rule Task on page 518](#)).

In the last page of the New Task Wizard, she selects the **Initialize baselines now** check box. With this setting, Tripwire Enterprise automatically creates a current baseline by applying the new COVR to the Cisco IOS device.

3. In the Node Manager, Julie selects the current baseline to open the element version properties dialog (see [Changing the Properties of an Element Version on page 327](#)). The **Content** tab should include the configuration information for the Cisco IOS device.

COVR Example #2: Version Checking Configuration Information

By adding selection criteria to a COVR, you can specify command output to be monitored by a version check of network devices. When a version check is run with a COVR containing selection criteria, Tripwire Enterprise scans all strings matching the selection criteria, and excludes all other output from the check.

In this example, Terry, a system administrator, wants to monitor the version numbers of Cisco IOS routers. To do this, she will create a COVR with selection criteria.

To create the new COVR, Terry completes the steps below:

1. In the New Rule Wizard, Terry enters **show version** in the **Commands to run** field (see [Creating a Command Output Validation Rule on page 446](#)).
2. In the **Selection Method** page, she selects **Include lines containing** and enters the following regular expression in the **Pattern** field:

```
^IOS
```

With this setting, version checks (run with the COVR) will only check lines that begin with the letters “IOS.”

Notes For a list of common characters used with regular expressions, see [Table 34 on page 108](#).

To edit the selection method for an existing COVR, see [Changing the Properties of a Rule on page 437](#).

3. In the Task Manager, Terry creates a check rule task, and associates the new COVR and a Cisco IOS router with the task (see [Creating a Check Rule Task on page 518](#)).
- In the last page of the New Task Wizard, she selects the **Initialize baselines now** check box. With this setting, Tripwire Enterprise automatically creates a current baseline by applying the new COVR to the Cisco IOS router.
4. In the Node Manager, Terry selects the new baseline to open the element version properties dialog (see [Changing the Properties of an Element Version on page 327](#)). The **Content** tab should only include lines that begin with the letters “IOS.”

COVR Example #3: Masking Data in Command Output

In some cases, it may be useful to replace dynamic or sensitive command-output data with dummy data. For instance, if you filter dynamic data from command output, you may want to replace the data with a marker indicating that output content has been removed. In this example, Dagny, a system administrator, uses the COVR search-and-replace feature to substitute dummy data for user passwords generated in command output.

Recently, Dagny created a COVR to check the configurations of Cisco IOS routers. To generate configuration output, she entered **show running-config** in the **Commands to capture** field (see [Creating a Command Output Validation Rule on page 446](#)).

To test the new rule, she baselined one of the routers with the COVR (see [Initial Baselineing of Monitored Objects on page 382](#)). When Dagny reviewed the resulting baseline, she found the following content (see [Changing the Properties of an Element Version on page 327](#)):

```
...
aaa processes 6
enable secret 5 $1$xbajx9jRxLXXYx/H/xX8Uwn3jH/
enable password 7 14111E1A0416261A2C
!
username admin privilege 15 password 7 140FA2041A0FF17
username user password 7 060206224241
...
```

Since the command output included several weakly encrypted passwords, Dagny decides to mask the passwords in future output generated by the COVR.

To edit the COVR, Dagny completes the steps below:

1. Dagny opens the properties dialog for the COVR (see [Changing Filter or Search-and-Replace Criteria for a COVR or COCR on page 442](#)).
2. In the **Filter** tab, she enters the following regular expression in the **Search pattern** field:

```
((password|secret)\s+\d+)(.*)
```

3. In the **Replacement string** field, she enters the following regular expression:

```
$1 XXXXXX
```

To test the updated rule, Dagny re-baselines the router (see [Re-baselineing Monitored Systems on page 383](#)). When she reviews the resulting baseline version, she discovers the following output. As intended, the COVR now replaces each password entry with the string “XXXXXX.”

```
...
aaa processes 6
enable secret 5 XXXXXX
enable password 7 XXXXXX
!
username admin privilege 15 password 7 XXXXXX
username user password 7 XXXXXX
...
```

How Do Regular Expressions Work?

In Tripwire Enterprise, a **regular expression** is a specially formatted pattern that can be used to identify instances of a string in command output or element version content. For instance, when used in a COCR or COVR, regular expressions identify a string(s) that TE should include or exclude when monitoring command output, or a string to be replaced by another string (with the search-and-replace feature; see [Table 33 on page 103](#)).

Note **Tripwire Enterprise Agents** use Java 2 regular expressions, which are compatible with Perl-based regular expressions. For a complete list of Java regular-expression constructs, see the Java pattern class online reference:

<http://download.oracle.com/javase/8/docs/api/java/util/regex/Pattern.html#sum>

Axon Agents use Perl Compatible Regular Expressions (PCRE). For more information, see www.pcre.org.

The syntax differences between these types of regular expressions are minor, and rules with regular expressions authored on a TE Agent will function correctly on an Axon Agent. However, a rule with regular expressions authored on an Axon Agent may not work on a TE Agent.

For more information on regular expressions, see the following resources.

- For definitions of regular-expression characters, see [Table 34 on the next page](#).
- For a discussion of advanced search-and-replace operations, see [Advanced Search-and-Replace with Variables on page 109](#).
- For examples of how regular expressions may be used in practice, see [Regular Expression Examples on page 109](#).
- For an authoritative guide to regular expressions, see:
Mastering Regular Expressions, Jeffrey E.F. Friedl (O'Reilly, 2002)

Table 34. Regular-expression syntax

Matching Characters	Description
.	This character matches any single character (a letter, number, symbol, etc.).
^	A caret matches the beginning of a line. For example, <code>^dir</code> matches lines beginning with the letters "dir."
\$	A dollar sign matches the end of a line. For example, <code>dir\$</code> matches lines ending with the letters "dir."
\n	This character matches a new line.
\s	This character matches a single whitespace character; for example, spaces or tabs. Note: Literal whitespace characters are ignored when a regular expression is processed.
\d	This character matches a single digit from 0 to 9.
\	This character is used to match special characters. For example, to match a * character, enter *. Note: Use this character to match literal instances of the regular-expression characters defined in this table.
Character Classes	Description
[...]	This character class matches any single character contained in the brackets. For example, <code>[a-z]</code> matches any lower-case letter.
[^...]	This character class matches any character that is <i>not</i> contained in the brackets. For example, <code>[^ABC]</code> matches any character except upper-case letters A, B, or C.
Modifying Characters	Description
*	This character requires zero or more matches of the preceding sub-expression.
+	This character requires one or more matches of the preceding sub-expression.
?	This character indicates that the preceding match is optional.
Scopes	Description
	This character signifies the operator "or." Example: <code>X Y</code> means "X or Y"
(... ...)	Parentheses may be used to: <ul style="list-style-type: none"> • Limit the scope of an expression to one or more of the specified values (delimited with the or character), or • Subdivide a regular expression into sub-expressions.

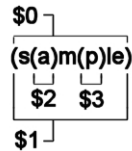
Advanced Search-and-Replace with Variables

To perform advanced search-and-replace operations on command output generated by a COCR or COVR, use the $\$n$ variable in the **Replacement string** field of the rule's properties dialog (see [Changing Filter or Search-and-Replace Criteria for a COVR or COCR on page 442](#)). $\$n$ returns matched text from the captured command output itself.

For each match of the pattern:

- $\$0$ returns the complete match,
- $\$1$ returns the 1st sub-expression of that match,
- $\$2$ returns the 2nd sub-expression of that match, and so on.

Within a regular expression, sub-expressions are enclosed in parentheses. For example, consider the following regular expression:



In this example, $\$0$ returns `sample`, because that is the first complete match of the pattern. $\$1$ returns `sample`, because that is the first sub-expression (defined by the first pair of enclosing parentheses). $\$2$ returns `a`, and $\$3$ returns `p`.

Regular Expression Examples

Regular Expression Example 1

```
Configuration\s register\s is\s [0-9a-zA-Z]+
```

This expression matches any string that:

1. begins with the words “Configuration register is ” (`Configuration\s register\s is\s`), followed by
2. any combination of concatenated letters (upper- and/or lower-case) and numbers (`[0-9a-zA-Z]+`).

Regular Expression Example 2

```
.*inet\s addr:10\.10\.10\.[0-9].*
```

This expression matches any string that:

1. begins with an unlimited number of instances of any character (`.*`), followed by
2. the literal value “inet addr:10.10.10.” (`inet\s addr:10\.10\.10\.`), followed by
3. any single digit from 0 to 9 (`[0-9]`), followed by
4. an unlimited number of instances of a single character (`.*`).

Regular Expression Example 3

The following text is the routing table from a UNIX system:

10.0.0.0	10.101.104.2	U	1	33
224.0.0.0	10.101.104.2	U	1	0
default	10.1.1.1	UG	1	0
127.0.0.1	127.0.0.1	UH		301619933

In the routing table, the last two columns (columns 4 and 5) contain dynamic data. To remove the dynamic data from command output generated by a COVR, you can add search-and-replace criteria to the rule.

To enter search-and-replace criteria to remove the routing table’s dynamic data:

1. In the **Search pattern** field, enter the following regular expression:

```
((U.)(\s+\d+)(\s+\d+)?)
```

2. In the **Replacement string** field, enter the following expression:

```
(U.)
```

The **Search pattern** expression defines four sub-expressions. The whole expression and sub-expressions are stored in the following \$n variables:

```
Whole expression $0 = ((U.)(\s+\d+)(\s+\d+)?)
```

```
Sub-expression $1 = (U.)(\s+\d+)(\s+\d+)?
```

```
Sub-expression $2 = (U.)
```

```
Sub-expression $3 = (\s+\d+)
```

```
Sub-expression $4 = (\s+\d+)?
```

The **Search pattern** regular expression matches any string that:

1. begins with an upper-case letter “U” and any single character (U.), followed by
2. one or more spaces followed by one or more digits (\s+\d+), followed by
3. one or more spaces followed by one or more digits (\s+\d+). The ? character makes this last sub-expression optional.

With these search-and-replace entries, Tripwire Enterprise replaces each string matching the **Search pattern** with a string that matches the **Replacement string**. Therefore, if the COVR is run with a version check of the UNIX system, the routing table columns with dynamic data will *not* appear in the command output.

10.0.0.0	10.101.104.2	U
224.0.0.0	10.101.104.2	U
default	10.1.1.1	UG
127.0.0.1	127.0.0.1	UH

About Severity Levels and Severity Ranges

What are Severity Levels?

Ranging from 1 (least important) to 10,000 (most important), a **severity level** is a numeric value that indicates the relative importance of a change detected by Tripwire Enterprise or a policy requirement assessed by a policy test. This section explains how Tripwire Enterprise assigns severity levels to detected changes.

A severity level is assigned directly or indirectly to every **rule** in a Tripwire Enterprise implementation.

- For a **network device rule**, **virtual infrastructure rule**, or **command output capture rule**, you assign a single severity level to the rule.
- For a **directory rule**, **database metadata rule**, **Windows file system rule**, **UNIX file system rule**, or **Windows registry rule**, you assign a severity level to each start point in the rule.
- For a **database query rule** or **Windows RSoP rule**, you assign a severity level to each query defined by the rule.

Note To create a rule, start point, or query without an associated level of importance, you may assign a severity level of zero (0).

If Tripwire Enterprise detects a change and creates a new change version, the application assigns a severity level to the new version. The version's severity level is determined by the type of rule that identified the changed element.

- For a **network device rule**, **virtual infrastructure rule**, or **command output capture rule**, TE assigns the severity level associated with the rule.
- For a **directory rule**, **database metadata rule**, **Windows file system rule**, **UNIX file system rule**, or **Windows registry rule**, TE assigns the severity level of the start point that identified the changed monitored object.
- For a **database query rule** or **Windows RSoP rule**, TE assigns the severity level of the query that identified the changed monitored object.

Note When TE detects a change on a node without a Change Audit license, all change versions created on that node are assigned a severity level of zero (0). If you add a Change Audit license to the node, severity levels will be assigned to subsequent change versions as described above.

For more information about the functionality that is available with each type of license, see [About Tripwire Enterprise Licenses on page 202](#).

To adjust the severity levels associated with start points and rules, see:

- [Changing the Properties of a Rule \(on page 437\)](#)
- [Changing or Deleting Start Points \(on page 466\)](#)

For greater control, you can assign a **severity override** to a specific attribute in a criteria set. If TE creates a change version for the attribute, the severity level specified by the attribute's override is assigned to the change version. These overrides can also be used to reduce the 'noise' generated by Tripwire Enterprise.

- If you assign a severity override of zero (0) to an attribute in a criteria set, TE will not create change versions for the attribute.
- If TE creates a change version for an element with two or more changed attributes that have severity overrides, TE assigns the highest severity level to the change version.





To assign or adjust severity overrides in a criteria set, see [Changing Criteria Set Properties on page 308](#).

You can also use **severity override actions** to explicitly assign a severity level to change versions. For more information, see [What are Actions and Action Types? \(on page 116\)](#).




<p>Note In a policy test, a severity level indicates the relative importance of the requirement evaluated by the test. For more information, see About Severity Levels and Policy Tests on page 132.</p>

What are Severity Ranges?

A **severity range** is a range of severity level values (1 to 10,000) associated with a specific color. When a new change version is created, Tripwire Enterprise determines which severity range contains the version's severity level. The application then applies a severity indicator to the following icons in the Node Manager:

-  The icon of the change version itself
-  The icon of the version's element
-  The icon of the element's node
-  The icon of each node group containing the element's node

A **severity indicator** is a circular emblem that displays the color of the severity range containing the change version's severity level. In the Node Manager, severity indicators provide a visual key for evaluating the seriousness of changes detected on your network. When applied to the icon of an element or element version, a severity indicator also includes one of the following symbols to indicate the type of change:

-  A plus sign indicates the addition of a new monitored object.
-  A minus sign indicates that a monitored object no longer exists.
-  An exclamation point indicates that an existing monitored object has been modified.

Note When TE detects a change on a node without a Change Audit license, all change versions created on that node are assigned a severity level of zero (0). Because this severity level falls outside of any severity range, TE does not display a severity indicator for changes detected on nodes without a Change Audit license.

For more information about the functionality that is available with each type of license, see [About Tripwire Enterprise Licenses on page 202](#).

By default, Tripwire Enterprise is configured with three severity ranges (see [Table 35](#)). As needed, you can create and delete severity ranges in the Settings Manager. In addition, you can change the color or severity levels associated with any existing severity range. For instructions, see [Working with Severity Ranges on page 270](#)

Table 35. Default severity ranges

Severity Range	Severity Indicator Color	Severity Level Values
High	Red	67 - 10,000
Medium	Yellow	34 - 66
Low	Blue	1 - 33

Example: Using Severity Levels and Severity Ranges

Jane, the system administrator for Tripwire, Inc., uses a configuration file rule to run a version check on a router. The rule has a severity level of 80, and Jane has *not* modified the default severity ranges for her Tripwire Enterprise implementation (see [Table 35](#)).

When Jane runs the version check, Tripwire Enterprise detects a system file that no longer conforms to the configuration file rule. In response, Tripwire Enterprise creates a new change version and assigns a severity level of 80. Since Jane has not modified the default severity ranges, and the change version's severity level (80) falls between 67 and 10,000, the application assigns the new version to the High severity range. In addition, in the Node Manager, the application applies a red severity indicator to each Tripwire Enterprise object affected by the change.

About Actions

What are Actions and Action Types?

An **action** is a Tripwire Enterprise object that initiates a response to detected changes. You can run any action as part of a version check. In addition, some actions can be run manually in the Node Manager with the Run Actions feature.

By running actions with a version check, you can ensure a timely and appropriate response to detected changes. To run an action with a version check, you first associate the action with a rule or check rule task. If the version check results in the creation of change versions, Tripwire Enterprise automatically executes the applicable actions. (For further details, see [About Version Checks on page 44](#).)

Action types are grouped in the following categories:

- **Common actions** can be run in response to detected changes in all types of monitored systems (see [Table 36 on the next page](#)).
- **Conditional** actions run one response if a detected change meets specified conditions, or another response if the conditions are not met. In either case, a response could be a TE action, action group, or no action. For more information, see [How Does a Conditional Action Work? on page 125](#).
- A **network device action** can only be run in response to detected changes in network devices (see [Table 37 on page 118](#)).

In the Action Manager, you can create action groups to organize the actions in your TE implementation. For more information, see [How Does an Action Group Work? on page 120](#).

For more information, see:

- [Using the Run Actions Feature \(on page 402\)](#)
- [Running Actions with Version Checks \(on page 119\)](#)

Table 36. Types of common actions

Action Type	Description
E-mail	An e-mail action sends an e-mail notification to specified recipients. For more details, see How Does an E-mail Action Work? on page 120 .
Execution	An execution action runs a command on either the TE Server or an Agent. For more information, see How Does an Execution Action Work? on page 121 .
Outside Change Window	Created by default when TE is installed, this action indicates if a detected change occurred within the time frame specified by an authorized maintenance window. For further details, see How Does the Outside Change Window Action Work? on page 122 . Note: This action cannot be deleted, and the name and description cannot be changed.
Promote-by-match	A promote-by-match action runs a promote-by-match operation. To do so, TE uses a matching strategy and match file specified by the action. (The match file must reside on your TE Server.) For more information, see: <ul style="list-style-type: none"> • What is the By-Match Selection Method? (on page 73) • Creating a Promote Action (on page 495) Note: This action can 1) add a comment to each current baseline created by the action, and 2) limit the scope of the promotion to specific software-installation packages (see Promotion and Software-Installation Packages on page 48).
Promote-by-reference	A promote-by-reference action runs a promote-by-reference operation. With the following exceptions, this process is identical to a promote-by-reference operation run in the Node Manager. <ul style="list-style-type: none"> • Tripwire Enterprise runs the operation with a reference node specified by the action. • The target nodes are all systems for which at least one change version was created by the version check. For more information, see: <ul style="list-style-type: none"> • What is the By-Reference Selection Method? (on page 76) • Creating a Promote Action (on page 495) Note: This action can 1) add a comment to each current baseline created by the action, and 2) limit the scope of the promotion to specific software-installation packages (see Promotion and Software-Installation Packages on page 48).
Promote specific versions	A promote specific versions action promotes each new change version created by a version check. For more information, see Creating a Promote Action on page 495 . Note: This action can 1) add a comment to each current baseline created by the action, and 2) limit the scope of the promotion to specific software-installation packages (see Promotion and Software-Installation Packages on page 48).
Promote to Baseline	Created by default when TE is installed, this action automatically promotes each new change version created by a version check. For more information about promotion, see What is Promotion? on page 47 . Note: This action cannot be deleted, and the name and description cannot be changed.
Run report	A run report action runs a specified report. For more information, see How Does a Run Report Action Work? on page 188 .

Action Type	Description
Run rule	If a version check detects a change in a monitored system, this action runs an additional version check of the system. For more information, see How Does a Run Rule Action Work? on page 123 .
Run task	A run task action runs a specified task. For more information, see: <ul style="list-style-type: none"> • What are Task Types? (on page 127) • Creating a Run Task Action (on page 498) Note: If this action runs a baseline rule task or check rule task, TE baselines or checks the node (or node group) that is assigned to the task.
Set custom value	If a version check creates a change version, this action assigns a value to a specified custom property for one of the following Tripwire Enterprise objects: <ul style="list-style-type: none"> • The change version's node • The change version's element • The change version itself For more information, see How Does a Set Custom Value Action Work? on page 124
Severity override	As described in What are Severity Levels? (on page 112) , TE automatically assigns a severity level to each change version. This action replaces the original severity level with a specified value. For example, if the original severity level of a change version is 100, but the severity override action has a severity level of 200, TE assigns a severity of 200 to the change version. For more information, see Creating a Severity Override Action on page 499 .
SNMP	An SNMP action sends an SNMP trap to a trap receiver, such as an Enterprise Management System (EMS). For more information, see How Does an SNMP Action Work? on page 124 .
Syslog	A syslog action sends an event notification to a system log. For more information, see Creating a Syslog Action on page 500 .
Tag	A tag action applies or unapplies tags to nodes. For more information on tags, see Working with Tags and Tag Sets on page 352 .

Table 37. Types of network device actions

Action Type	Description
Restore	A restore action automatically overwrites the content of a changed file with the content of the file's current baseline. For further details, see How Does a Restore Action Work? on page 123 . Note: A restore action cannot be assigned to a COVR.
Run command	A run command action executes one or more commands on a changed network device. For more information, see Creating a Run Command Action on page 497 .

How Do I Run an Action?

Running Actions with the Run Actions Feature

If Tripwire Enterprise creates a change version for a monitored object, you can use the **Run Actions feature** to manually run selected actions in response to the change. For example, you can run a severity override action to assign a specified severity level to the change version, or run the Outside Change Window Action to flag the change version as an unauthorized change.

In the Tripwire Enterprise interface, the  **Run Actions** button is available in a variety of locations, including:

- The Node Manager
- Node property dialogs
- Element property dialogs
- Node Manager search tabs (Node Search, Element Search, and Version Search)

For further instructions, see:

- [Running Actions for Specific Elements \(on page 402\)](#)
- [Running Actions for a Node or Node Group \(on page 403\)](#)
- [Restoring a Changed File with the Run Actions Feature \(on page 404\)](#)
- [Restoring Multiple Files with the Run Actions Feature \(on page 405\)](#)

Running Actions with Version Checks

For an introduction to version checks, see [About Version Checks on page 44](#).

To run an action with a version check, you may assign the action to a **rule** or **check rule task**.

- If a rule identifies a changed monitored object during a version check, Tripwire Enterprise executes each of the rule's actions.
- If a check rule task detects one or more changed monitored objects, Tripwire Enterprise runs each of the actions assigned to the task.

Note If an action is assigned to a rule used in a check rule task, the action will only run if that rule identifies a changed element. If changed elements are only identified by other rules, the action is not run.
--

How Does an Action Group Work?

In the Action Manager, you can create multiple action groups to organize your actions. You can then assign an action group to rules and check rule tasks. If an action group runs in response to a detected change, Tripwire Enterprise executes the group's actions in the order specified by the group. For example, an action group might run an e-mail action followed by a run task action.

- To modify the order in which a group's actions will be executed, see [Changing the Properties of an Action Group on page 487](#).
- For more information about groups, see [About Groups on page 29](#).

How Does an E-mail Action Work?

When changes are detected by a version check, an e-mail action sends a single e-mail notification to specified recipients. Tripwire Enterprise includes two types of e-mail notifications.

- **Summary e-mails.** A summary e-mail consists solely of a subject line that indicates:
 - a. The number of changes detected
 - b. The node for which a change was detected (or the total number of changed nodes)
 - c. The rule that identified a changed monitored object (or the total number of rules that identified changes)
- **Detailed e-mails.** In addition to a subject line, a detailed e-mail includes further information about each detected change. The content of a detailed e-mail depends upon the type of rule that identified each change.

For more information, see [Creating an E-mail Action on page 492](#).

How Does an Execution Action Work?

An execution action spawns a sub-process that runs a user-specified command. The specified command can invoke either binary executables or shell scripts.

- If an execution action runs in response to changes detected in a **network device**, the sub-process runs on the TE Server.
- If an execution action runs in response to changes detected in a **file system, database, or directory server**, the sub-process can run on either the TE Server or the responsible Agent system.

Note If you have implemented whitelists on Agent nodes, the command specified in an execution action must exactly match a command in a whitelist file. For more information, see [Restricting Commands on Agent Nodes with Whitelists on page 424](#).

As needed, variables may also be used to pass relevant information about the changes detected by a version check. For security purposes, Tripwire Enterprise automatically discards output and logs errors generated during initiation of a sub-process. For more information, see [Creating an Execution Action on page 493](#).

Caution Before assigning an execution action to a rule or check rule task, you should first verify that the action's commands are compatible with the types of monitored systems to be checked by the rule or task.

How Does the Outside Change Window Action Work?

A **change window**, or **maintenance window**, is a period of time when changes to a monitored system are permitted. When a change window is enforced, any system modification that occurs outside of the window is unauthorized. For example, if the change window for a router is 2AM to 4AM daily, only changes made between 2AM and 4AM are permitted.

A change window may be defined for one or more systems on a network. While change windows are determined by your organization, TE can assist with their enforcement. With the **Outside Change Window Action**, TE automatically flags element versions created outside of a change window.

Note The Outside Change Window Action is automatically created when Tripwire Enterprise is installed and cannot be deleted.

To apply the Outside Change Window Action to a monitored system, complete the following steps:

1. Create a new check rule task (**Task A**), and assign the following items to the task:
 - The node that represents the monitored system
 - All rules used to detect changes on the monitored system
 - The Outside Change Window Action

Then, schedule the task to run at the **beginning** of the change window. For further instructions, see [Creating a Check Rule Task on page 518](#).

2. Create another check rule task (**Task B**), and assign the same node and rules that you assigned to Task A. Then, schedule Task B to run at the **close** (or end) of the change window.

Caution Do **not** assign the Outside Change Window Action to Task B.

To illustrate how the Outside Change Window Action works, assume that the change window extends from 11PM to 2AM daily. Therefore, Task A is scheduled for 11PM, while Task B runs at 2AM.

Since the same node and rules are assigned to Task A and Task B, both tasks scan the same monitored objects for change. However, Task A detects all changes made to those objects since Task B was last run (in other words, between the hours of 2AM and 11PM). Since the Outside Change Window Action is assigned to Task A, Tripwire Enterprise will flag each element version created by this task as an **unauthorized change** that occurred outside of the change window.

Tip To review the authorized and unauthorized changes identified by the Outside Change Window Action, you can run a Change Window Report. For more information on reports, see [What are Reports and Report Types? on page 172](#).

How Does a Restore Action Work?

If a version check is run with a restore action, and a change is detected in a monitored file on a network device, the restore action automatically returns the file to the state of its current baseline. In other words, restore actions are used to maintain the monitored system in a known-and-trusted state.

In Tripwire Enterprise, a restore action may be created for most network devices. However, monitored objects on Nokia devices, HP ProCurve XL devices, and Cisco VPN devices *cannot* be restored.

- To create a restore action, see [Creating a Restore Action on page 496](#).
- To restore network devices at your own discretion, you should run restore actions with the Node Manager Run Actions function. For more information, see [Restoring a Changed File with the Run Actions Feature \(on page 404\)](#) and [Restoring Multiple Files with the Run Actions Feature \(on page 405\)](#).

How Does a Run Rule Action Work?

To create a run rule action, you assign a single rule or rule group to the action. If you then run the action with a version check that detects changes, the action may trigger a **second version check** in response. In this case, TE uses the action's rules to run the second version check.

- If the run rule action was assigned to a **check rule task**, TE checks all monitored systems for which the task detected changes.
- If the run rule action was assigned to a **rule**, Tripwire Enterprise only checks a monitored system if the rule identified a changed element for the system during the initial version check.

For more information, see:

- [About Version Checks \(on page 44\)](#)
- [Creating a Run Rule Action \(on page 498\)](#)

How Does a Set Custom Value Action Work?

Note For an introduction to custom properties, see [What are Custom Properties?](#) on page 197.

If one or more change versions are created by a version check, a set custom value action assigns a custom property value to Tripwire Enterprise objects. Specifically, this action can do one of the following:

- In the properties of each node that represents a changed monitored system, the action can assign a specified value for a single **node custom property**.
- In the properties of each element that represents a changed monitored object, the action can assign a specified value for a single **element custom property**.
- In the properties of each change version, the action can assign a specified value for a single **version custom property**.

To create a set custom value action, see [Creating a Set Custom Value Action](#) on page 499.

For an example involving the use of a set custom value action, see [Example: Using Custom Properties](#) on page 199.

How Does an SNMP Action Work?

When change versions are created by a version check, an SNMP action sends one or more SNMP traps to a trap receiver, such as an Enterprise Management System (EMS). An SNMP action can either send:

- A single trap for **each change version** created by the version check. In this case, the trap includes the version's severity level and change type (addition, modification, or removal), along with the name of the rule that identified the changed object.
- A trap for **each rule** that identified changed objects. In this case, the trap includes the total number of changed objects identified by the rule, the highest severity level assigned to the resulting change versions, and the total number for each type of change version (additions, modifications, and removals).

For more information, see [Creating an SNMP Action](#) on page 500.

How Does a Conditional Action Work?

A conditional action runs one response if a detected change meets specified conditions, **or** a different response if the conditions are not met. In each case, the response could be an action group, an action, or no action at all.

A **conditional response** is the response of a conditional action if its specified conditions are satisfied. For each type of conditional action, [Table 38](#) describes the conditions that trigger the action's conditional response.

Table 38. Types of conditional actions

Conditional Action Type	This action initiates its conditional response if a new change version ...
Attributes	... has attributes specified by the conditional action. (For an introduction to attributes, see What Does Tripwire Enterprise Monitor? on page 37.)
Audit Trail	... generates a TE log message (category = Audit Event) containing specified user, message, and date criteria.
By-Match	... represents a monitored object identified by a matching strategy and match file provided by the conditional action. (For more information about matching strategies and match files, see What is the By-Match Selection Method? on page 73.)
By-Reference	... has a hash that matches the hash of a current baseline associated with a reference node specified by the conditional action.
By-Reference Attributes	... has specified attribute values that match the values for a current version of an element associated with a reference node specified by the conditional action.
Change Type	... represents a monitored object that has been added, modified, and/or removed.
Content	... represents a file and has content specified by the conditional action.
Custom Properties	... has a custom property specified by the conditional action. or ... is associated with a node or element that has a custom property specified by the conditional action.
Element Name	... represents an element with a name that satisfies criteria defined by the conditional action.
Package	... represents a file or directory in a software-installation package specified by the conditional action.
Policy Test Result	... passes all applicable policy tests in one or more TE policies specified by the conditional action.
Severity Range	... has a severity level that falls within a severity range defined by the conditional action.

Conditional Action Type	This action initiates its conditional response if a new change version ...
Tag	... is associated with a node that has tags defined by the conditional action. or ... is associated with a node in a saved filter defined by the conditional action.
Time Range	... was created within a time window(s) specified by the conditional action.

For example, when you create a **severity range conditional action**, you define a single severity range. The severity range determines how Tripwire Enterprise responds to a change version created by a version check run with the action.

- If the change version has a severity level that falls **within** the specified range, Tripwire Enterprise responds by initiating its conditional response. The conditional response can either be an action group, a single action, or no action.
- If the change version's severity level falls **outside of** the specified range, Tripwire Enterprise initiates the other response defined for the conditional action (either an action group, a single action, or no action).

For more sophisticated responses, you can 'nest' multiple conditional actions. For example, you might create the severity range conditional actions in [Table 39 below](#), and then assign **Conditional Action A** to a check rule task. If the task creates a new change version, the version's severity level determines the response of Conditional Action A.

- If the severity level falls between 0 and 5999, no action is taken.
- If the severity level falls between 6000 and 10,000, Tripwire Enterprise runs **Conditional Action B**. In this case, if the severity level is between 8000 and 10,000, Tripwire Enterprise runs an **SNMP action**. Otherwise, the application runs an **e-mail action**.

To create a conditional action, see [Creating a Conditional Action on page 491](#). (For another example involving the use of a conditional action, see [Example: Using Custom Properties on page 199](#).)

Note Policy test result conditional actions cannot be nested.

Table 39. Example of nested severity range conditional actions

Severity Range Conditional Action	Severity Range	Responses
Conditional Action A	6000 to 10,000	Within range=Run Conditional Action B Outside range=No action taken
Conditional Action B	8000 to 10,000	Within range=Run SNMP action Outside range=Run e-mail action

About Tasks

What are Task Types?

A **task** is a Tripwire Enterprise object that performs an operation. In Tripwire Enterprise, you can run tasks on a manual or scheduled basis. When you schedule a task, you specify the dates and times when the task will automatically run. (To schedule a task, see [Changing the Properties of a Task on page 512](#)). [Table 40](#) defines each type of task that can be run in Tripwire Enterprise.

Tips In the Root Group of the Task Manager, you can create task groups to organize the tasks in your TE implementation. For more information, see [About Groups on page 29](#).

At any time, you can stop a running baseline rule task or check rule task with the **Stop** button in the Task Manager. For further details, see [Stopping Tasks and Task Groups Manually on page 523](#).

Table 40. Types of tasks

Task Type	Definition
Archive Log Messages task	This task archives all TE log messages that exceed a specified age or number. For more information, see How Does the Archive Log Messages Task Work? on page 170 . Note: TE log messages in the Audit Event, RADIUS, and TACACS+ categories (see Table 47 on page 167) are not archived.
Baseline rule tasks	A baseline rule task runs a baseline operation on one or more monitored systems. For more information, see How Does a Baseline Rule Task Work? on the next page . Note: Rule task is a term that refers to both baseline rule tasks and check rule tasks.
Check rule tasks	A check rule task runs a version check of one or more monitored systems. For more information, see How Does a Check Rule Task Work? on page 129 .
Compact Element Versions task	This task removes all content and attributes from element versions that exceed a specified age or number. You can also configure the task to archive any Audit Event, RADIUS, and TACACS+ TE log messages (see Table 47 on page 167) that identify any element versions removed by the task. For more information, see How Does the Compact Element Versions Task Work? on page 130 .
Configure Axon Agents task	This task updates the audit event collection and real-time monitoring configurations for Event Generators on Axon Agents. For more information, see What is Audit Event Collection? (on page 63) and How Does Real-Time Monitoring Work? (on page 70) . By default, this task runs every day at midnight. The TE Console status bar displays the last time that the Configure Axon Agents task ran (either manually or as a scheduled task).
Clear Unlinked Groups task	This task permanently deletes all objects in all of the Unlinked groups in Tripwire Enterprise. This task can also be run manually when deleting or unlinking objects.
Report tasks	A report task generates output for a single report or dashboard . For more information, see How Does a Report Task Work? on page 186 .

How Does a Baseline Rule Task Work?

A baseline rule task baselines the monitored objects identified by the nodes and rules assigned to the task. For an introduction to baselining, see [About Baselines on page 43](#).

Each monitored object is identified by a **node/rule pair**, which consists of a single node and a single rule. For a baseline rule task to successfully baseline a monitored object identified by a node/rule pair, the following permissions must be assigned to the effective user role of the user who created the task:

- For the node, the user must have the **Element Management > Update** permission.
- For the rule, the user must have the **Rule Management > Use** permission.

For more information about user permissions and effective user roles, see:

- [What is an Effective User Role? \(on page 207\)](#)
- [What are User Permissions and User Roles? \(on page 204\)](#)

If you have the default Administrator user account, or a user account with the default Administrator user role, you can designate another user account as the creator of a baseline rule task. In this case, the task will only baseline a monitored object if the designated user account has an effective user role with the required permissions cited above.

When configuring a baseline rule task, you can specify whether the task should create baselines for all elements, or only for those elements that don't have element versions.

To create a baseline rule task, see [Creating a Baseline Rule Task on page 517](#).

How Does a Check Rule Task Work?

A check rule task runs a version check of the monitored objects identified by the nodes and rules assigned to the task. For an introduction to version checking, see [About Version Checks on page 44](#)

Each monitored object is identified by a **node/rule pair**, which consists of a single node and a single rule. For a check rule task to successfully check a monitored object identified by a node/rule pair, the following permissions must be assigned to the effective user role of the user who created the task:

- For the node, the user must have the **Element Management > Check** permission.
- For the rule, the user must have the **Rule Management > Use** permission.

For more information about user permissions and effective user roles, see:

- [What is an Effective User Role? \(on page 207\)](#)
- [What are User Permissions and User Roles? \(on page 204\)](#)

If you have the default Administrator user account, or a user account with the default Administrator user role, you can designate another user account as the creator of a check rule task. In this case, the task will only check a monitored object if the designated user account has an effective user role with the required permissions cited above.

To create a check rule task, see [Creating a Check Rule Task on page 518](#).

How Does the Compact Element Versions Task Work?

To reduce the amount of element version data in your Tripwire Enterprise implementation, you may run the **Compact Element Versions Task** in the Task Manager. Automatically created when Tripwire Enterprise is installed, this task removes all content and attributes from element versions that exceed a specified age or number. In addition, you may configure the task to archive TE log messages in the Audit Event, RADIUS, and TACACS+ categories.

As needed, you can modify the following properties of the Compact Element Versions Task:

- **Limited to older than.** With this setting, you instruct Tripwire Enterprise to compact all element versions older than a specified number of days. By default, element versions created more than 365 days ago are compacted, while those created within the last 365 days are not.
- **Limited to oldest exceeding.** This setting establishes the maximum number of element versions that will remain incompact. By default, Tripwire Enterprise compacts all versions of an element in excess of 100.
- **Archive and remove corresponding audit events.** If enabled, this setting will archive any Audit Event, RADIUS, and TACACS+ log messages that identify element versions compacted by the task. To do so, TE exports the log messages to compressed XML files in a zip file in:

```
<te_root>\Server\data\log\directory
```

Tripwire Enterprise applies the following naming convention to zipped log message files:

```
<yyyy>-<mm>-<dd>-audit-archive-X.zip
```

where

<yyyy> is the current year,

<mm> is the current month,

<dd> is the current date, and

X is a numeric counter of archive files for each date. X begins at zero and increases by one digit for each archive file created on the same day. For example, if you ran the task three times on November 7, 2009, the following archive files would be created:

```
2009-11-07-audit-archive-0.zip
2009-11-07-audit-archive-1.zip
2009-11-07-audit-archive-2.zip
```

To change the settings for your Compact Element Versions Task, see [Changing the Properties of a Task on page 512](#). As with other tasks, the Compact Element Versions Task may be run on a manual or scheduled basis.

- To run the task manually, see [Running Tasks and Task Groups Manually on page 523](#).
- To schedule the task for automatic execution, see [Changing the Properties of a Task on page 512](#).

About Policies and Compliance

What are Policy Manager Objects?

A **policy** is a collection of standards with which monitored systems on your organization's network must conform; for example, a federal regulation or internal guidelines. To measure the compliance of your monitored systems with a policy, you can create objects in the Policy Manager. **Policy Manager objects** are TE policies, policy tests, and policy test groups.

A **TE policy** determines if monitored systems satisfy all requirements of a policy. To assess conformance with policy requirements, you add policy tests to a TE policy. A **policy test** determines if the current versions of specified monitored objects comply with a specific requirement of a policy.

For example, a policy might assess the degree to which Windows domain servers comply with a set of security standards. In this case, the corresponding TE policy would contain policy tests that monitor specific security requirements for the servers; for instance, a policy test might require a minimum of 6 characters for all user account passwords used with monitored Windows domain servers.

In the Policy Manager, you can organize TE policies and policy tests in **policy test groups** (see [About Groups on page 29](#)). A policy test group may contain TE policies, policy tests, and other policy test groups.

A TE policy can also contain policy tests and policy test groups. A TE policy that contains a policy test is known as a **parent policy** of the test, and a single policy test can be linked under multiple parent policies. However, a TE policy can not contain another TE policy.

Note The Tripwire Web site provides a collection of TE policies and policy tests configured by Tripwire to evaluate system compliance with common industry standards. If you download the XML files containing these pre-configured TE policies and policy tests from the Web site, you can import these objects to the Policy Manager. For more information, see [What are Pre-Configured Rules and Policies? on page 219](#).

When you create a new policy test, you define the properties of the test, including:

- The **effective scope** of the test, which determines the nodes and elements for which the test will run. For further details about effective scopes, see [What are Scopes and Effective Scopes? on page 133](#).
- The **pass/fail criteria** for the test, which determine if the current versions of elements in the test's effective scope comply with the policy requirement evaluated by the test. [Table 41](#) describes the pass/fail criteria for each type of policy test.

Table 41. Types of policy tests

Policy Test Type	Pass/Fail criteria based on ...
Attribute test	... change-version attribute values specified by one or more conditions.
Content test	... change-version content specified by one or more conditions. This type of test can be run on any change version that represents: <ul style="list-style-type: none">• A file• Command output• An RSoP report• Database query results
Windows ACL test	... change-version attribute values for the DACL or SACL of: <ul style="list-style-type: none">• Files and directories in a Windows file system• Keys in a Windows registry

About Severity Levels and Policy Tests

A severity level is defined in the properties of each policy test. Ranging from 1 (least important) to 10,000 (most important), the severity level indicates the relative importance of the policy requirement evaluated by the test. Zero (0) indicates a policy requirement without an associated level of importance.

With the Test Severity Range criterion, you can limit the output of some reports to policy tests that have severity levels within a specified range. For more information, see [Changing the Properties of a Report on page 589](#).

What are Scopes and Effective Scopes?

Each TE policy and policy test has a **scope**. For a **TE policy**, the scope identifies all of the nodes for which the policy's tests may be run. The policy tests in a TE policy will only be run on elements of nodes specified by the TE policy's scope. If no nodes are specified by the scope properties of a TE policy, the policy's tests will not run on any elements.

- [Table 42](#) identifies the properties of a TE policy that may specify nodes for the policy's scope, as well as the associated tab in the TE policy's properties dialog.
- To view or modify the scope properties of a TE policy, see [Changing the Properties of a TE Policy on page 534](#).

For a **policy test**, the scope specifies elements for which the test may be run, and may limit the test to one or more nodes.

- [Table 43 \(on the next page\)](#) identifies the properties that determine the scope of a policy test, as well as the associated tab in the test's properties dialog.
- To view or modify the properties of a policy test, see [Changing the Properties of a Policy Test on page 536](#).

Note By default, the scope of each pre-configured TE policy does not specify any nodes. To run the policy's tests, you must specify nodes with the policy's scope properties. For more information about pre-configured TE policies, see [What are Pre-Configured Rules and Policies? on page 219](#).

Table 42. Properties defining the scope of a TE policy

Properties	Defined in	Description
Nodes	Nodes tab	(Optional) Specifies nodes and/or node groups to be included in the scope of the policy.
Node names	Node Names tab	(Optional) Specifies a string in the names of nodes to be included in or excluded from the scope of the policy.
Node custom property conditions	Node Properties tab	(Optional) Defines conditions that specify the values of node custom properties. If any conditions are defined, the policy's scope is limited to nodes with custom properties that have the specified values.

Table 43. Properties defining the scope of a policy test

Properties	Defined in	Description
Element names	Scope tab	Specifies a string in the names of elements to be included in or excluded from the scope of the policy test.
Excluded nodes	Excluded Nodes tab	(Optional) Specifies nodes and/or node groups to be excluded from the scope of the policy test.
Node custom property conditions	Included Node Properties tab	(Optional) Defines conditions that specify the values of node custom properties. If any conditions are defined, the policy test's scope is limited to nodes with custom properties that have the specified values.
Rules	Rules tab	Specifies one or more rules. The policy test's scope is limited to elements that represent monitored objects identified by one of the rules.

The **effective scope** of a policy test consists of all elements for which TE will actually run the test. To determine the effective scope of a policy test, TE considers the scope of the test itself, as well as any TE policies from which the test is descended. Specifically, an element only falls within the effective scope of a policy test if all of the following conditions are true:

1. If the test has one or more parent policies, the scope of at least one of the parent policies must include the element's node.
2. The scope of the policy test must include the element's node.
3. The scope of the policy test must include a rule that identifies the monitored object represented by the element.
4. The scope of the policy test must include the name of the element.

Tip To simplify the management of scopes, Tripwire recommends that you avoid specifying nodes in the scopes of individual policy tests.

How Does a Policy Test Work?

Once the effective scope and pass/fail criteria have been defined for a new policy test, you should run the test manually in the Policy Manager. You can either run the test alone, or run all tests in a new parent policy or test group at the same time (see [Running Policy Tests Manually on page 561](#)).

When a policy test runs for the first time, Tripwire Enterprise:

1. Compares the current version of each element identified by the test's effective scope with the pass/fail criteria defined by the test (see [Table 41 on page 132](#)).
2. Generates a **policy test result** for each current version, which indicates if the version passed or failed the test. If the current version complies with the pass/fail criteria defined by the test, the element passes the test.

Note A node is in full compliance with a TE policy when its monitored elements have passed all of the policy's tests.

3. Calculates **compliance statistics** for each node in the test's effective scope, as well as each parent policy of the test. For further details, see [How Do I Monitor Compliance Statistics? on page 137](#).

From this point on, Tripwire Enterprise automatically runs the policy test whenever a version check results in the creation of change versions for elements in the effective scope of the test

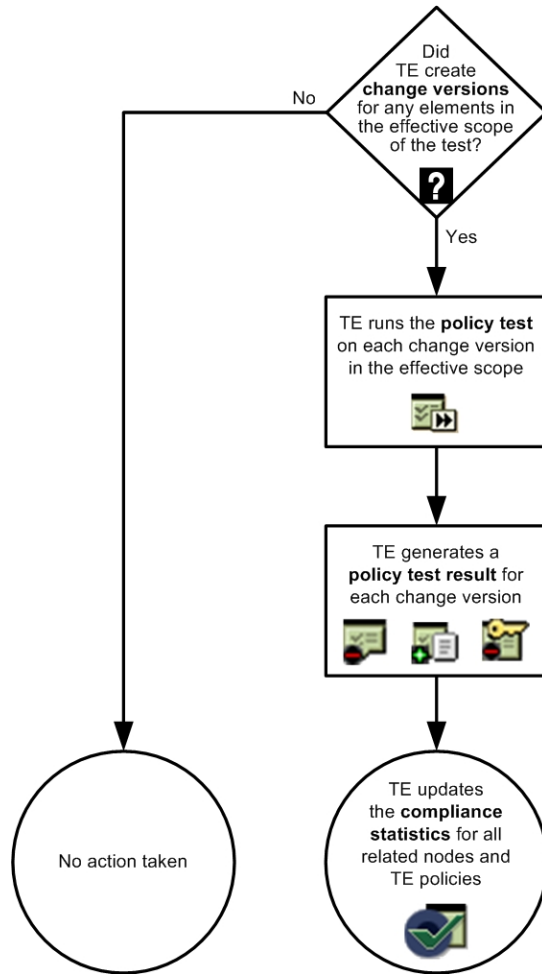
Tip In the Policy Manager, you can manually run a policy or policy test at any time. However, Tripwire only recommends doing so in the following cases:

1. When you create or import a new policy test.
2. If you change the properties of a policy test(s) and want to update the related compliance scores.
3. If you initially baseline a node covered by the effective scope of a policy test.

When a version check creates one or more change versions for elements in the effective scope of a policy test, TE runs the test and takes the following steps (see [Figure 11](#)):

1. Compares each change version with the pass/fail criteria defined by the test (see [Table 41 on page 132](#)).
2. Generates a **policy test result** for each change version, which indicates if the version passed or failed the test. If the version complies with the pass/fail criteria defined by the test, the element passes the test.
3. Updates the **compliance statistics** for each node in the test's effective scope, as well as each parent policy of the test. For further details, see [How Do I Monitor Compliance Statistics? on page 137](#).

Figure 11. A policy test run in response to a version check



How Do I Monitor Compliance Statistics?

Compliance statistics assess the conformance of nodes and elements with your organization's policies. Whenever a policy test runs, Tripwire Enterprise creates a policy test result for each of the elements in the effective scope of the test. Upon completion of the test, TE re-calculates and updates the compliance statistics in the Policy Manager.

Note To calculate compliance statistics, TE uses only the latest test results generated by each policy test.

To assess the conformance of nodes and elements with your organization's policies, you can review compliance statistics in the Policy Manager and Report Manager. In the Policy Manager, Tripwire Enterprise presents compliance statistics in the Compliance tab. For details, see [Viewing Policy Manager Objects in the Compliance Tab on page 550](#).

In the Report Manager, you can monitor compliance statistics with the following reports:

- Compliance History
- Test Result Summary
- Scoring
- Scoring History

For more information, see [What are Reports and Report Types? on page 172](#).

What are Policy Scores?

A **policy score** is a percentage measurement indicating the overall conformance of a node with the policy tests in a TE policy. To calculate a policy score for a node, Tripwire Enterprise evaluates the latest test results for all of the TE policy's tests run on the node's elements. A policy score of 0% indicates that the node has no elements that satisfied the pass/fail criteria of the TE policy's tests, while a score of 100% indicates that all of the node's elements complied with the pass/fail criteria. For further details, see [How Does Tripwire Enterprise Calculate a Policy Score? on the next page](#).

As needed, you can fine tune the calculation of policy scores by applying waivers and weights to a TE policy. A **waiver** is a property of a TE policy that overrides failed policy test results when TE calculates a policy score for the policy. Each waiver specifies one or more test/node pairs. A **test/node pair** consists of a single policy test and a single node in the scope of the TE policy. When calculating a policy score for a node identified by a test/node pair in a waiver, TE automatically evaluates the associated test result as 'passing.' In other words, even if the node failed the most recent run of the policy test, TE treats the result as a 'passing' value for the policy score calculation.

Tip In the properties of a waiver, you can set an expiration date. When the expiration date passes, TE stops overriding failed policy test results for the test/node pairs specified by the waiver.

In the properties of a TE policy or policy test group, **weights** indicate the relative importance of the Policy Manager objects on the top level of the object's group hierarchy. For instance, if the top level of a TE policy consists of two policy test groups and three policy tests, you can adjust the weights for these five objects in the properties of the TE policy.

Weights range from a value of 1 (least important) to 10 (most important). When you add a Policy Manager object to the top level of a TE policy or policy test group, TE assigns the object a weight of 1. To change this default value, you must modify the weight in the object's properties dialog.

- To adjust the weights for a TE policy, see [Changing the Properties of a TE Policy on page 534](#).
- To adjust the weights for a policy test group, see [Changing the Properties of a Policy Test Group on page 538](#).
- To add a waiver to a TE policy, see [Creating a Waiver on page 564](#).

How Does Tripwire Enterprise Calculate a Policy Score?

When a policy test runs, TE generates a policy test result for each element in the effective scope of the test. If the effective scope identifies multiple elements for a single node, then the test will create multiple policy test results for the node.

To calculate a policy score for a node, Tripwire Enterprise first determines which tests in the specified TE policy have generated results for the node's elements. TE then assigns a **pass/fail score** for each of those results.

- If the latest policy test result for an element passed, or the associated test/node pair has a waiver, then the test result receives a pass/fail score of 1 (one).
- If the latest result failed, and a waiver does not exist for the associated test/node pair, then the test result receives a pass/fail score of 0 (zero).

Next, TE calculates a **weighted score** for each of the policy test groups on the lowest level of the TE policy's group hierarchy. To calculate a weighted score for a policy test group, TE applies the following algorithm:

$$\text{Weighted score} = \frac{(S1 \times W1) + (S2 \times W2) + \dots}{W1 + W2 + \dots}$$

where:

S# = The score for one of the Policy Manager objects on the top level of the group's hierarchy; either the pass/fail score of a policy test result (0 or 1), or the weighted score of a policy test group.

W# = The weight assigned by the policy test group to a Policy Manager object on the top level of the group's hierarchy.

Once the weighted score has been calculated for each of the lowest policy test groups, TE uses the weighted score algorithm to calculate the score for each group on the next level of the group hierarchy. This process continues until TE has a weighted score for every Policy Manager object on the top level of the TE policy's group hierarchy. At this point, TE runs the weighted score algorithm one last time to determine the policy score for the node. (The policy score is simply the weighted score for the TE policy.)

Example: Calculating a Policy Score for a Node

Figure 12 on the next page illustrates a simple group hierarchy for a TE policy. For each object in the hierarchy, Figure 12 also shows the data employed by TE to calculate the policy score for a hypothetical node.

In this example, only one of the node's elements is in the effective scope of each policy test in the TE policy. Therefore, each policy test has only a single policy test result involved in the calculation of the policy score.

To calculate the policy score, TE takes the following steps:

1. For each policy test in the TE policy, TE assigns the appropriate pass/fail score for the most recent policy test result generated by the test.
 - Since the element tested by **Policy Test A** failed, and the test lacks a waiver, TE assigns a pass/fail score of zero (0).
 - Since the elements tested by **Policy Test B** and **Policy Test C** passed, TE assigns a pass/fail score of one (1).
 - Since the element tested by **Policy Test D** failed, but the TE policy has a waiver that specifies the node and Policy Test D in a test/node pair, TE assigns a pass/fail score of one (1).
2. In the properties of Policy Test Group 1, the following weights are assigned to the three policy tests in the group:

Weight of Policy Test A = 8

Weight of Policy Test B = 10

Weight of Policy Test C = 2

With the pass/fail scores and weights of each policy test in Policy Test Group 1, Tripwire Enterprise now calculates the group's **weighted score**:

$$\frac{(0 \times 8) + (1 \times 10) + (1 \times 2)}{8 + 10 + 2} = \frac{12}{20} = .60$$

3. In the properties of the TE policy, the following weights are assigned to the two objects on the top level of the policy:

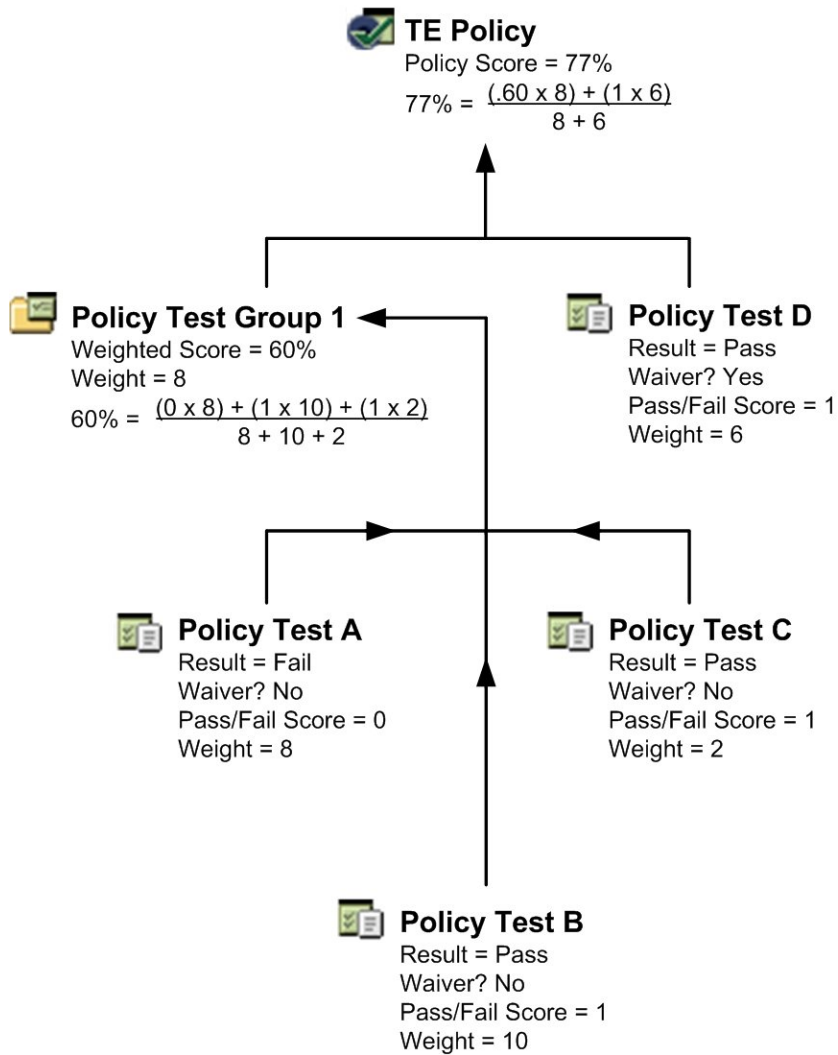
Weight of Policy Test Group 1 = 8

Weight of Policy Test D = 6

Having determined the pass/fail score of Policy Test D, and the weighted score of Policy Test Group 1, Tripwire Enterprise is now prepared to calculate the **policy score** for the node. To do so, TE applies the weighted score algorithm with the following values:

$$\frac{(.60 \times 8) + (1 \times 6)}{8 + 6} = \frac{10.8}{14} = .77$$

Figure 12. Example group hierarchy for a policy score calculation



What are Scoring Thresholds?

A **scoring threshold** is a property of a TE policy that specifies a color and a policy score value from 0 to 100 (see [What are Policy Scores? on page 138](#)). By defining scoring thresholds for a TE policy, you create a relative scale to assess the values of policy scores and the compliance status of nodes in the TE policy's scope.

When you create a new TE policy, Tripwire Enterprise adds two scoring thresholds to the policy by default:

- The **Passing** threshold has a default value of 100. To establish a more lenient standard for 'passing' scores, a lesser value may be entered for this threshold.
- The **Failing** threshold has a static value of 0 (zero).

As needed, you can create additional scoring thresholds for any TE policy.

A color is assigned to each scoring threshold in a TE policy. When you review the policy's Node Scores chart in the Compliance tab (see [Figure 34 on page 553](#)), the color provides a visual cue for the percentage of nodes with current policy scores that exceed the threshold.

Example: Using Scoring Thresholds

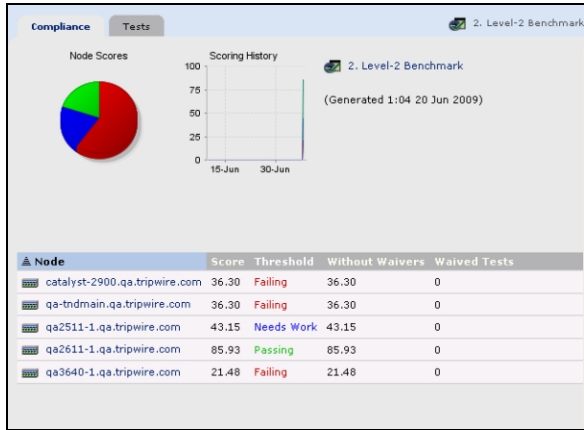
Consider a TE policy with the scoring thresholds defined in [Table 44 \(below\)](#). In the Compliance tab for the TE policy (see [Figure 13 on the next page](#)), the Node Scores chart indicates the percentage of nodes with a current policy score that exceeds each of the thresholds. For example, the blue shading indicates the number of nodes with scores that surpassed the Needs Work threshold, but fell short of the Passing threshold. (These nodes have policy scores between 40 and 79.)

To add a scoring threshold to an existing TE policy, see [Creating a Scoring Threshold for a TE Policy on page 555](#).

Table 44. Example of scoring thresholds

Threshold Name	Score	Color	This threshold indicates ...
Passing	80	Green	... nodes that are in compliance with enough of the TE policy's requirements to be considered 'passing.'
Needs Work	40	Blue	... nodes that are close to achieving the Passing threshold, but still need some work.
Failing	0	Red	... nodes that do not comply with enough of the TE policy's requirements.

Figure 13. Example of scoring thresholds in the Compliance tab

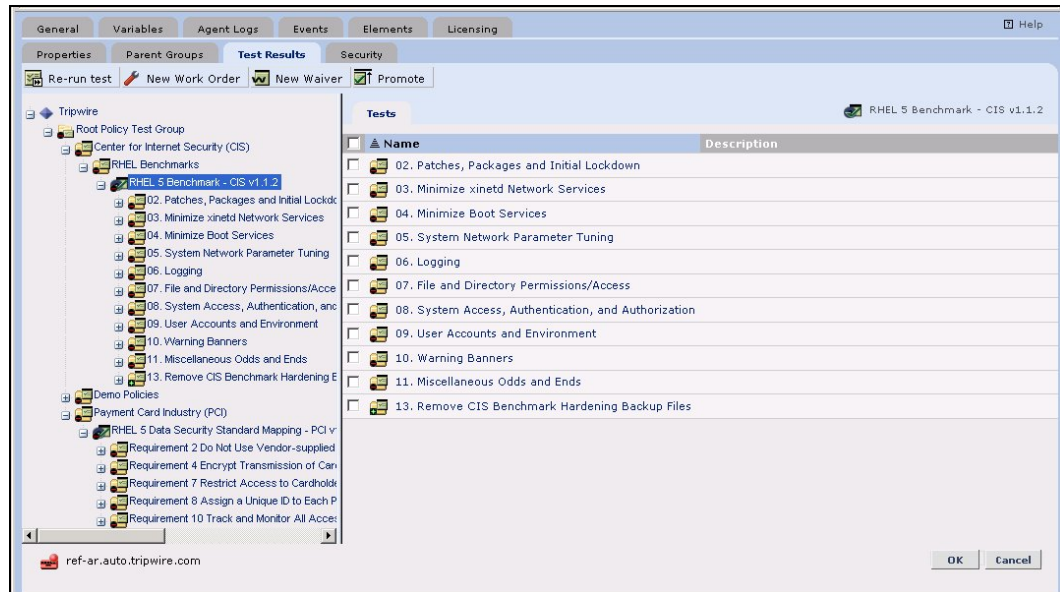


How Do I Review the Results of Policy Tests?

When a policy test runs on a node, TE generates a policy test result for each element in the effective scope of the test. To review the policy test results for a node, open the node's properties dialog and select the **Test Results** tab (see [Figure 14](#)).

Note To open a node properties dialog, see [Changing the Properties of a Node \(on page 321\)](#) or [Viewing Policy Test Results from the Compliance Tab \(on page 554\)](#).

Figure 14. Test Results tab in node properties dialog



In the Test Results tab, a **test result indicator** overlays the icon of each policy test result and Policy Manager object. When applied to a **TE policy** or **policy test group**, a test result indicator signifies the following:



A green + means that the TE policy or group contains policy tests that generated only passing results for the node on their last run.



A red - means that the TE policy or group contains at least one policy test that generated a failing result for the node on its last run.



A white circle means that the TE policy or group contains no policy tests that have generated results for the node.

When applied to a **policy test**, a test result indicator signifies the following:



A green + means that all of the node's elements in the test's effective scope passed the last run of the test.



A red - means at least one of the node's elements failed the last run of the test.



A white circle means the test has not generated any results for the node.

Tip To view the pass/fail criteria of a policy test, select the test in the **Name** column of the Test Results tab. Then, select the **Conditions** tab in the policy test properties dialog.

If you select a policy test in the tree pane of the Test Results tab, TE presents the latest results that have been generated for the node's elements by the test in the main pane. When applied to a **policy test result**, an indicator signifies if the tested element passed or failed the test.



A green + means the element passed the test.



A red - means the element failed.

To open a properties dialog for a test result, select the result's link in the main pane. For further details, see [Viewing Policy Test Results from the Compliance Tab on page 554](#).

In the Report Manager, you can run a number of reports to compile data on policy tests and test results. For more information, see [What are Reports and Report Types? on page 172](#).

How Do I Purge Policy Data from Tripwire Enterprise?

Policy test results and waivers can consume a significant amount of space in your Tripwire Enterprise Console database. To minimize this problem, you can have TE automatically purge (delete) this data for a TE policy. If you enable purging in the properties of a TE policy, you also enter a specified number of days. Thereafter, TE will automatically delete the following data for the TE policy:

- Policy test results older than the specified number of days.
- Waivers that have been expired or closed for more the specified number of days.

To configure purging for a TE policy, open the policy's properties dialog and select the **Purge Settings** tab. For further details, see [Changing the Properties of a TE Policy on page 534](#).

What is Policy Test Promotion?

With the Promote feature in the Policy Manager, you can modify the pass/fail criteria of one or more specified policy tests at the same time. To adjust the pass/fail conditions for a test, you can either:

- **Promote** the value(s) in the latest result generated by the policy test. With promotion, TE replaces the test's existing pass/fail conditions with a new condition(s) that only specifies the value(s) in the test result.
- **Expand** the pass/fail conditions by adding a new condition(s) that specifies the value(s) of the test result.
- **Customize** the test's existing pass/fail conditions. With customization, you can add, change, and delete conditions however you like.

To modify the pass/fail conditions of multiple policy tests, see:

- [Promoting Policy Test Results \(on page 562\)](#)
- [Promoting Policy Test Results Generated for a Node \(on page 337\)](#)

Example: Enforcing a 'Golden Build' with Policy Test Promotion

Betty, the system administrator for NapSys, Inc., has carefully configured an IIS server in accordance with her company's Windows domain policy, which is based on the CIS Benchmark for IIS 6.0 on Windows Server 2003 (v. 1.0). The **NapSys policy** defines a set of standards for security settings and parameters on IIS servers. Betty intends to use the configured IIS server as a “**Golden Server**” against which other IIS servers may be measured.

Recently, Betty learned that Tripwire provides a pre-configured TE policy that enforces the requirements specified by the CIS benchmark. To monitor the compliance of IIS servers with the Napsys policy, Betty decides to adapt the pre-configured TE policy to the requirements of the NapSys policy. To do so, she completes the following steps:

1. First, Betty downloads the XML file containing the pre-configured TE policy from the Tripwire Web site, and imports the file's contents in the Policy Manager (see [What are Pre-Configured Rules and Policies? on page 219](#)).
2. Since Betty intends to modify the pass/fail criteria of some of the TE policy's tests, she creates a copy of the imported TE policy (see [Duplicating Policy Tests on page 548](#)). She names the copy “**NapSys IIS 6.0 Policy**.”
3. Betty runs the NapSys IIS 6.0 Policy on the Golden Server's node (see [Running Policy Tests Manually on page 561](#)).
4. In the Test Results tab of the Golden Server node's properties dialog, Betty reviews the failed test results and makes a note of which test generated each failure (see [How Do I Review the Results of Policy Tests? on page 144](#)). Each failed result identifies a discrepancy between the requirements of the NapSys policy and the requirements of the CIS Benchmark.

5. Since each failure represents a monitored object with content or attributes that satisfy the requirements of the Napsys policy, Betty now promotes all failed test values for the NapSys IIS 6.0 Policy (see [Promoting Policy Test Results on page 562](#)). This step aligns the pass/fail criteria of the NapSys IIS 6.0 Policy with the requirements of NapSys policy.
6. Betty reviews the remediation text in the properties dialog of each policy test that generated a failed result for the Golden Server's node (see [Changing the Properties of a Policy Test on page 536](#)). As needed, Betty edits the text to make it consistent with the requirements of the NapSys policy. For more information about remediation, see [About Remediation on page 151](#).

The NapSys IIS 6.0 Policy is now ready to monitor other IIS servers for compliance with the NapSys policy. To monitor these servers, Betty defines the scopes of the NapSys IIS 6.0 Policy and its descendant policy tests. For more information, see [What are Scopes and Effective Scopes? on page 133](#).

Example: Using TE Policies to Enforce PCI Standards

As the Tripwire administrator for DiFalco Insurance, Robert is responsible for enforcing compliance with Payment Card Industry (PCI) standards. Specifically, the company has 12 e-commerce servers running Windows 2008 Server, and each of these servers must conform with the following requirements in the PCI Data Security Standard:

- Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

To begin, Robert downloads the latest pre-configured Windows 2008 rules, TE policies, and policy tests from the Tripwire Web site. He then imports the rules and policy tests in the Tripwire Enterprise interface. (For more information, see [What are Pre-Configured Rules and Policies? on page 219](#)).

To discuss how Tripwire Enterprise can assist DiFalco Insurance with PCI conformance, Robert schedules a meeting with Becky, the company's Network Security Officer. In the meeting, Robert and Becky review the imported Policy Manager objects ([Viewing Policy Manager Objects in the Tests Tab on page 530](#)). They quickly determine that two policy test groups consist of policy tests designed for requirements 1 and 2 of the PCI Data Security Standard (see [Table 45 below](#) for details).

To begin work, Robert completes the following steps:

1. In the Root Group of the Policy Manager, Robert creates a new TE policy called **PCI E-commerce Tests** ([Creating a TE Policy on page 543](#)).
2. Robert links the policy test groups in [Table 45](#) to the **PCI E-commerce Tests** policy (see [Linking Policy Manager Objects on page 571](#)).

Table 45. Pre-configured policy test groups for PCI requirements

PCI Requirement	Default path and name of corresponding policy test group in Policy Manager
Requirement 1	Payment Card Industry (PCI) Data Security Standard Mapping > Windows 2008 DSS > Build and Maintain a Secure Network > 01 - Install and maintain a firewall configuration to protect cardholder data
Requirement 2	Payment Card Industry (PCI) Data Security Standard Mapping > Windows 2008 DSS > Build and Maintain a Secure Network > 02 - Do not use vendor-supplied defaults for system passwords and other security parameters

During their review of the pre-configured Policy Manager objects, Robert and Becky determined that one of the policy tests does not adhere to the requirements of DiFalco Insurance. Specifically, the test requires a minimum password length of eight (8) characters, while DiFalco Insurance only requires seven (7) characters.

To customize the policy test for use in the PCI E-commerce Tests policy:

1. In the tree pane of the Policy Manager, Robert selects the following sub-group in the PCI E-commerce Tests policy:

- 2.2 Develop configuration standards for ... >
- 2.2.0 Tests >
- 2.2.0.1 Minimum Password Length

2. In the main pane, he selects and duplicates the following policy test (see [Duplicating Policy Tests on page 548](#)):

- Minimum Password Length: >=8

Once done, Tripwire Enterprise creates a duplicate test called:

- Minimum Password Length: >=8 (1)

3. Robert unlinks the original policy test from the PCI E-commerce Tests policy (see [Unlinking Policy Manager Objects on page 572](#)).

4. To configure the duplicate test, Robert completes the following steps in the test's properties dialog (see [Changing the Properties of a Policy Test on page 536](#)):

- a. In the General tab, Robert enters the following values:

- Name** = Minimum Password Length: >=7

- Description** = All passwords are at least 7 characters long (minimum).

- b. In the Conditions tab, he changes the value of the 5th field in the second condition from 8 to 7.

- c. In the Remediation and Remediator tabs, Robert edits any existing remediation content to conform with the revised password-length value, and then clicks **OK** (see [About Remediation on page 151](#)).

Now the policy tests are ready to monitor the e-commerce servers for PCI conformance. To track compliance, Robert and Becky follow the guidelines described in [How Do I Monitor Compliance Statistics? \(on page 137\)](#).

As discussed in [About Remediation \(on page 151\)](#), some pre-configured policy tests contain remediation information provided by Tripwire. To simplify troubleshooting of any future test failures for the PCI E-Commerce Tests TE policy, Robert creates a **Detailed Test Inventory Report** in the Report Manager (see [Creating a Report on page 592](#)). In the report's Criteria tab, Robert completes the following steps:

1. In the General criterion, Robert selects the **Descend Test Groups** check box.
2. In the Test criterion, he adds the PCI E-commerce Tests TE policy.

3. In the remaining criteria, he accepts the default settings.

With these settings, the report will compile a complete list of all policy tests in the PCI E-Commerce Tests TE policy. If remediation information exists in the properties of a policy test, the report output includes this information as well. Consequently, the output serves as a convenient resource for resolving test failures identified by the TE policy. For further details about reports, see [What are Reports and Report Types?](#) on page 172.

About Remediation

Remediation is the process of resolving failures generated by a policy test. Policy tests may be remediated in two ways:

- With **automated remediation**, when a policy test fails on a file server node, the Tripwire Enterprise Agent on that node runs a script or performs other activities to bring the node into compliance with the policy test. The specific actions performed to remediate each policy test are listed in the test's Remediator tab. For more information, see [How Does Automated Remediation Work? below](#)
- With **manual remediation**, a user manually performs the actions required to bring a node into compliance with a policy test. These actions are listed in the test's Remediation tab. For more information, see [What is Manual Remediation? on page 165](#)

Both of these remediation techniques can be used in the same Tripwire Enterprise implementation. For example, you may configure some policy tests to support automated remediation and require others to be manually remediated. Or you may want to limit the use of automated remediation to only some nodes or node groups.

Note Axon Agent does not support automated remediation, so if you want to automate remediation on a file server node, install Tripwire Enterprise Agent on the monitored system instead.

In order to use automated remediation on a node, the node must have a valid Automated Remediation license. For more information, see [About Tripwire Enterprise Licenses \(on page 202\)](#)

How Does Automated Remediation Work?

Tripwire Enterprise manages automated remediation using work orders. A **work order** defines a set of policy test failures to be remediated on specific nodes. Each work order has a unique name in Tripwire Enterprise. In addition, you can assign an Approval ID to a work order, which enables you to identify and track the work order in an external ticketing system. Each work order is made up of one or more remediation entries. A **remediation entry** describes a single policy test failure on a single node.

A user with the appropriate permissions can create a work order from any part of the Tripwire Enterprise interface that displays failed policy tests. Once created, multiple users can view and edit a work order using a remediation work order widget. Using TE user permissions, the TE administrator can control the work orders that a specific user can see, and the actions that a user can perform on a work order. For example, most organizations require that different users approve a remediation and perform the remediation.

The process below describes the basic automated remediation workflow in Tripwire Enterprise. By changing the permission assigned to different users, you can modify this workflow to match your organization's processes. For detailed step-by-step information about configuring TE for automated remediation, see [Implementing Automated Remediation in Tripwire Enterprise on page 155](#).

1. Tripwire Enterprise displays a policy test failure in one of the following places:
 - the Compliance tab of the Policy Manager
 - a node's Test Results tab
 - a failing tests widget on a home page
 - the Test Results Table View in a report
2. A Compliance Administrator selects one or more failing policy tests and creates a remediation work order. A work order could contain a single policy test failure that occurs across multiple nodes, multiple policy test failures on a single node, or different test failures across multiple nodes that are all owned by a single system administrator. For more information, see [Creating a Remediation Work Order \(on page 255\)](#).
3. The Compliance Administrator configures the work order. For example, a user can:
 - specify that elements that are remediated should be promoted automatically by Tripwire Enterprise
 - specify post-remediation activities that Tripwire Enterprise should perform (for example, restarting a service after changing its configuration)
 - specify a Reference URL to link the work order to an external ticketing or workflow system
 - specify TE reports that should be run and e-mailed after remediation
4. After configuring the work order, the Compliance Administrator changes the owner of the work order to assign it to a Change Approver (either an individual TE user or a user group). For more information, see [Assigning a Work Order on page 257](#).

Tip TE assigns each work order a unique Launch URL that can be distributed via e-mail or using other methods. If a user browses to this URL while currently logged in to TE, the Work Order Editor will open to this work order. If the user is not logged into TE, they must first log in before viewing the work order.

5. A Change Approver can view all of the work orders assigned to them in a work order widget on their home page. The Approver can either approve or deny each entry in the work order. For more information, see [Approving or Denying Remediation Entries in a Work Order on page 258](#).

6. Because a single work order may involve remediation work to be performed by multiple people, Tripwire Enterprise supports different workflows. For example:
 - As soon as a Change Approver has approved at least one remediation entry, they could assign the work order to a System Owner for remediation. Once the System Owner has performed remediation on the systems for which they are responsible, they would assign the work order back to the Approver. This process would repeat until all remediation entries have been addressed.
 - Alternately, the Change Approver could approve (and/or deny) all of the entries in a work order at once, and then allow System Owners to assign the work order to each other as necessary.
7. A System Owner can view all of the work orders assigned to them in a work order widget on their home page. For each remediation entry in a work order, the System Owner can either run remediation or defer the remediation. A **remediation run** is the process of running automated remediation for one or more entries in a work order. For more information, see [Running or Deferring Remediation in a Work Order on page 259](#).
8. During a remediation run:
 - a. For each policy test, the TE Agent performs the remediation steps listed on the test's Remediator tab.
 - b. If the work order is configured to run post-remediation service commands, TE may stop, start, restart, or reload services on remediated TE Agent nodes to complete the remediation process. For more information, see [What are Post-Remediation Service Commands? on page 164](#).
 - c. If any of the automated remediation activities or post-remediation service commands generate an error, TE logs the errors to both the TE Console and the TE Agent node. For more information, see [How Automated Remediation is Logged on the next page](#)
 - d. If there are no errors and the work order is configured to promote remediated elements, TE promotes any changed elements that a) caused the policy test to fail and/or b) are listed in the **Remediated Elements** field for a policy test. TE promotes these elements using the Approval ID from the work order.
 - e. TE logs the successful remediation run. For more information, see [How Automated Remediation is Logged on the next page](#)
9. Once all remediation entries for a work order have been successfully remediated, denied, or deferred the work order's status is **Complete**. Any user with the correct permissions can close a completed work order. For more information, see [Closing or Deleting a Work Order on page 260](#).

How Automated Remediation is Logged

Tripwire Enterprise logs the results of automated remediation to both the TE Console and the TE Agent node where the remediation is run. When a failing policy test is remediated on a TE Agent node, information about the remediation activities that were run, the exit status, and the data written to standard output and standard error are written to the TE Agent's log file at `<te_root>/agent/data/log/teagent.log`.

TE also generates a log message (with a category of Remediator) in the Log Manager for each remediation entry. These log messages include the same information that is logged on the TE Agent, plus information about the failed test that was remediated, the node that it was remediated on, the status of the remediation, and the remediation run's Approval ID, reference URL, and comment. At the end of a remediation run, TE generates a summary log message that lists the number of affected nodes and tests.

To search for remediation log messages in the TE Console, you can use the Log Search tab. For more information, see [Searching for TE Log Messages on page 579](#).

Preventing Automated Remediation from Running on a Node

It is possible to prevent Tripwire Enterprise from running automated remediation on specific TE Agent nodes by editing the Agent's properties file, located at `<te_root>/agent/data/conf/agent.properties`. If the `tw.agent.preventRemediation` system property is set to `true` in this file, the TE Agent will prevent TE from running any automated remediation or post-remediation service commands. Any remediation log messages associated with the node will have a return code of Blocked.

Note that the `tw.agent.preventRemediation` system property cannot be accessed from the Tripwire Enterprise Console; it must be set by editing the TE Agent configuration file directly. This ensures that only users who have access to the Agent machine, and not any TE administrator, can change automated remediation behavior.

Another way to manage automated remediation on specific nodes is with a whitelist. A **whitelist** file, installed on an Agent system, contains an explicit list of commands (including automated remediation commands) that Tripwire Enterprise can run on that Agent. Each command that Tripwire Enterprise attempts to execute must **exactly** match a command in the whitelist file. Any other command initiated by Tripwire Enterprise on the Agent system will be denied. For more information, see [Restricting Commands on Agent Nodes with Whitelists on page 424](#).

Implementing Automated Remediation in Tripwire Enterprise

This section describes the process of implementing automated remediation in Tripwire Enterprise. For more information on this feature, see [How Does Automated Remediation Work? on page 151](#)

Caution To implement automated remediation of failing policy tests, configuration assessment (TE policies, policy tests, etc) must first be set up correctly.

Implementing automated remediation includes these steps:

Step 1: Install and Apply an Automated Remediation License (below)

Step 2: Download and Import TE Policies with Remediation Content (on the next page)

Step 3: Download and Import Post-Remediation Service Commands (on page 158)

Step 4: Create or Edit TE User Roles for Each Type of Remediation User (on page 159)

Step 5: Create TE User Accounts for Each Remediation User (on page 161)


Step 6: Create a Home Page for Each Remediation User (on page 162)

Step 7: Create Additional Widgets and Reports to Support Remediation (on page 163)


Step 1: Install and Apply an Automated Remediation License

In order to use automated remediation on a node, TE Agent must be installed on the node, and it must have a valid Automated Remediation license. You must first add an Automated Remediation license file to the Tripwire Enterprise Console, and then specify which TE Agent nodes in your installation will use automated remediation.

To add a license file:

1. Download the Automated Remediation license to a location that is accessible by Tripwire Enterprise Console.
2. Log in to TE Console with administrative privileges.
3. In the Manager bar, click **SETTINGS**.
4. Under the Administration folder, click  **Licenses**.

Note If **File System Remediation** is listed under the Licenses tab, an Automated Remediation license is already installed.

5. Click  **Add License**.
6. In the Add License dialog, click **Browse**.
7. Locate and select the Automated Remediation license file and click **Open**.
8. Click **OK**.

Next, you will verify that the Automated Remediation licenses in the TE Console are assigned to the correct nodes. Axon Agent does not support automated remediation, so automated remediation can only be used on nodes that have Tripwire Enterprise Agent installed.


To apply an Automated Remediation license to specific TE Agent nodes:

1. In the Manager bar, click **NODES**.
2. In the tree pane, select the node group containing the nodes.

Tip You can also search for nodes and manage licenses using the Node Search tab.

3. To apply licenses to specific nodes, select the check box of each node and/or group in the main pane.

To apply licenses to all nodes in the selected node group, do not select any check boxes.

4. Click **Modify** >  **Licenses**.
5. In the Update Node Licenses dialog, select **Enable license for Configuration Assessment** and **Enable license for Automated Remediation** for each node on which you want to use automated remediation.

Tip For more information, see [About Tripwire Enterprise Licenses on page 202](#).

6. Click **OK** to close the Update Node Licenses dialog.

Step 2: Download and Import TE Policies with Remediation Content

Starting with Tripwire Enterprise 8.0, the pre-configured policies on the Tripwire Web site include automated remediation content. You must download and import version 8.0 or later policies to use automated remediation with TE. If you are already using version 8.0 or later policies, skip to the next step.

Tip To determine which policy version you have installed, examine the policy import files that you downloaded from the Tripwire Web site. For example, Tripwire Enterprise 8.0 policy import files have TE_8.0 in their filenames.

To download TE policies from the Tripwire Web site:


1. Navigate to the Tripwire Customer Center:
<https://tripwireinc.force.com/customers>
2. Log in to the site using your Tripwire Customer Center credentials.
3. Click **Downloads** in the navigation bar at the top of the page.
4. Select and download the policies that match the node types in your TE installation.
5. Save the downloaded zip file to a directory on your Tripwire Enterprise Server.

6. On your local machine, extract the zip file and examine the contents. Each zip file consists of several XML files containing rules or policies, and documentation that describes the files.

Before you can use downloaded rules and TE policies, you must import them into your Tripwire Enterprise installation. Because the policy tests contained in the TE policies depend on rules downloaded with them, **you must import the rules before you import the TE policies.**


Caution If you have modified rules or TE policies that are already installed, you may overwrite those modifications when you import the new rules and policies. For more information on how Tripwire Enterprise handles imports, see [How Does Tripwire Enterprise Import an XML File?](#) on page 222.

To import rules into Tripwire Enterprise:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the **Root Rule Group**.
3. Click  **Import**.
4. In the Import Rules dialog, click **Browse**.
5. Browse to and select one of the XML rule files that you downloaded.
6. In the Import Rules dialog, click **OK**.
7. Repeat steps 3 through 6 for each rule XML file that you want to import.

Next, import each of the XML policy files that you just downloaded.

To import Policy Manager objects into Tripwire Enterprise:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the **Root Policy Test Group**.
3. In the main pane, select the **Tests** tab.
4. Click  **Import**.
5. In the Import Tests dialog, click **Browse**.
6. Browse to and select one of the XML policy files that you downloaded.
7. In the Import Tests dialog, click **OK**.
8. Repeat steps 4 through 7 for each policy XML file that you want to import.

Step 3: Download and Import Post-Remediation Service Commands

Post-remediation service commands are activities initiated by Tripwire Enterprise on an Agent node following automated remediation. Post-remediation service commands start, stop, restart, or reload a service on an Agent node in order to implement the changes made by automated remediation. For more information, see *What are Post-Remediation Service Commands?* on page 164.



Like policies, post-remediation service commands must be downloaded from the Tripwire Web site and imported into Tripwire Enterprise.

To download post-remediation service commands from the Tripwire Web site:

1. Navigate to the Tripwire Customer Center:
<https://tripwireinc.force.com/customers>
2. Log in to the site using your Tripwire Customer Center credentials.
3. Click **Downloads** in the navigation bar at the top of the page.
4. Select and download the post-remediation service commands for each type of Agent in your Tripwire Enterprise installation.

Next, import each of the post-remediation service command files that you just downloaded.

To import post-remediation service commands:

1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Post-Remediation Service Commands**.
3. Click  **Import**.
4. In the Select File dialog, click **Browse**.
5. To locate and select the XML file, complete the standard steps for your system.
6. In the Select File dialog, click **OK**.



Step 4: Create or Edit TE User Roles for Each Type of Remediation User

In Tripwire Enterprise, user roles control what actions a user can perform. You first create a role, and can then assign that role to one or more users. For more information, see [What are User Permissions and User Roles? on page 204](#).

Based on your organization's change management processes, you may want to create a user role for each type of user that is involved in automated remediation. In this example, we'll create user roles for a Compliance Administrator, Change Approver, and System Owner.

Note If you have already configured user roles in your TE installation, you may want to edit those roles to add the user permissions in [Table 46 on the next page](#) instead of creating new user roles.

To create or edit a user role:

1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Roles**.
3. To create a new role, click  **New Role**. Enter a **Role Name** (for example, "Change Approver") and **Description** (optional) and click **Next**.

To edit an existing role, click the role's name and select the Permissions tab.

4. Select the automated remediation permissions for the role, using [Table 46 on the next page](#) as a guideline.
5. Click **Finish** or **Close**.

Table 46. Suggested User Permissions for Automated Remediation



Permission Group: - Specific Permission	User		
	Compliance Administrator	Change Approver	System Owner
Remediation Work Orders:			
- Approve		X	
- Assign	X	X	X
- Close	X		
- Create	X		
- Delete	X		
- Update	X	X	X
Policy Test Management:			
- Execute Remediation			X
- All except Execute Remediation	X		
Report Management:			
- Load	X		
Post-Remediation Service Commands:			
- Update	X		
Home Page Settings:			
- Manage Own	X	X	X
Log Management:			
- Load	X	X	X
Node Management:			
- Load	X	X	X
- View	X	X	X


Step 5: Create TE User Accounts for Each Remediation User

If you plan to use existing TE user accounts for automated remediation and you have updated the user roles for those accounts, skip to the next step.

If you are creating new TE user accounts for automated remediation, you should create a separate user account for each person who is involved with remediation. This will enable you to track which user made each change in a remediation work order.

To create a user account:

1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Users**.
3. Click  **New User**.
4. Enter a **Username**, **E-mail address** (optional), and **Description** (optional). Then, click **Next**.



<p>Tips For field descriptions, click  Help.</p> <p>If your login method is LDAP/Active Directory, Tripwire Enterprise usernames must match the LDAP/Active Directory usernames. To define the login method, see Configuring the Tripwire Enterprise Login Method on page 294.</p>

5. Enter and confirm a **Password** for the user and click **Next**.
6. Select a user role (from [Step 4: Create or Edit TE User Roles for Each Type of Remediation User on page 159](#)) and click **Next**.
7. (Optional) Assign the user account to one or more user groups, and click **Next**. For more information, see [What are User Accounts and User Groups? on page 206](#).
8. Click **Finish**.

Step 6: Create a Home Page for Each Remediation User

In Tripwire Enterprise, users interact with automated remediation using work orders. Each user who works with automated remediation must have a home page with a remediation work order widget in order to view and update the remediation work that is assigned to them.

To create a home page and remediation work order widget:

1. In the Manager bar, click **HOME**.
2. In the main pane, select the **Create New Home Page** tab. Tripwire Enterprise opens a new tab labeled 'NEW Home Page.'
3. To name the new home page:
 - a. In the Configuration pane, select the **Home Pages** tab.
 - b. Click **NEW Home Page** and enter a name for the page. The name should reflect the name of the user who will use it - for example "Bob's Home Page".
4. In the main pane, click  to configure the three regions of the home page. For example, you may want to collapse the top and bottom regions, and expand the remaining region to one wide column.
5. Next, add a remediation work order widget to the new home page:
 - a. In the Configuration pane, select the **Widgets** tab.
 - b. In the Widgets tab, select **Remediation Work Orders**. TE adds the widget in the main pane.
 - c. (Optional) To change the name of the widget, click  in the widget's panel in the main pane and edit the Title.
6. To manage the information displayed in the home page, click the **Filters** dropdown and select the types of work orders that are displayed. For example, the Compliance Manager may want to see all types of work orders, but a System Owner might only see work orders where they are the Owner. For more information, see [Working with a Remediation Work Order Widget on page 253](#).

Note If a user has the Manage or Manage Own home page permission, they can edit the Filters dropdown in a work order widget on their home page.
--

7. Assign user accounts that can view the new home page:
 - a. In the Configuration pane, select the **Users** tab.
 - b. In the Users tab, select the check box of a user that you created in [Step 5: Create TE User Accounts for Each Remediation User \(on the previous page\)](#).

Step 7: Create Additional Widgets and Reports to Support Remediation

A remediation work order widget is required for each user who needs to interact with work orders. However, you may also want to add some additional widgets or reports to support automated remediation. For example:

- Add a failing tests widget to the home page of the Compliance Administrator or other users who create work orders. The failing tests widget lists failing policy tests results for specified nodes and/or policies, and can be used to create remediation work orders. For more information, see [Working with a Failing Tests Widget on page 249](#).
- Add a remediation alert generator to an alert widget on a home page. This type of alert generator posts information to the widget after TE completes a remediation run. For more information, see [How Do Alert Widgets and Alert Generators Work? \(on page 192\)](#).
- Create a Remediation Work Orders Details report to track the number of work orders that have been created, reviewed, completed, and closed. This report can also be used to track the status of remediation entries within specific work orders. For information on creating reports, see [Creating a Report on page 592](#). For details on the criteria in any report, click the **Help** link in the reports Criteria tab.
- Create a Remediation Assessment report that lists remediation entries that failed, were blocked by the node, or that were interrupted. On the Settings tab of a work order, you could configure TE to run this report after each remediation run.

What are Post-Remediation Service Commands?

Post-remediation service commands are activities initiated by Tripwire Enterprise on a TE Agent node following automated remediation. Post-remediation service commands start, stop, restart, or reload a service on a TE Agent node in order to implement the changes made by automated remediation. Although post-remediation service commands are closely related to automated remediation, they are managed separately to give users more control over what activities Tripwire Enterprise can perform on TE Agents. For more information on the relationship between automated remediation and post-remediation service commands, see [How Does Automated Remediation Work?](#) on page 151.

The specific activities that a post-remediation performs on a TE Agent node are defined in post-remediation files in the Settings Manager. Each post-remediation file lists all of the post-remediation commands for a single TE Agent operating system, or for a group of operating systems. These post-remediation files cannot be created in Tripwire Enterprise; they must be imported from the Tripwire Customer Center Web site (<https://tripwireinc.force.com/customers>) or from another TE installation. For more information on working with post-remediation service commands, see:

- [Administration Settings](#) (on page 283)
- [Exporting Post-Remediation Service Commands](#) (on page 284)
- [Changing Post-Remediation Service Commands](#) (on page 283)
- [Deleting Post-Remediation Service Commands](#) (on page 284)

In order for Tripwire Enterprise to run a post-remediation service command on a TE Agent node, all of the following conditions must be satisfied:

- The type of command to be run must be selected in the work order that initiated the automated remediation. The **Post-Remediation Service Commands Execution** setting is located on the Settings tab of a remediation work order. For information on changing this setting, see [Working with Remediation Work Orders](#) (on page 255).
- The name of the service affected by the post-remediation command must be specified in the **Post-Remediation Category** field of each policy test being remediated.
- The correct post-remediation file for the TE Agent node's operating system must be installed on the Tripwire Enterprise Console. The installed post-remediation files are listed in the Administration section of the Settings Manager.
- If you have implemented whitelists on Tripwire Enterprise Agents, the command specified in a post-remediation service command must exactly match a command in a whitelist file. For more information, see [Restricting Commands on Agent Nodes with Whitelists](#) on page 424.

As with automated remediation commands, Tripwire Enterprise logs the results of post-remediation service commands to both the TE Console and the TE Agent node where the remediation is run. For more information, see [How Automated Remediation is Logged](#) (on page 154).

What is Manual Remediation?

Note For information on how Tripwire Enterprise can automate the remediation of policy tests, see [How Does Automated Remediation Work? on page 151](#).

The Remediation tab of a policy test's properties dialog may contain instructions that can be used to manually resolve any failures generated by the test. If a monitored object fails a test run, users can refer to the manual remediation information to determine exactly how to bring the monitored object into compliance with the requirements of the test.

If you change the pass/fail conditions of a policy test, you should also review the test's Remediation tab to determine if any related changes are needed in the manual remediation content.

- Tripwire provides manual remediation information in the properties of some pre-configured policy tests (see [What are Pre-Configured Rules and Policies? on page 219](#)).
- To view or modify manual remediation text in a policy test, see [Changing the Properties of a Policy Test on page 536](#).
- To run a report that presents the remediation information for failed tests, create a Detailed Test Inventory Report (see [What are Reports and Report Types? on page 172](#)).

About Log Messages

What are Log Messages?

A **log message** is a system-generated record of an event or activity. Created by Tripwire Enterprise, **TE log messages** document the following events:

- TE user activities, such as logging in, creating a node group, or running a task manually
- TE-initiated events, such as running a scheduled task or executing an action
- Audit events harvested by Agents or forwarded to TE from a TACACS+ or RADIUS system
- Errors, such as network or system failures

If you integrate TE with Tripwire Log Center (TLC), **TLC log messages** are also available in TE. These log messages document events in applications that report to TLC.

- When you integrate TE with TLC, you have the option of configuring TE to forward TE log messages to TLC. If you do so, TLC log messages will include TE log messages.
- With log transfer rules, you can configure TE Agents to forward event data directly to TLC. In this case, TLC converts the data directly into TLC log messages (see *How Does a Log Transfer Rule Work?* on page 98).

You can review TE log messages in the **Messages** and **Message Search** tabs of the Log Manager. For more information, see:

- *Viewing TE Log Messages in the Log Manager* (on page 576)
- *Viewing the Properties of a Log Message* (on page 577)
- *Searching for TE Log Messages* (on page 579)

To review TLC log messages, you can run a search in the **Log Center Events** tab (see *Searching for TLC Log Messages* on page 581). In addition, you can access the TLC log messages created for a single node or element by opening the **Log Center Events** tab in the object's properties dialog. For further details, see:

- *Changing the Properties of a Node* (on page 321)
- *Changing the Properties of an Element* (on page 326)

For more information about TLC, see the Tripwire Log Center documentation:

<http://tlcdocumentation.tripwire.com/>

What are TE Log Message Categories?

A TE log message category indicates the type of activity or event that generated a log message in Tripwire Enterprise (see [Table 47](#)).

Table 47. TE log message categories

Category	These TE log messages are generated when ...
Action	... one of the following occurs: <ul style="list-style-type: none"> • An action running in response to a version check encounters an error • An element version is promoted to the baseline • A monitored object is restored to its baseline state
Agent CSR	... a FIPS-enabled Agent attempts to establish a secure connection with your TE Server.
Agent Discovery	... TE `discovers` an Agent for the first time, and adds the new Agent node to the Discovered Nodes group in the Node Manager. For more information, see Creating a Node by Installing Agent Software on page 54 .
Asset View Change	... an object is changed or an error occurs in the Asset View tab. For more information, see Using the Asset View Tab on page 346 .
Audit Event	... audit events are received from an external auditing utility or an Event Generator (see What is Audit Event Collection? on page 63).
Baseline	... a monitored object is baselined, or when an error occurs during baselining.
Change	... a TE object other than a node, node group, rule, or rule group is created, modified, or deleted.
Element Check	... a version check is run, or when an error occurs during a version check.
Node Change	... one of the following occurs for: <ul style="list-style-type: none"> • A node or node group (other than an Agent node or those descended from a VI management node) is created or deleted (see Creating a Node Manually on page 56) • The properties of a node or node group (other than those descended from a VI management node) are changed
Policy Score Change	... TE calculates a new policy score for a node that crosses a scoring threshold - in other words, the related TE policy has at least one scoring threshold with a value between the new score and the previous score calculated for the node. For more information, see: <ul style="list-style-type: none"> • What are Policy Scores? (on page 138) • What are Scoring Thresholds? (on page 142)
Policy Test	... one of the following occurs: <ul style="list-style-type: none"> • A TE policy, policy test, or policy group starts running • An error occurs when a TE policy, policy test, or policy group is running or finishes running • A TE policy, policy test, or policy group finishes running
Push Upgrade	... an Agent's software is upgraded with the Node Manager's upgrade feature, or when an error occurs during an upgrade (see Upgrading Agents on page 413).

Category	These TE log messages are generated when ...
RADIUS	<p>... RADIUS logs are received from the Tripwire Enterprise AAA Log Monitoring Tool (see What is the Tripwire Enterprise AAA Log Monitoring Tool? on page 237).</p> <p>Note: RADIUS (Remote Authentication Dial-In User Service) is an authentication protocol used in communications between a remote access server and an authentication server.</p>
Remediation Work Order	<p>... a remediation work order is created or changed. For more information on automated remediation, see How Does Automated Remediation Work? on page 151.</p>
Remediator	<p>... one of the following occurs:</p> <ul style="list-style-type: none"> • A failed policy test is remediated on a TE Agent node. This log message contains details about the remediation actions performed, and the outcome of the remediation on the node. • A remediation run involving multiple remediation entries finishes. This log message lists the number of failed tests that were remediated and the number of nodes that were affected. <p>For more information on automated remediation, see About Remediation on page 151.</p>
Rule Change	<p>... one of the following occurs:</p> <ul style="list-style-type: none"> • A rule or rule group is created or deleted • The properties of a rule or rule group are changed by a user
Security	<p>... one of the following occurs:</p> <ul style="list-style-type: none"> • A user logs in or out (or a login failure occurs) • A user imports a license file • A user changes a password for a user account • A user attempts to perform an operation involving a TE object for which his or her effective user role lacks sufficient permissions • TE detects another issue related to the security of the software itself
SOAP Client	<p>... a log message is generated by the Tripwire Enterprise CLI or the SOAP interface. For more information, see Creating Log Messages with the CLI in the Tripwire Enterprise Reference Guide.</p>
System	<p>... an unexpected error occurs.</p> <p>Note: These messages also include general system notes.</p>
TACACS+	<p>... TACACS+ log messages are received from the Tripwire Enterprise AAA Log Monitoring Tool (see What is the Tripwire Enterprise AAA Log Monitoring Tool? on page 237).</p> <p>Note: TACACS (Terminal Access Controller Access Control System) is a network-access protocol that authenticates users by allowing a remote access server to communicate with an authentication server.</p>
Task Run	<p>... one of the following occurs:</p> <ul style="list-style-type: none"> • A task starts or ends • A service overrun error • A scheduled task fails to run at a scheduled time • TE synchronizes a VI management node with VI management software
Task Stop	<p>... a user manually stops a task or a task times out.</p>

Category	These TE log messages are generated when ...
Test Login	... a user clicks the Test Login button in a node properties dialog.
Unknown	... an event or activity of unknown origin is detected by TE.
VI Node Change	<p>... one of the following occurs for a VI node or node group descended from a VI management node:</p> <ul style="list-style-type: none"> • The object is created by the VI node discovery process (see Monitoring Virtual Systems with Tripwire Enterprise on page 59) • The object is added, moved, or deleted by the VI synchronization process • The properties of the object are changed by a user

How Does the Archive Log Messages Task Work?

Configuring the Archive Log Messages Task

The **Archive Log Messages Task** is automatically created and configured when Tripwire Enterprise is installed. To maintain optimal system performance, you should periodically archive TE log messages by running this task. When this task runs, TE exports specified log messages from the Log Manager to an XML file.

Note The Archive Log Messages Task retains (i.e. does not export/archive) TE log messages in the Audit Event, RADIUS, and TACACS+ categories (see [Table 47 on page 167](#)). However, these log messages may be archived by configuring the Compact Element Versions Task. For more information, see [How Does the Compact Element Versions Task Work? on page 130](#).

As needed, you can modify the following properties of the Archive Log Messages Task:

- **Age of archived log messages.** With this setting, you instruct Tripwire Enterprise to archive all log messages older than a specified number of days. By default, log messages generated more than 31 days ago are archived, while those created within the last 31 days are retained.
- **Number of log messages retained.** This setting establishes the maximum number of log messages to be retained in the Log Manager. By default, Tripwire Enterprise archives all log messages in excess of 10,000.

To change these settings, or to schedule the task for automatic execution, see [Changing the Properties of a Task on page 512](#).

To run the Archive Log Messages Task manually, see [Running Tasks and Task Groups Manually on page 523](#).

Running the Archive Log Messages Task

When the Archive Log Messages Task is run, Tripwire Enterprise exports the selected TE log messages to compressed XML files in a zip file in the following directory:

```
<te_root>/server/data/log
```

Tripwire Enterprise applies the following naming convention to zipped log message files:

```
<yyyy>-<mm>-<dd>-log-archive-X.zip
```

where

<yyyy> is the current year,

<mm> is the current month,

<dd> is the current date, and

X is a numeric counter of archive files for each date. X begins at zero and increases by one digit for each archive file created on the same day.

For example, if you ran the Archive Log Messages Task three times on November 7, 2007, the following archive files would be created:

```
2007-11-07-log-archive-0.zip  
2007-11-07-log-archive-1.zip  
2007-11-07-log-archive-2.zip
```

About Reports

What are Reports and Report Types?

A **report** compiles information about Tripwire Enterprise objects and monitored objects on your network.

- For a list of reports that may be created and run in Tripwire Enterprise, see [Table 48 on the next page](#).
- To create a report, see [Creating a Report on page 592](#).

Report output is the data compiled by Tripwire Enterprise when a report is run. TE displays report output in tables and graphs. For a description of the output generated by each report type, see [Table 48](#).

Report criteria are settings that determine which data will be included in the output of a report. For instance, you could limit report output to data associated with particular nodes or elements.

Note The data in a report may be affected by the types of licenses applied to the nodes included in that report. For example, severity information is only available for nodes that have a Change Audit license applied, and information on policy scores is only available for nodes that have a Configuration Assessment license installed.

For information about what functionality is available with each type of license, see [About Tripwire Enterprise Licenses on page 202](#).

You can run reports either manually or on a scheduled basis.

- To run a report manually, see [Running a Report Manually on page 601](#).
- To run a report on a scheduled basis, you must assign the report to a **report task**. For more information, see [How Does a Report Task Work? on page 186](#).

Tips By default, Tripwire Enterprise displays all report criteria values in the output generated for a report. To limit this content to criteria for which a value(s) has been specified, select the **Show only applied report criteria** check box on the System Preferences page in the Settings Manager (see [Changing System Preferences on page 266](#)).

In the Root Group of the Report Manager, you can create report groups to organize the reports in your TE implementation. For more information, see [About Groups on page 29](#).

Table 48. Types of reports

Report Type	Report Output	Typically used as ...
Baseline Elements	This report identifies all baseline versions that meet the specified criteria.	... a summary of baselined elements and associated approval IDs.
Change Audit Coverage	This report identifies the properties of rules that meet the specified criteria. As applicable, report output includes each rule's commands, specifiers, start points, stop points, and/or criteria set(s).	... an administrative report to identify which rules are applied to a specified file server or directory server.
Change Process Compliance	This report identifies change versions that represent authorized and unauthorized changes to specified monitored systems. An authorized change is associated with a valid change request ticket ID.	... a management report showing a historic trend in the effectiveness of change-process controls.
Change Rate	This report shows the total number of change versions (additions, removals, and modifications) created for specified monitored systems over a period of time. Within the selected time period, the report displays the number of change versions at a regular interval (or 'frequency'); for instance, daily, weekly, or monthly.	... a management report showing trends in detected changes over time.
Change Variance	<p>This report identifies all monitored objects that differ between the monitored systems specified by the report. Tripwire Enterprise includes a monitored object's element in report output if both of the following conditions are satisfied:</p> <ul style="list-style-type: none"> • The monitored object's current version is a change version. • The monitored object does not exist for all specified nodes or the object's change version differs from the current version of the object for other specified nodes. <p>As appropriate, you can limit report output to specific nodes, rules, and/or elements.</p>	... a means of identifying unexpected changes made by deployment of a patch or installation package on multiple nodes. To determine which new change versions should be promoted, you may review the report for inconsistencies across the updated systems.
Change Window	This report indicates the number of detected changes for a specified monitored system(s) that have occurred inside and outside a defined change window.	... a report used to demonstrate that changes were made inside an approved change window, as required by established change-control policies.
Changed Elements	<p>This report identifies elements that have been added, modified, and/or removed. For each element, the report can also identify a variety of associated data, such as approval IDs or specific attributes that changed.</p> <p>Note: To compile data on attribute values, run a Detailed Changes Report.</p>	... a summary of detected changes for compliance purposes.

Report Type	Report Output	Typically used as ...
Changes by Node or Group	This report calculates the number of change versions created for one or more monitored systems. For each system, the report also calculates the total number of change versions for each type of change (added, removed, or modified).	... a means of identifying network resources that experience an abnormally high rate of change.
Changes by Rule or Group	This report calculates the number of change versions for monitored objects identified by each specified rule or rule group. For each rule or group, the report also calculates the total number of change versions for each type of change (added, removed, or modified).	... a means of identifying network resources that experience an abnormally high rate of change.
Changes by Severity	For a specified monitored system, this report shows the total number of change versions that fall within a specified range of severity levels.	... a high-level report showing unresolved changes within a specified severity range. To identify systems that have deviated from their known-and-trusted state, this report would typically be run at the end of a day.
Compliance History	For each specified time interval, this report calculates the number of passing and failing policy test results created for all specified nodes.	... a management report showing the historic trend of compliance with a policy.
Composite Changes	<p>This report calculates the number of authorized and unauthorized composite changes for each specified node and/or node group within a specified period of time.</p> <p>A composite change consists of one or more element versions created for a single node in a single time interval specified by the report (such as a day or week).</p> <ul style="list-style-type: none"> • If TE assigned the same Approval ID to any of the new element versions, these versions collectively comprise a single authorized composite change. Within a single time interval, a node can have an unlimited number of authorized composite changes. • If any of the new versions lack an Approval ID, these versions collectively comprise a single unauthorized composite change. Within a single time interval, a node can have no more than one unauthorized composite change. <p>For more information, see Example: Running a Composite Changes Report on page 179.</p> <p>Note: An authorized composite change only applies to the same node, Approval ID, and time interval. If TE assigned the same Approval ID to change versions created in the same time interval for multiple nodes in a node group, then TE creates a separate authorized composite change for each node when calculating the totals for the group.</p>	... means to enforce change management policies by tabulating the number and authorization of composite changes.

Report Type	Report Output	Typically used as ...
Detailed Changes	This report provides detailed information about current baselines and/or change versions. If the current version of a specified monitored object is a change version, the report output includes the version's severity level, as well as any changed content or attributes.	... one of the following: <ul style="list-style-type: none"> • A template documenting changes made to a staging server prior to deployment on production servers. By using the template with a report-by-match operation, you can ensure that Tripwire Enterprise only approves changes on production servers that are identified by the template. • Documented evidence of a successful, authorized change. For verification, the report may be appended to a change ticket. • Background information to assist investigation of an unexpected change.
Detailed Test Inventory	This report identifies the name, type, remediation text, and other properties (optional) for each policy test that satisfies the report's criteria.	... a reference list that documents the properties of specified policy tests.
Detailed Test Results	For each specified node, this report lists all policy results that meet the specified report criteria. For each result, the output indicates which element was tested, as well as the outcome of the test (passed/failed).	... a means of identifying specific settings that are out of compliance with a policy.
Detailed Waivers	This report lists the properties of all waivers that meet the specified report criteria.	... a reference list that documents the properties of specified waivers.
Device Inventory	This report provides the make, model, and version of each monitored system identified by report criteria.	... a reference list of monitored systems.
Element Contents	This report presents the contents of specified element versions.	... an inventory of the contents of monitored objects.
Elements	This report lists all elements identified by the specified criteria. Optionally, the report can also identify the software-installation package associated with the monitored object represented by the element (if any).	... a reference list of all monitored objects for a node or node group.
Frequently Changed Elements	This report ranks the most frequently changed elements that meet the specified criteria. For each element, the report identifies the total number of changes, the time of the most recent change, and the element's node.	... a means of identifying elements that change on a regular basis as part of normal business processes. With this data, you can adjust your rules to optimize the efficiency of version checks.
Frequently Changed Nodes	This report ranks the most frequently changed monitored systems that meet the specified criteria. The report includes the total number of detected changes for each system, as well as the totals for each type of change (added, removed, or modified).	... a means of identifying monitored systems that experience frequent changes.

Report Type	Report Output	Typically used as ...
Inventory Changes	For your Tripwire Enterprise implementation, this report calculates the number of nodes that have been added, modified, and deleted over a specified period of time.	... a means of verifying that the removal of nodes from Tripwire Enterprise was authorized.
Last Node Check Status	<p>Within a specified time range, this report lists the date and time of the last version check run on each monitored system identified by report criteria. As appropriate, report output can include:</p> <ul style="list-style-type: none"> • The names of all nodes for which the last version check ran successfully. • The names of all nodes for which the last version check failed. • The names of all nodes for which a version check was <i>not</i> run. 	... verification that version checks are running as expected and without failures.
Missing Elements	This report identifies nodes that lack 1) elements with specific names or 2) elements created by a specific rule or rule group.	... an administrative tool to detect configuration drift in monitored systems.
Nodes with Changes	This report identifies all changed monitored systems that meet the specified criteria.	... a high-level report showing the proportion of monitored systems that are not in their baseline state.
Reference Node Variance	This report identifies all elements that differ between one node (the reference node) and another (the compare node). In a single report, the reference node may be compared with one or more compare nodes.	... a means of detecting configuration drift among monitored systems that should be identical.
Remediation Assessment	<p>This report summarizes information generated by automated remediation activities.</p> <p>Note: This report type is only available if an Automated Remediation license is installed on the TE Console.</p>	<p>... a summary of automated remediation activities that were performed, or</p> <p>... a “punch list” of manual post-remediation steps to be performed.</p>
Remediation Work Orders Details	<p>This report provides detailed information about remediation work orders and remediation entries that meet the specified criteria.</p> <p>Note: This report type is only available if an Automated Remediation license is installed on the TE Console.</p>	... a means for users to review detailed information about automated remediation activities that have been performed, or that need to be performed.
Remediation Work Orders Summary	<p>This report provides a high-level summary of remediation work orders and remediation entries.</p> <p>Note: This report type is only available if an Automated Remediation license is installed on the TE Console.</p>	... an administrative tool for managers who oversee remediation activities performed by others.
Scoring	For each specified TE policy, this report provides the latest policy score calculated for each specified node, as well as the number of waivers employed in the calculation of the score.	... an audit report that shows the policy scores for selected nodes.

Report Type	Report Output	Typically used as ...
Scoring History	<p>For all policy scores that satisfy the report's criteria, this report presents the following data for each period in the specified time range:</p> <ul style="list-style-type: none"> • The highest and lowest policy scores for the period. • The average policy score for the period. 	... a management report that may indicate past trends in the policy scores of selected nodes.
System Access Control	This report lists the user permissions associated with each user role that meets the specified criteria.	... a reference list that provides a complete overview of current user-access authorizations and permissions.
System Log	This report identifies all Tripwire Enterprise log messages that meet the specified criteria.	... a user-defined query of the Tripwire Enterprise system log.
Tasks	This report indicates the current status of specified tasks.	... a means of quickly determining the current status of tasks.
Test Result Summary	<p>For each specified Policy Manager object, this report indicates:</p> <ul style="list-style-type: none"> • The number of specified nodes that are not in full compliance with the Policy Manager object. • The number and percentage of specified nodes that are in full compliance with the object. <p>Note: In previous versions of Tripwire Enterprise, this report was known as a 'Policy Scorecard Report.'</p>	... a high-level management report that provides a comprehensive view of compliance throughout your organization.
Test Results By Node	<p>This report presents data about policy test results for all nodes specified by the report criteria. The output of the report contains:</p> <ul style="list-style-type: none"> • A summary list of nodes, which includes the total number of policy test results that each node passed and failed. • A detailed list of nodes, which includes a sub-list of policy tests run on each node. For each policy test, this list may also indicate the test's rule(s) and version-attribute conditions. • A list of nodes that experienced errors when a policy test was run. 	... a reference list showing failed policy test results that indicate monitored systems requiring remediation.
Unreconciled Change Aging	This report identifies nodes that have one or more elements with a current change version. For each node, the report calculates the age of the oldest current change version. In the report's output, TE chronologically groups the nodes according to this age.	... a means of identifying monitored systems in need of attention.

Report Type	Report Output	Typically used as ...
Unchanged Elements	<p>For one or more nodes, this report identifies all elements for which Tripwire Enterprise did <i>not</i> detect a change within the specified time range. Alternatively, this report can identify the rules used to baseline any unchanged elements.</p> <p>Note: Since the number of unchanged elements may be extremely large, you should narrow report criteria to the greatest extent possible.</p>	... a means of identifying unchanged monitored objects that were expected to change over a specified period.
Unmonitored Nodes	<p>This report identifies:</p> <ul style="list-style-type: none"> • Nodes that lack a valid Tripwire Enterprise license (see About Tripwire Enterprise Licenses on page 202). • Nodes that have not been baselined or version checked within a specified period of time. • Monitored virtual machines on which a Tripwire Enterprise Agent has not been installed and enabled (see How are Nodes Created? on page 54). 	... an administrative report to ensure that the proper nodes are being monitored.
User Roles	<p>For one or more nodes and/or node groups, this report identifies the effective user role for each specified user account. For more information, see What is an Effective User Role? on page 207.</p> <p>Note: This report is a legacy feature of Tripwire Enterprise. In TE 7.0.1 and later, you should instead create a User Roles All Object Types Report.</p>	... a means to ensure that proper levels of control have been assigned to existing user accounts.
User Roles All Object Types	<p>For one or more TE objects, this report identifies the effective user role for each specified user account. For more information, see What is an Effective User Role? on page 207.</p>	... a means to ensure that proper levels of control have been assigned to existing user accounts.

Example: Running a Composite Changes Report

Note For a description of the Composite Changes Report, see [Table 48 on page 173](#).

As a network administrator, Charlie monitors his company's file servers with Tripwire Enterprise. In the Node Manager, Charlie has created a node group for the file server nodes hosted at each of the company's sites — Toronto, Miami, and London.

To enforce the company's change-management policy for the file server nodes, Charlie creates a Composite Changes Report. The report's criteria include:

- A **Nodes** criterion that specifies the Toronto, Miami, and London node groups.
- A **Frequency** criterion that specifies a daily interval for a time frame of the last seven days.

The Toronto node group contains three (3) file servers — File Server A, File Server B, and File Server C. When Charlie runs the report for the first time, Tripwire Enterprise identifies a number of composite changes for the servers. For instance, File Server A has the following authorized composite changes (see [Table 49](#)):

- Two (2) authorized composite changes for Approval ID W1538 — one for six change versions created on Tuesday, and another for two versions created on Friday.
- One (1) authorized composite change for Approval ID W3688, which was assigned to 12 change versions created on Tuesday.

Table 49. Calculating authorized composite changes for File Server A

	Number of Authorized Composite Changes							
Approval ID	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Totals
W1538		1			1			2
W3688		1						1
Totals	0	2	0	0	1	0	0	3

To calculate the number of **authorized composite changes** for the Toronto node group, Tripwire Enterprise adds the number of changes for File Server A to the number of changes for File Servers B and C (see [Table 50](#)). In the output of the Composite Changes Report, TE presents a total of 11 authorized composite changes for the Toronto group.

Table 50. Calculating authorized composite changes for the Toronto node group

	Number of Authorized Composite Changes							
File Server	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Totals
File Server A		2			1			3
File Server B	1				4		1	6
File Server C			2					2
Totals	1	0	2	0	5	0	1	11

Tripwire Enterprise uses a similar calculation to determine the total number of **unauthorized composite changes** for the Toronto node group (see [Table 51](#)). If TE created one or more element versions without an Approval ID for a file server in a single day, those versions are collectively considered a single unauthorized composite change. For example, TE created six (6) versions without an Approval ID for File Server A on Tuesday. When tabulating totals for the report, TE treats these six versions as a single unauthorized composite change.

Table 51. Calculating unauthorized composite changes for the Toronto node group

	Number of Unauthorized Composite Changes							
File Server	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Totals
File Server A	1	1			1	1		4
File Server B				1	1			2
File Server C				1				1
Totals	1	1	0	2	2	1	0	7

How Do I Manage Report Output?

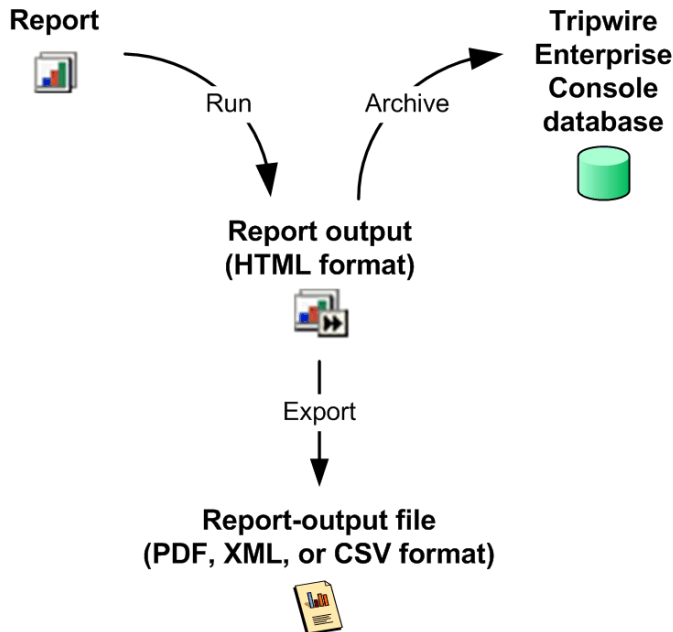
When you run a report, Tripwire Enterprise compiles report output based on the specified report type and criteria. To save the output for future reference, you can either archive or export the compiled data (see [Figure 15](#)).

When you **archive** report output, Tripwire Enterprise saves the data in the **Tripwire Enterprise Console database**. At any time, you can easily review the archived output of a report (see [Working with Archived Report Output on page 608](#)).

Note To create or delete archived report output, the Create Archived Reports and Delete Archived Reports permissions must be assigned to your user account (see [What are User Permissions and User Roles? on page 204](#)).

When you **export** report output, Tripwire Enterprise formats and saves the data in a PDF, XML, or CSV file. Exported **report-output files** offer a convenient means of sharing report data with other people. If needed, archived report output can also be exported. For further instructions, see [Working with Archived Report Output on page 608](#).

Figure 15. Running, exporting, and archiving a report



What are Dashboards?

A **dashboard** is a user-defined collection of reports that may be run and viewed together in the Report Manager. Only reports with graphic output may be added to a dashboard.

When you run a dashboard, TE compiles output for all of the dashboard's reports. Displayed in a single window called the **Dashboard Viewer**, the output of each report is formatted as a thumbnail of a graph.

To create and run a dashboard, see:

- [Creating a Dashboard \(on page 594\)](#)
- [Running a Dashboard \(on page 607\)](#)

As needed, you can change the list of reports compiled by a dashboard, as well as the order in which report thumbnails appear in the Dashboard Viewer. You can also adjust the layout of the Dashboard Viewer, including the number of columns and the size of the window. For further instructions, see [Changing the Properties of a Dashboard on page 591](#).

How Do Embedded Report Links Work?

With the **Links** criterion, you can embed links in the output of some reports. When a user clicks one of these links, TE generates and displays the output of another report in a separate browser window. The output of the linked report is determined by:

- The **context** of the link in the original report (determined by the Links criterion and report type).
- The **report criteria** for the original report.

With the Links criterion, you can also embed links to report groups. When a user clicks one of these links in the output of a report, TE opens a dialog with a list of the group's reports that are compatible with the current report's output. To compile output for one of the listed reports, the user selects the report's link in the dialog. For more information, see [Example: Embedding Links in a Change Rate Report \(on the next page\)](#).

Embedded links only work in generated report output displayed in the Tripwire Enterprise interface. Links do **not** work in archived report-output files, PDF report-output files, or report-output files that are generated and e-mailed by a report task.

To configure the Links criterion for a report, see [Changing the Properties of a Report on page 589](#).

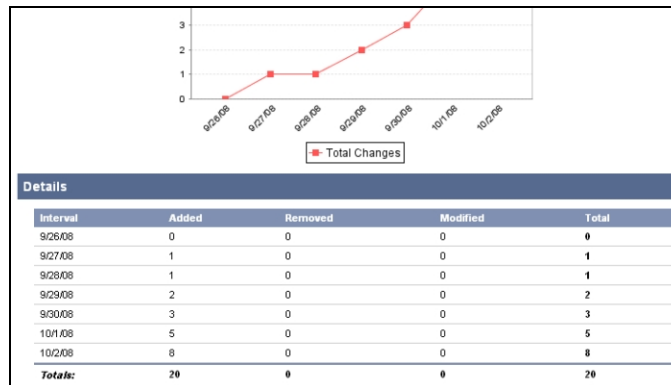
Example: Embedding Links in a Change Rate Report

Lucy is responsible for enforcing her company's change policy on a group of Windows file servers. To automatically calculate the number of change versions created on each of the previous seven days, Lucy created a Change Rate Report. When Lucy runs the report, the output indicates the total number of change versions created on each day, along with the totals for each type of change (additions, removals, and modifications).

When reviewing the output of the Change Rate Report, Lucy would like to have the option of generating a Detailed Changes Report for any of the report's subtotals. To do so, she completes the following steps:

1. In the **Links** criterion of the Change Rate Report, Lucy selects the Detailed Changes Report in the following fields:
 - **Change type link**
 - **Total link**
2. In the Report Manager, she runs the Change Rate Report.
3. TE compiles and presents the output in the Report Viewer. Lucy scrolls down to the **Details** section, where all subtotals are now linked to the Detailed Changes Report (see [Figure 16](#)).
4. Lucy clicks a link and TE compiles the Detailed Changes Report for the selected subtotal. In a separate Report Viewer, TE presents the output of the Detailed Changes Report. In this case, the output is a list of all change versions that comprise the selected subtotal.

Figure 16. Details section in the output of a Change Rate Report



What are System Reports and User Reports?

A **system report** can be viewed and run by any Tripwire Enterprise user with the **Load Report Manager** permission (see [What are User Permissions and User Roles?](#) on page 204). A **system report group** contains one or more system reports, and a **system dashboard** contains one or more system reports.

A **user report** can only be viewed and run by the person who created it (the owner) or a user with the Administrator user role. A **user report group** solely consists of user reports, and a **user dashboard** only contains user reports.

Note Access controls (see [What are Access Controls?](#) on page 208) can affect the information displayed in user reports. If a TE Console is configured to hide nodes that are managed with access controls (see [Restricting Node Visibility with Access Controls](#) on page 212), nodes may be excluded from user reports if the user who created the report does not have the appropriate permissions.

System reports, if run automatically from a task, will run as the system user and have access to all data.

Any user can create a user report. In addition, any user can change, move, or link any user report that he or she created. However, only users with the **Manage System Reports** permission can perform similar functions with system reports. By default, only the default administrator user account has the Manage System Reports permission. [Table 52 \(on the next page\)](#) compares the Report Manager capabilities of users with and without the Manage System Reports permission.

Note For an introduction to linking, see [What are Links and Linked Objects?](#) on page 213.

To assign the Manage System Reports permission to another user:

1. Create a customized user role that includes the Manage System Reports permission (see [Working with User Roles](#) on page 293).
2. Assign the customized user role to the user's account (see [Changing User Account Properties](#) on page 286).

Table 52. Manage System Reports permission

Report Manager Function	Users with Manage System Reports Permission	All Other Users
Create, edit, or delete system reports ?	Yes	No
Create, edit, or delete system report groups ?	Yes	No
Create, edit, or delete system dashboards ?	Yes	No
Create or edit user reports, user report groups, or user dashboards ?	Yes	Yes
Delete user reports, user report groups, or user dashboards ?	Yes	No
Move or link a system report, system report group, or system dashboard to a system report group ?	Yes	No
Move or link a system report, system report group, or system dashboard to a user report group ?	Yes	No
Move or link a user report, user report group, or user dashboard to a system report group ?	Yes	Yes
Move or link a user report, user report group, or user dashboard to a user report group ?	Yes	Yes

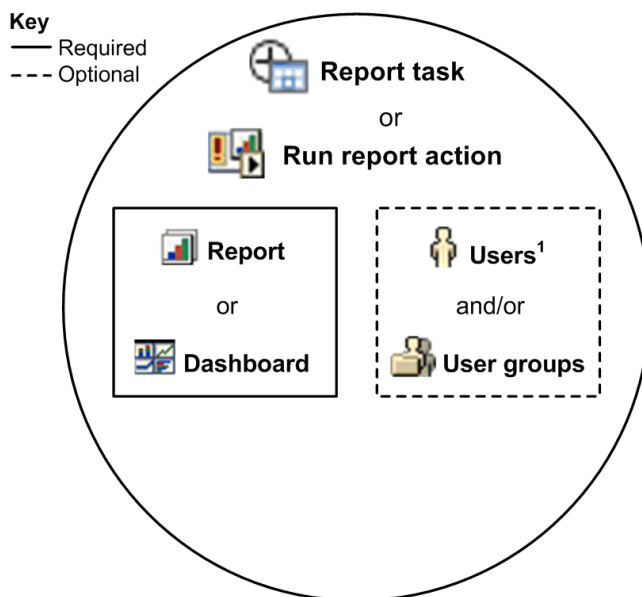
How Does a Report Task Work?

When you run a **report task**, Tripwire Enterprise compiles output for a single report or dashboard. If desired, the application may save the output in a file (HTML, XML, CSV, or PDF format), and then e-mail the file to selected users and user groups. In addition, Tripwire Enterprise may archive the report output in the Tripwire Enterprise Console database.

- [Figure 17](#) identifies the Tripwire Enterprise objects that may be associated with a report task.
- [Figure 18 on the next page](#) diagrams the process flow of a report task.

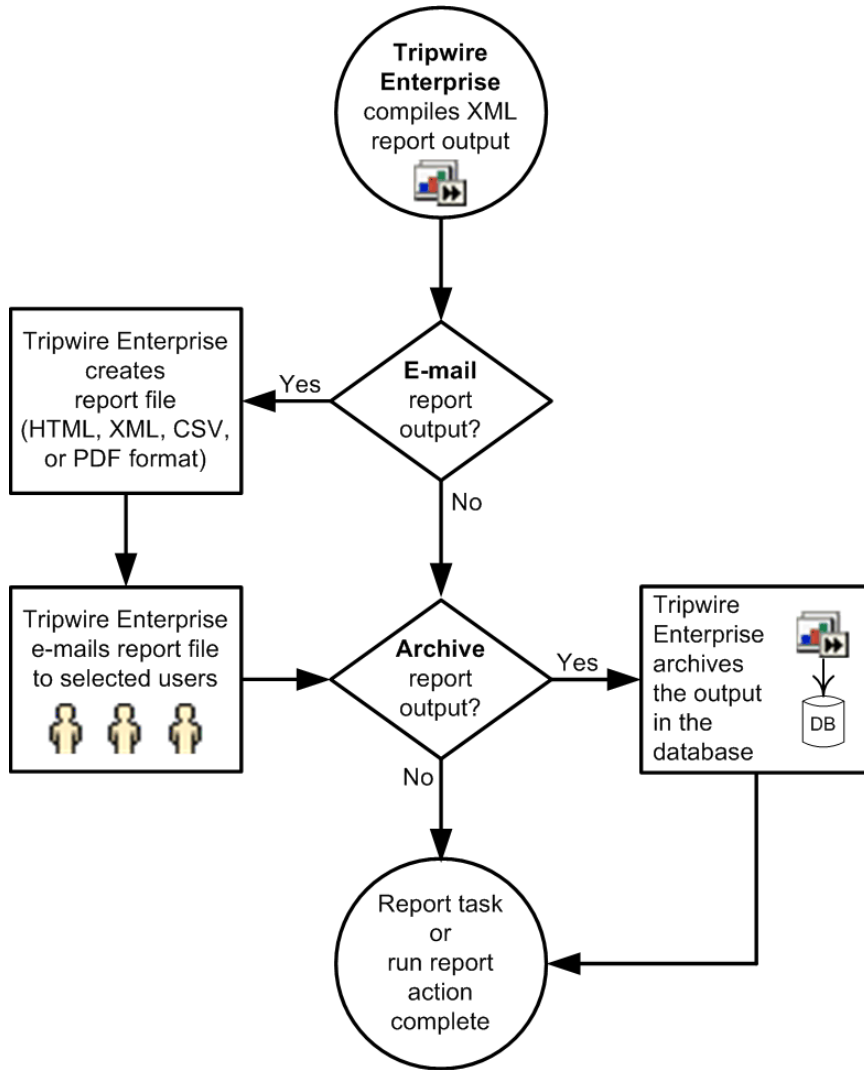
To create a report task, see [Creating a Report Task on page 519](#).

Figure 17. Objects in a report task or run report action



¹ Multiple users and user groups may be assigned as recipients of report output compiled by a report task or run report action.

Figure 18. Running a report task or run report action



How Does a Run Report Action Work?

For an introduction to actions, see [What are Actions and Action Types? \(on page 116\)](#). A **run report action** compiles output for a single report or dashboard. You can either run the report (or the reports in the dashboard) with its defined report criteria, or further limit the report's output to the context of the operation in which the action is run; either a version check or the Run Actions feature (see [Running Actions with the Run Actions Feature on page 119](#)). In this case, you specify one or more scope criteria in the action's properties to limit output to change-related data. For descriptions of the scope criteria available with a run report action, see [Table 53 below](#).

For example:

- If the Node Scope is enabled for a run report action used in a version check, the action will limit report output to nodes for which the version check resulted in the creation of one or more change versions.
- If the Rule Scope is enabled for a run report action run on a node with the Run Actions Feature, the action will limit report output to rules that identified elements of the node that have current change versions.

Table 53. Optional scope criteria in a run report action

Scope Criteria	This scope criterion limits report output to data associated with ...
Node Scope	... changed nodes specified by the operation with which the action is run.
Rule Scope	... rules used to identify changed elements specified by the operation with which the action is run.
Element Scope	... changed elements specified by the operation with which the action is run.
Version Scope	... selected element versions targeted by the Run Actions feature. Note: The Version Scope criterion only applies if you run the action with the Run Actions feature by manually selecting a version(s) displayed in a list of element versions.

When you create a run report action, you can specify one or more users and/or user groups to whom TE will e-mail any report output compiled by the action. In this case, TE saves the output in a file (HTML, XML, or PDF format), and then e-mails the file to the specified recipients. In addition, you can have TE save compiled report output in the Tripwire Enterprise Console database.

- [Figure 17 on page 186](#) identifies the Tripwire Enterprise objects that may be associated with a run report action.
- [Figure 18 on the previous page](#) diagrams the process flow for a run report action.

To create a run report action, see [Creating a Run Report Action on page 497](#).

About Home Pages

What are Home Pages and Widgets?

Created and viewed in the Home Page Manager (see [Figure 19 on the next page](#)), a **home page** is a configurable tab that provides users with convenient access to Tripwire Enterprise reports and event data. Typically, a home page presents information of interest to a specific group of users — for example, security personnel who want a summary view of the security status of a data center.

To configure a home page, you add one or more widgets to the page. A **widget** is a customizable home page component that may be viewed in the main pane of the Home Page Manager. [Table 54 \(on the next page\)](#) describes each type of widget.

- To create a new home page, see [Creating a Home Page on page 241](#).
- To learn about the factors controlling the availability of home pages, see [Who Can View and Configure a Home Page? on page 192](#). [What are Home Pages and Widgets?](#)
- To add a widget to an existing home page, see [Working with Widgets on page 245](#).

As shown in [Figure 19 on the next page](#), the main pane of the Home Page Manager is divided into three **regions**: Top, Middle, and Bottom. To customize the layout of a home page, you can:

- Hide (or display) the Top or Bottom regions.
- Add a widget to any of the columns in a region. (Each region may contain up to four columns.)
- Move a widget (within the same region or between regions) by clicking-and-dragging its title bar.

For further details, see [Changing the Layout of Regions and Widgets in a Home Page \(on page 242\)](#).

Tips If your user account has the Manage home page permission, you can also create, modify, and delete home pages in the Settings Manager (see [What are Settings? on page 194](#)).

If you enable the **Always log in to Home Page** setting in the Settings Manager, Tripwire Enterprise will automatically open the Home Page Manager whenever you log in. Otherwise, TE opens the last Manager you visited.

Figure 19. The Home Page Manager

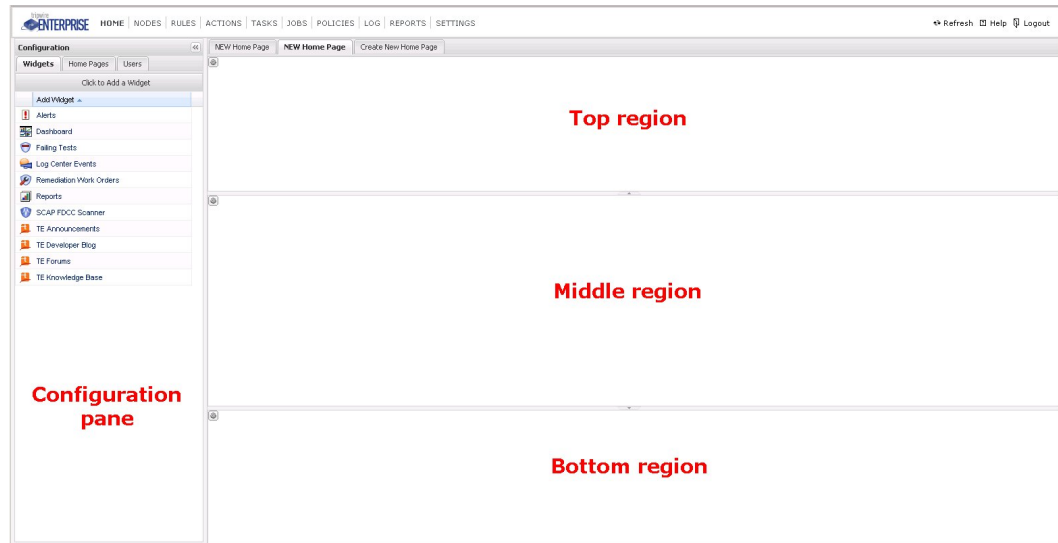


Table 54. Types of widget

Type of Widget	Description
Alert	Presents information about Tripwire Enterprise events that satisfy specified criteria. To learn more, see How Do Alert Widgets and Alert Generators Work? on page 192.
Customer Center	<p>These widgets provide content from the Tripwire Customer Center (https://tripwireinc.force.com/customers).</p> <ul style="list-style-type: none"> • The TE Announcements widget presents links to the latest Tripwire announcements posted on the Customer Center. • The TE Developer Blog widget presents links to recent blog posts from Tripwire Enterprise developers. • The TE Forums widget presents links to the latest posts in the Tripwire Enterprise Discussion Forums. • The TE Knowledge Base widget presents links to the Tripwire Enterprise Resource Library, Knowledge Base, Tech Talk Forum, and training enrollment page.
Dashboard	<p>Presents the graphic output of reports in a specified dashboard.</p> <ul style="list-style-type: none"> • For an introduction to dashboards, see What are Dashboards? on page 182. • To specify the dashboard to be displayed by an existing dashboard widget in a home page, see Changing the Properties of a Dashboard Widget on page 248. • To run a report presented in a dashboard widget, see Running a Report in a Dashboard Widget on page 248.

Type of Widget	Description
Failing Tests	<p>Presents a list of failed policy tests that meet specified criteria. This widget can be used to create remediation work orders for automated remediation.</p> <ul style="list-style-type: none"> • For information on policy tests, see How Does a Policy Test Work? on page 135. • For information on automated remediation, see How Does Automated Remediation Work? on page 151. • For information on using this widget, see Working with a Failing Tests Widget on page 249.
Log Center Event	<p>Presents a list of Security Information and Event Management (SIEM) events in Tripwire Log Center (TLC) that satisfy specified criteria. With this type of widget, you can review various field values for SIEM events, as well as change the state assigned to each event.</p> <ul style="list-style-type: none"> • This type of widget is only available if you have configured TE to query a TLC Server for log messages (see Changing Log Management Settings on page 268). • To change the criteria for SIEM events presented by a TLC event widget, see Changing the Properties of a Log Center Event Widget on page 251. • For more information about SIEM events, see the Tripwire Log Center documentation: http://tlcdocumentation.tripwire.com/
Remediation Work Orders	<p>Presents a list of work orders for automated remediation.</p> <ul style="list-style-type: none"> • For information on automated remediation, see How Does Automated Remediation Work? on page 151. • For information on using this widget, see Working with a Remediation Work Order Widget on page 253.
Report	<p>Presents a list of specified reports.</p> <ul style="list-style-type: none"> • For an introduction to reports, see What are Reports and Report Types? on page 172. • To change the list of reports displayed in an existing report widget in a home page, see Changing the Properties of a Report Widget on page 251. • To run a report in a report widget, see Running a Report in a Report Widget on page 252.

How Do Alert Widgets and Alert Generators Work?

A component of a home page (see [Figure 19 on page 190](#)), an alert widget consists of one or more alert generators. An **alert generator** is a utility that automatically posts information about TE system events that satisfy specified criteria. An alert generator's **scope** defines the criteria that determine which events are reported by the generator, and any event information posted by a generator is known as **alert data**. Alert data remains visible in an alert generator until the time you manually clear the data from your view of the generator.

[Table 55](#) describes each type of alert generator that may be added to an alert widget.

- To configure the scope of an alert generator, see [Changing the Properties of an Alert Widget on page 246](#).
- To view current alert data, see [Reviewing Alert Data in an Alert Generator on page 247](#).
- To erase alert data, see [Clearing Alert Data from an Alert Generator on page 247](#).

Who Can View and Configure a Home Page?

If a user account is assigned to a home page, the user can view the home page and its widgets in the Home Page Manager. To assign a user account to a home page, see [Changing the List of User Accounts Assigned to a Home Page on page 243](#).

For a user account to have the ability to create, configure, or delete home pages (and widgets), the account must have the Manage or Manage Own user permission.

If multiple users are assigned to the same home page, only users with the Manage permission can create, modify, or delete widgets in the home page. Such changes to the content of a home page are visible to all user accounts assigned to the page. However, if a user makes a change that only affects his or her view of the home page — for instance, rearranging the home page's widgets in the main pane — the change is not visible to other users.

Table 55. Types of alert generators

Type of Generator	This type of generator posts alert data when ...
Discovered nodes	<p>... Tripwire Enterprise (TE) adds a new Agent node to the Discovered group in the Node Manager. For more information, see Creating a Node by Installing Agent Software on page 54.</p> <p>Note: The scope of a Discovered nodes alert generator is limited to the Discovered node group and cannot be changed.</p>
Node errors	<p>... TE creates an Error log message for a node identified by the generator's scope. For more information about Error messages, see What are Log Messages? on page 166.</p>
Policy score change	<p>... TE creates a Policy Score Change log message (see What are TE Log Message Categories? on page 167).</p> <p>This type of TE log message indicates that TE has calculated a new policy score for a node that has crossed a scoring threshold - in other words, the related TE policy has at least one scoring threshold with a value between the new score and the previous score calculated for the node.</p> <p>To define the scope for this type of alert generator, you specify the following objects:</p> <ul style="list-style-type: none"> • A node or node group, and • A TE policy or a policy test group containing one or more TE policies <p>For more information, see:</p> <ul style="list-style-type: none"> • What are Policy Scores? (on page 138) • What are Scoring Thresholds? (on page 142)
Remediation messages	<p>... TE completes an automated remediation run. For more information, see How Does Automated Remediation Work? on page 151.</p>
VI node change	<p>... TE discovers or synchronizes a VI management node. For more information, see Monitoring Virtual Systems with Tripwire Enterprise on page 59.</p>
Waiver expiration	<p>... a waiver identified by the generator's scope is due to expire within a specified period of time. For more information, see What are Policy Scores? on page 138.</p>

About the Settings Manager

What are Settings?

In the Settings Manager, you can control TE interface features, severity range values, user access levels, and several other application parameters. For a list of setting categories available in the Settings Manager, see [Table 56 below](#).

Table 56. Settings Manager categories

Category	Description
User	<p>For the current user only, these settings control the following parameters:</p> <ul style="list-style-type: none">• Preferences control the behavior and display settings of the Tripwire Enterprise interface. For more information, see Changing User Preference Settings on page 262.• Differences control the use of context lines when you compare element versions in the Difference Viewer (see Responding to Changes on page 46). For more information, see Changing User Difference Settings on page 265.
System	<p>System settings apply to all users of your Tripwire Enterprise implementation. These settings include:</p> <ul style="list-style-type: none">• Preferences (see Changing System Preferences on page 266)• Log Management (see Changing Log Management Settings on page 268)• Database (see Recalculating Database Index Statistics on page 269)• Severity Ranges (see What are Severity Ranges? on page 114)• Global Variables (see What are Global and Local Variables? on page 196)• Approval Templates (see Working with Approval Templates on page 273)• E-mail Servers (see What are E-mail Servers? on page 196)• Configure TE Console (see Configuring Tripwire Enterprise Console Properties on page 274)• Import Settings (see Importing Settings on page 276)• Export Settings (see Exporting Settings on page 277)• Support Data (see Creating Diagnostic Files for Tripwire Support on page 278)
Administration	<p>Administration settings control user access for your Tripwire Enterprise implementation. These settings include:</p> <ul style="list-style-type: none">• Post-Remediation Service Commands (see What are Post-Remediation Service Commands? on page 164)• Users (see What are User Accounts and User Groups? on page 206)• User Groups (see What are User Accounts and User Groups? on page 206)• Home Pages (see What are Home Pages and Widgets? on page 189)• Roles (see What are User Permissions and User Roles? on page 204)• Login Method (see What are Login Methods? on page 207)• Licenses (see About Tripwire Enterprise Licenses on page 202)

Category	Description
Custom Properties	<p>A custom property is a user-defined property that can be assigned to nodes, elements, or element versions. These settings include:</p> <ul style="list-style-type: none"> • Version Properties • Element Properties • Node Properties <p>For more information, see What are Custom Properties? on page 197.</p>
Monitoring	<p>These settings control how Tripwire Enterprise monitors systems for changes. These settings include:</p> <ul style="list-style-type: none"> • Custom Node Types. (see Working with Custom Node Types on page 299) • Criteria Sets. This setting defines the criteria sets that may be added to the following rule types: <ul style="list-style-type: none"> - File system rules (see How Does a File System Rule Work? on page 83) - Windows registry rules (see How Does a Windows Registry Rule Work? on page 85) - Windows RSoP rules (see How Does a Windows RSoP Rule Work? on page 88) - Database metadata rules (see How Does a Database Metadata Rule Work? on page 89) - Database query rules (see How Does a Database Query Rule Work? on page 92) • File Systems. This setting controls how Tripwire Enterprise runs a version check of file systems (see Setting File System Preferences on page 310). • LDAP Directories. This setting specifies the binary attributes for monitored LDAP directories. • Active Directories. For monitored Active Directories, this setting 1) specifies binary and security attributes, and 2) enables or disables the collection of audit events. <p>Note: For an introduction to directory attributes, see What are Binary Attributes and Security Attributes? on page 97.</p>

What are E-mail Servers?


The E-mail Servers setting defines the **e-mail servers** used to send Tripwire Enterprise e-mail notifications and report output. For more information, see:

- [Working with E-mail Servers](#) (on page 272)
- [How Does an E-mail Action Work?](#) (on page 120)
- [What are Reports and Report Types?](#) (on page 172)

What are Global and Local Variables?

A **global variable** is a user-defined variable that may be selected for entry in a Tripwire Enterprise interface field. In the Settings Manager, you may create two types of global variables.

- A **text variable** may be entered in some fields in wizards and properties dialogs.
- A **password variable** may be entered as the login password for a network device, directory server, or database server. Passwords are entered in the Login tab of a node properties dialog (see [Changing the Properties of a Node](#) on page 321).

To enter a variable in a variable-enabled field, you click  **Choose Variable** to select the variable from a list. In addition, you can directly type a text variable in a variable-enabled field with the following format:

Format: `$(<variable_name>)`

where `<variable_name>` is the name of the variable

Example: `$(MachineName)`

For more information on global variables, see [Working with Global Variables](#) on page 271.

In the properties dialog of a file server node, directory server node, or database node, you can define local variables for the node. A **local variable** is a text variable that only applies to a single node. If a local variable has the same name (case sensitive) as a global variable, the value of the local variable will override the value of the global variable. To create a local variable, see [Changing the Properties of a Node](#) on page 321.

What are Custom Properties?

A **custom property** is a user-defined property that can be applied to nodes, elements, or element versions in the Node Manager. When you create a custom property in the Settings Manager, you specify the following:

1. The type of data that the property will store.
2. A **default value** for the property.
3. Whether or not users can enter a **custom value** if the property is applied to a TE object in the Node Manager.
4. Whether or not a TE object will inherit the property's default value if a custom value is *not* specified for the object.

Table 57 identifies each of the data types that can be selected for a custom property. In addition, the table describes the possible values for each data type.

Table 57. Custom property data types

Data Type	A value for this data type must be ...	Example
Date	... a single date.	November 5, 2006
Numeric	... a single integer in a specified range of numeric values.	The number "60" in a possible range of 1 - 100
Select	... a specified value from a set of one or more values.	The number "3" from a set of 1, 2, and 3
Text	... a string of characters.	%TE_root/bin
Yes/No	... a binary value (either yes or no).	No
Note: In a select or text property, a value can consist of any combination of characters.		

Once a custom property has been created, you can apply the property to Tripwire Enterprise objects in the Node Manager.

- A **node custom property** can be applied to any node.
- An **element custom property** can be applied to any element.
- A **version custom property** can be applied to any element version.

If you apply a custom property to a Node Manager object (either a node, element, or element version), you can assign the property's default value to the object. If the **Editable in property editor** setting is selected for the property, you can also enter a **custom value** that applies solely to the object.

- For a **date** or **yes/no** custom property, a custom value can be any value that is compatible with the data type. For instance, any date can be entered as a custom value for a date custom property.
- For a **numeric** custom property, a custom value can be any integer that falls within a range of numbers specified by the property.
- For a **select** custom property, a custom value can be any value defined by the property.
- For a **text** custom property, a custom value can be any string of characters that does not exceed the maximum number of characters specified by the property.

If you do **not** enter a custom value for a Node Manager object, the property's value is determined by its inheritance setting (specified in the Settings Manager).

- If the inheritance setting is enabled, the property's default value automatically applies to the object.
- Otherwise, the property does not apply to the object.

For an example of how custom properties work, see [Example: Using Custom Properties on the next page](#).

To create a custom property in the Settings Manager, see [Working with Custom Properties on page 298](#).

To apply a custom property to a Node Manager object, see:

- [Defining Custom Property Values for a Node \(on page 328\)](#)
- [Defining Custom Property Values for an Element \(on page 330\)](#)
- [Defining Custom Property Values for an Element Version \(on page 331\)](#)

Example: Using Custom Properties

Geoff is the database administrator for Examplatronics, Inc. Recently, the company introduced the following change-control policies for six Oracle production servers in its Vancouver, Canada office:

- Only Geoff is authorized to make changes to the Oracle servers.
- All changes must be made within a change window of 2AM - 4AM daily.

As the company's systems administrator, Dawn has been asked to enforce these policies with Tripwire Enterprise. If a detected change is in compliance with both policies, management wants Tripwire Enterprise to automatically promote the new change version. Otherwise, Tripwire Enterprise should notify Geoff of the unauthorized change.

To begin, Dawn creates the following Tripwire Enterprise objects:

- A version custom property named **Owner** with the **text** data type (see [Table 57 on page 197](#)).
- The six **actions** listed in [Table 58 on the next page](#).

She then creates a **check rule task** and assigns the following TE objects to the task:

- The **nodes** that represent the Oracle production servers.
- An **Oracle metadata rule** to identify the objects to be monitored on the Oracle production servers.
- An **action group** that runs the Audit Trail Conditional Action followed by the Time Range Conditional Action.

Dawn schedules the check rule task to run daily at 5AM. If the task runs and creates a change version for a monitored object on one of the servers, Tripwire Enterprise runs the action group. For each change version, [Figure 20 on page 201](#) outlines the sequence of possible actions that may be triggered by the action group.

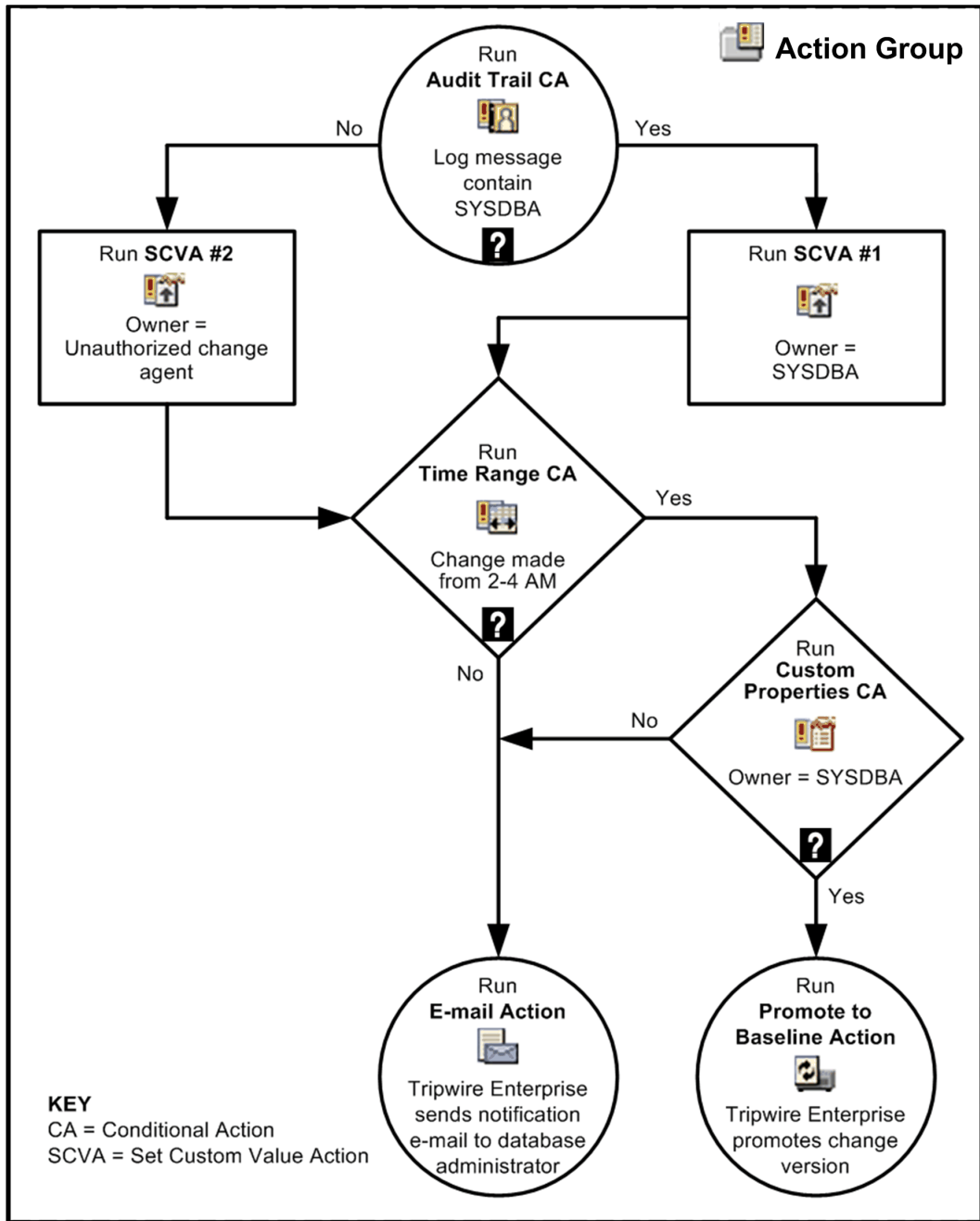
Due to Dawn's efforts, Tripwire Enterprise now enforces Examplatronics' change policies. As an added benefit, Dawn and Geoff can easily gather information about unauthorized changes made to the Oracle production servers. For instance:

- To review unauthorized changes at any time, Geoff can run a search for element versions that have a value of "Unauthorized change agent" for the Owner version custom property (see [Searching for Element Versions on page 364](#)).
- To identify Oracle production servers with unauthorized changes, Dawn creates a **Nodes with Changes Report** (see [Creating a Report on page 592](#)). Dawn schedules the report to run daily, and she limits the report output to Oracle servers that have one or more change versions with a value of "Unauthorized change agent" for the Owner version custom property. To automatically e-mail the report output to Geoff, Dawn also assigns the report to a new report task ([Creating a Report Task on page 519](#)).

Table 58. Actions created by Exemplatronics systems administrator

Action	Description
Set Custom Value Action #1	For a specified change version, this action assigns a value of "SYSDBA" for the Owner version custom property.
Set Custom Value Action #2	For a specified change version, this action assigns a value of "Unauthorized change agent" for the Owner version custom property.
E-mail Action	If a version check creates one or more change versions, this action sends a single notification e-mail to the database administrator (Geoff).
Audit Trail Conditional Action	<p>Tripwire Enterprise generates a log message for each change version created by a version check. This action searches these log messages for a User value of SYSDBA.</p> <ul style="list-style-type: none"> • If a log message's User is "SYSDBA," this action runs Set Custom Value Action #1. • Otherwise, this action runs Set Custom Value Action #2.
Custom Properties Conditional Action	<p>This action determines if a change version has a value of "SYSDBA" for the Owner version custom property.</p> <ul style="list-style-type: none"> • If so, the action runs the default Promote to Baseline Action. • If not, this action runs the E-mail Action.
Time Range Conditional Action	<p>This action defines a change window of 2AM - 4AM.</p> <ul style="list-style-type: none"> • If a change version reflects a change made between the hours of 2AM and 4AM, this action runs the Custom Properties Conditional Action. • Otherwise, this action runs the E-mail Action.

Figure 20. Process flow for the Examplatronics action group



About User Access

About Tripwire Enterprise Licenses

To work with Tripwire Enterprise, you must first acquire a **license file** from Tripwire, Inc., and then import the file to the Settings Manager. Each license file contains one or more of the following types of licenses:

- A **Change Audit license** enables change auditing for a single monitored system of a specific type. Each Change Audit license can only be used with its applicable node type; for example, a license created for a database node cannot be used with a network device node.
- A **Configuration Assessment license** enables TE to check a single node for compliance by running policy tests on that node.
- An **Automated Remediation license** enables TE to remediate failed policy tests on a single file server node. To automatically remediate failed policy tests for a node, the node must have a valid Configuration Assessment license **and** an Automated Remediation license.

Change Audit and Configuration Assessment licenses can be applied to each node independently. When a node is created, TE attempts to apply all three license types to the node. If no licenses of a specific type are available, TE creates a log message stating that that license type was not applied to the node.

For a comparison of the functionality available with each type of license, see [Table 59 on the next page](#).

Notes Tripwire Enterprise cannot run an operation on an unlicensed node (such as a baseline operation or policy test). However, TE can compile report output for an unlicensed node.

If you remove all licenses from a node, Tripwire Enterprise disables version checks and baseline operations on the node until a license is applied to the node again. For more information, see [Temporarily Disabling Checks and Baselines on a Node on page 387](#).

To add or delete license files, see:

- [Adding a License File \(on page 297\)](#)
- [Deleting Licenses \(on page 297\)](#)

You can enable or disable licenses on specified nodes in the Node Manager. For instructions, see [Managing Licenses for Nodes on page 418](#).

Table 59. Functionality available with each type of Tripwire Enterprise license

	Change Audit	Config Assessment	Automated Remediation
Check assets for change (see How Tripwire Enterprise Detects Change on page 36)	x		
View changes with the Difference Viewer (see Comparing Element Versions on page 388)	x		
View the severity of detected changes (see What are Severity Levels? on page 112)	x		
Collect audit events from assets (see What is Audit Event Collection? on page 63)	x		
Monitor assets for change in real-time (see How Does Real-Time Monitoring Work? on page 70)	x		
Generate reports with change data (see What are Reports and Report Types? on page 172)			
Check assets for compliance (see About Policies and Compliance on page 131)		x	
View and track compliance over time (see Viewing Results in the Compliance Tab on page 550)		x	
Generate reports with compliance data (see What are Reports and Report Types? on page 172)			
View remediation guidance for failed policy tests (see What is Manual Remediation? on page 165)		x	
Automatically remediate failed policy tests (see How Does Automated Remediation Work? on page 151)			x

How Do TE Licenses Work with VI Nodes?

The following licensing guidelines apply to VI nodes:

- VI management nodes do not require a license.
- When a VI management node is discovered (see [Monitoring Virtual Systems with Tripwire Enterprise on page 59](#)), Tripwire Enterprise assigns a single Change Audit and/or Configuration Assessment license to each supported hypervisor node. If not enough licenses are available, TE creates the remaining hypervisor nodes as unlicensed nodes and creates a log message about the license status for each unlicensed node.
- Supported hypervisor nodes use licenses like any other node. However, if a license is assigned to a supported hypervisor node, the license also applies to all virtual machine (VM) nodes, VM template nodes, and virtual switch nodes managed by the hypervisor.

What are User Permissions and User Roles?

A **user permission** is a system authorization that enables a user to view, create, or otherwise modify data in TE.

- [Table 60 \(on the next page\)](#) defines common types of permissions in TE. For a complete list, see [Appendix I: Definitions of User Permissions on page 611](#).
- [Appendix II: User Permissions for Procedures](#) (in the Tripwire Enterprise online help) identifies the required user permissions for each procedure in the *Tripwire Enterprise User Guide*.

A **user role** is a collection of user permissions that may be assigned to a user account or access control. When you install Tripwire Enterprise, the TE installer creates a collection of **default user roles** in the Settings Manager (see [Table 61 on the next page](#)). You can also create **customized user roles** with user permissions of your choice, or change the permissions assigned to a user role (see [Working with User Roles on page 293](#)).

Note To determine the actual set of permissions granted to a user for a Tripwire Enterprise object, TE calculates the **effective user role** for the user's account. The effective user role is based on the object's access controls and the permissions assigned to the user's role. For more information, see [What is an Effective User Role? on page 207](#).

Caution The Policy Manager, Policy User, Rule Manager, and Rule User default roles are used in access controls applied to the pre-configured TE objects that can be downloaded from the Tripwire Web site. To preserve the intended purpose of these roles, you should avoid assigning them to user accounts. For more information, see [What are Pre-Configured Rules and Policies? \(on page 219\)](#) and [How Do I Manage User Access for Pre-Configured Rules and Policies? \(on page 220\)](#).

Table 60. Common types of user permissions

Permission	This type of permission grants users the ability to ...
Create	... create TE objects in a specific Manager, or a component of the Settings Manager (for example, TE objects in the Action Manager, or the E-mail Servers setting).
Create ACL	... create access controls for objects in a specific Manager.
Delete	... permanently delete TE objects in a specific Manager, or a component of the Settings Manager. Deletion removes the object itself, along with any linked instances of the object.
Edit	... modify data in a specific component of the Settings Manager.
Link	... create links between TE objects in a specific Manager, or a component of the Settings Manager.
Load	... access a TE Manager. With a load permission, TE displays the Manager's button in the sidebar of the TE interface.
Manage	... work with system reports, system searches, or a component of the Settings Manager.
Update	... modify the properties of TE objects in a specific Manager, or a component of the Settings Manager.
Use	... use a rule or rule group in a baseline or version check operation.
View	... view the properties of nodes, node groups, and associated access controls in the Node Manager.

Table 61. Default user roles

User Role	With this role, a user has ...
Administrator	... full control of all TE objects and features in all Managers.
Monitor User	... read-only access in all Managers.
Policy Manager*	... the ability to manage policies, policy groups and policy tests.
Policy User*	... the ability to run and link policies, policy groups and policy tests.
Power User	... full control of TE objects and features in the Node Manager, Rule Manager, Action Manager, Task Manager, Policy Manager, and some components of the Settings Manager.
Regular User	... read access to all TE Managers, as well as the ability to run policy tests, run version checks, and change the properties of nodes (and node groups).
Rule Manager*	... the ability to manage rule groups and rules.
Rule User*	... the ability to use and link rule groups and rules.
User Administrator	... the ability to create, edit, and delete user accounts, user roles, and user groups.
<p>* Do not assign these roles to user accounts directly. They are used for access controls applied to rules and policies that can be downloaded from the Tripwire Web site. For more information, see What are Pre-Configured Rules and Policies? (on page 219) and How Do I Manage User Access for Pre-Configured Rules and Policies? (on page 220).</p>	

What are User Accounts and User Groups?

To provide a person with access to Tripwire Enterprise, an Administrator must create a **user account**. Each user account is assigned a username, a password, and a single user role. To log in to the system, a user enters the username and password associated with his or her account. An account's user role is involved in calculations that determine effective user roles (see [What is an Effective User Role? on the next page](#)).

Note When Tripwire Enterprise is installed, a user account called 'administrator' is automatically created and configured. Equipped with the Administrator role, this account is typically assigned to the person responsible for managing a Tripwire Enterprise implementation.

For more information on user accounts, see:

- [Creating a User Account \(on page 285\)](#)
- [Changing User Account Properties \(on page 286\)](#)
- [Changing the Password for a User Account \(on page 286\)](#)
- [Assigning a User Role to a User Account \(on page 287\)](#)
- [Associating User Accounts with User Groups \(on page 287\)](#)
- [Unlocking a User Account \(on page 288\)](#)
- [Deleting User Accounts \(on page 288\)](#)

To simplify the management of user accounts, Administrators and User Administrators may create an unlimited number of user groups. A **user group** is a collection of user accounts, and a single user account may be assigned to multiple user groups. Common criteria for user groups include the geographic location or responsibilities of users. For example, user groups may be based on office locations or areas of responsibility. For more information, see [Working with User Groups on page 289](#).

User roles and permissions *cannot* be directly assigned to a user group. However, you can provide a user group with exclusive write access to a Tripwire Enterprise object by creating an access control. For more information, see [What are Access Controls? on page 208](#).

What is an Effective User Role?

An **effective user role** is the actual level of control that a user account has over a Tripwire Enterprise object. To calculate a user's effective user role for a TE object, Tripwire Enterprise refers to the permissions of the user account, as well as any access controls that apply to the TE object.

- If the user account is the only source of permissions, the effective user role is the user role assigned to the user account.
- If an access control has been created for the TE object, or any groups containing the object, the effective user role is determined by inheritance rules. For more information, see [What are Access Controls? on the next page](#).

To determine the effective user role for specific nodes and/or node groups, create a User Roles Report in the Report Manager (see [Creating a Report on page 592](#)).

What are Login Methods?

When a user logs in to Tripwire Enterprise, he or she enters the username and password for their user account. In the Settings Manager, you can configure one of the following login methods to control how TE authenticates these login credentials.

- With the **Password** method, TE authenticates the username and password entered by each user.
- With the **LDAP/Active Directory** method, an LDAP or Active Directory server handles authentication.

Note Tripwire Enterprise always authenticates Administrator accounts with the **Password** login method, regardless of the specified login method.

To configure the system authentication method, see [Configuring the Tripwire Enterprise Login Method on page 294](#).

What are Access Controls?

For greater control of user access, Administrators can add access controls to the following Tripwire Enterprise objects:

- Nodes and node groups
- Rules and rule groups
- Actions and action groups
- Tasks and task groups
- TE policies, policy tests, and policy test groups

An **access control** is a setting that grants specified user accounts and/or user groups exclusive access to that object. Once an access control has been applied to a TE object, *only* the specified users can:

- View or edit the object's properties
- Delete the object
- Use the object in a TE operation or function

If a user is excluded by an access control, he or she cannot edit, delete, or use the object.

Note By default, users who are excluded by an access control can still see all excluded objects in the TEConsole UI. However, you can configure the Console to hide nodes from excluded users in the Node Manager and Report Manager. For more information, see [Restricting Node Visibility with Access Controls on page 212](#).

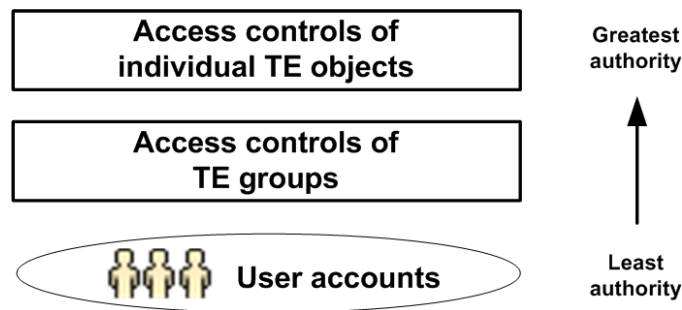
If appropriate, multiple access controls may be applied to a single TE object. In addition, an unlimited number of user accounts and user groups may be assigned to a single access control.

Note The default administrator account has access to all TE objects regardless of applied access controls. Therefore, the administrator account cannot be assigned to an access control. See [Helpful Hints for Access Controls on page 211](#) for more information on managing access controls for TE administrators.

Administrators assign a single **user role** to each access control. The user role defines the level of access granted to each user account and user group associated with the access control. When an authorized user works with a TE object governed by an access control, the access control's user role overrides the user role of the individual's user account. (For an introduction to user roles, see [What are User Permissions and User Roles? on page 204](#).)

When an access control is added to a group, it applies to all TE objects descended from the group. However, access controls applied to individual TE objects (such as a node or rule) override those applied to groups. For example, if an authorized user accesses a node governed by its own access control **and** a node group's access control, he or she will be granted the permissions of the user role in the node's access control. In short, access controls of individual TE objects take precedence over group access controls, and group access controls take precedence over the user roles assigned to user accounts (see [Figure 21](#)).

Figure 21. Authority of user role permissions



Some Tripwire Enterprise functions involve multiple TE objects. In such cases, users must have write access to all of the objects involved in the operation. For instance, a simple version check involves a single node and rule. If either object is governed by an access control from which you are excluded, you will be unable to run the version check.

When multiple access controls apply to a TE object, **inheritance rules** determine which access control takes precedence. [Table 62 on the next page](#) defines the inheritance rules in Tripwire Enterprise.

For more information, see:

- [Helpful Hints for Access Controls](#) (on page 211)
- [Example: Using Access Controls](#) (on page 211)
- [Creating an Access Control for a Node or Node Group](#) (on page 333)
- [Changing an Access Control for a Node or Node Group](#) (on page 333)
- [Deleting Access Controls for a Node or Node Group](#) (on page 334)

Table 62. Access control inheritance rules

Tripwire Enterprise Objects	Inheritance Rules
sub-groups	<p>A group access control applies to all subordinate TE objects. For instance, if you create an access control for a node group, the control applies to all nodes and sub-groups descended from the group.</p> <p>If a user accesses an individual TE object (such as a node or rule) contained within multiple, nested node groups with access controls, the applicable access control is determined by proximity to the object. In other words, the access control of the lowest sub-group in the hierarchy determines if the user has write access to the object and, if so, which user permissions are granted to the user.</p>
linked TE objects	<p>If a user accesses a TE object that is linked to multiple groups with access controls, Tripwire Enterprise grants the user all permissions assigned to the access controls.</p> <p>For an introduction to links, see What are Links and Linked Objects? on page 213.</p>
user accounts and user groups	<p>If a user group is assigned to an access control, the access control applies to all user accounts in the group. If you add another user account to the user group, TE automatically assigns the new account to all access controls that contain the group.</p> <p>When applied to the same TE object, individual user access controls override user group access controls. In other words, if a user account is assigned to an access control for a TE object, and that same account belongs to a user group assigned to a different access control for the same TE object, the user role associated with the user account takes priority over the user role assigned to the user group.</p>
tasks	<p>A user account (either the system account or another account) is assigned to each baseline or check rule task. When the task runs, TE calculates the account's effective user role for each of the task's nodes and rules. If an effective user role grants access to a node or rule, TE uses the object to run the task. Otherwise, the object is excluded from the task.</p> <p>For more information, see:</p> <ul style="list-style-type: none"> • How Does a Baseline Rule Task Work? (on page 128) • How Does a Check Rule Task Work? (on page 129) <p>Note: The system user account has access to all TE objects, regardless of applied access controls.</p>

Helpful Hints for Access Controls

Hint #1. Apply user groups to access controls. Although individual user accounts may be assigned to an access control, you can greatly simplify the management of access controls by relying primarily upon user groups. For example, if a user is assigned to a user group, and the user group is assigned to multiple access controls, you can un-assign the user from the access controls by removing the user from the user group.

Hint #2. Be sure to give Administrators access. A good practice is to have a user group of TE administrators, and to assign an access control from that group to the Administrator role. Otherwise, users with the Administrator role may not be able to access some objects with access controls applied.

Hint #3. Avoid access controls for individual TE objects. Although access controls may be added to individual TE objects, Tripwire recommends that you rely primarily on group access controls. By applying access controls to groups only, you will save considerable time in the management of user access to TE objects.

Hint #4. Create and run a User Roles Report. To determine effective user roles for nodes and/or node groups, create and run a User Roles Report in the Report Manager (see [Creating a Report on page 592](#)).

Example: Using Access Controls

Susie and Chris have user accounts that have been assigned the Regular User role. As such, they can both perform basic functions on the nodes in the Routers node group.

Jim, the system administrator, decides to apply an access control to the Routers node group. Jim adds Susie to the access control, but he excludes Chris. In addition, Jim assigns the Administrator role to the access control.

With the new access control, Susie now has full access to all nodes in the Routers node group. However, Chris cannot view the properties of the group or the properties of objects within the group since he was not included in the access control. Since Chris' work requires that he be able to version check the monitored systems in the Routers group, he notifies Jim of the problem.

To resolve the issue, Jim creates a second access control for the Routers node group. He adds Chris to the access control (but excludes Susie). Jim also assigns the Regular User role to the access control.

With the second access control in place, Chris regains Regular User access to the Routers node group. However, Susie also retains the Administrator permissions provided by the first access control.

Restricting Node Visibility with Access Controls

By default, users who are excluded by access control can still see excluded objects in the TE Console UI. However, starting with TE Console 8.6.1 you can configure the Console to hide nodes from excluded users in the Node Manager and Report Manager.

If this feature is enabled, users without the Node View permission for a specific node will not be able to see that node in the TE Console UI. If a user has access to objects such as tasks that directly reference a node or node group that they are not authorized to view, the reference to the restricted item will appear as "Unauthorized" instead of the actual node name. Clicking the Unauthorized link will open a message informing the user that access is not permitted.

Users who are assigned the Administrator role directly, rather than by access controls, can still view all nodes in the Node Viewer and Report Viewer.

To configure TE Console to hide nodes with access controls:

1. If you are using a MS SQL Server backend database:
 - a. Add the CREATE FUNCTION permission to the TE Console's user account on the database.
 - b. Restart the database.
2. Stop the TE Console service:

```
<te_root>/server/bin/twservices stop
```
3. On the TE Server, edit the `<te_root>/server/data/config/server.properties` file to include:

```
tw.node.viewable.enabled=true
```
4. Start the TE Console service:

```
<te_root>/server/bin/twservices start
```

Linking Tripwire Enterprise Objects

What are Links and Linked Objects?


Linking is the process of associating a Tripwire Enterprise object with a group. The resulting relationship is known as a **link**. With links, you can add a single Tripwire Enterprise object to multiple groups *without* creating redundant copies of the object.

Table 63 identifies the objects that can be linked in Tripwire Enterprise. When you create one of these TE objects, the application links the new object to a single group. However, once the object has been created, you may link it to an unlimited number of additional groups. A TE object that is linked to more than one group is known as a **linked object**.

Table 63. Links between Tripwire Enterprise objects

Tripwire Enterprise Object	This type of object may be linked to ...
Node	... node groups Note: Nodes and groups cannot be linked to a group under a VI management node.
Node group	... other node groups
Rule	... rule groups
Rule group	... other rule groups
Action	... action groups Note: If the true or false branch of a conditional action group contains one or more actions or groups, TE displays these objects in the Action Manager's tree pane.
Action group	... other action groups
Task	... task groups
Task group	... other task groups
TE policy	... policy test groups
Policy test	... policy test groups and TE policies
Policy test group	... other policy test groups and TE policies
Report	... report groups
Dashboard	... report groups
Report group	... other report groups

How Do Links Work?

In the TE interface, a Tripwire Enterprise object appears in all groups to which it is linked. In addition, the **link emblem**  overlays the icon of each linked object. To make changes to a linked object, you can open and edit the object's properties from any group to which the object is linked. The properties of a linked object do *not* vary from one group to another.

To link a Tripwire Enterprise object to a group, see:

- [Linking Nodes and Node Groups](#) (on page 380)
- [Linking Rules and Rule Groups](#) (on page 473)
- [Linking Actions and Action Groups](#) (on page 503)
- [Linking Tasks and Task Groups](#) (on page 525)
- [Linking Policy Manager Objects](#) (on page 571)
- [Linking Reports, Report Groups, and Dashboards](#) (on page 597)

At any time, you can **unlink** a TE object from any group to which the object is linked. When an object is unlinked from a group, only the specified link is removed from the system. All other links to the object remain intact, even if you unlink the object from the original group with which it was linked.

Caution If you delete a linked object, the object and all associated links are removed from Tripwire Enterprise.
--

To unlink Tripwire Enterprise objects, see:

- [Unlinking Nodes and Node Groups](#) (on page 381)
- [Unlinking Rules and Rule Groups](#) (on page 474)
- [Unlinking Actions and Action Groups](#) (on page 504)
- [Unlinking Tasks and Task Groups](#) (on page 526)
- [Unlinking Policy Manager Objects](#) (on page 572)
- [Unlinking Reports, Report Groups, and Dashboards](#) (on page 598)

Most Managers contain an **Unlinked group**. An Unlinked group contains TE objects that have been unlinked from all groups in the Manager. If you unlink an object that is linked only to a *single* group, Tripwire Enterprise moves the object to the Manager's Unlinked group.

To retrieve an object from an Unlinked group, see:

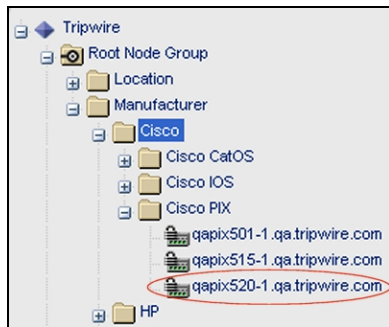
- [Moving Nodes and Node Groups](#) (on page 379)
- [Moving Rules and Rule Groups](#) (on page 473)
- [Moving Actions and Action Groups](#) (on page 503)
- [Moving Tasks and Task Groups](#) (on page 525)
- [Moving Policy Manager Objects](#) (on page 570)
- [Moving Reports, Report Groups, and Dashboards](#) (on page 597)

Example: Creating, Linking, and Unlinking a Node

As the system administrator for Tripwire, Inc., Jane has created a hierarchy of node groups to organize the nodes for monitored systems on her company's network. At the highest level, the hierarchy is divided into two node groups. The **Locations** node group sorts nodes by office location, while the **Manufacturers** node group categorizes nodes by vendor. Each node is linked to at least one sub-group in each of these node groups.

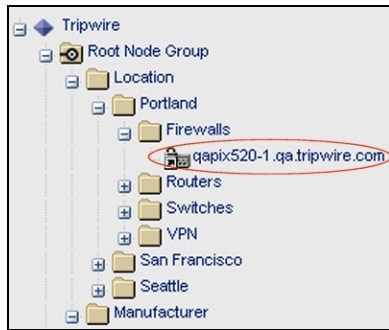
Since the Portland office recently installed a new Cisco PIX firewall, Jane wants to add the firewall to her Tripwire Enterprise implementation. First, she creates a network device node for the firewall in the **Manufacturers** node group. In [Figure 22 below](#), the new node has been added to the **Cisco PIX** node group. Since the new node is linked only to a single node group (Cisco PIX), a link emblem does **not** overlay the node's icon.

Figure 22. New firewall node in the Cisco PIX node group



Now that the Cisco PIX firewall has been added to Tripwire Enterprise, Jane can link the node to any other node group. In accordance with her established node hierarchy, Jane links the new node to the Portland **Firewall** node group in the **Locations** group (see [Figure 23](#)).

Figure 23. Linked firewall node in Portland Firewall node group




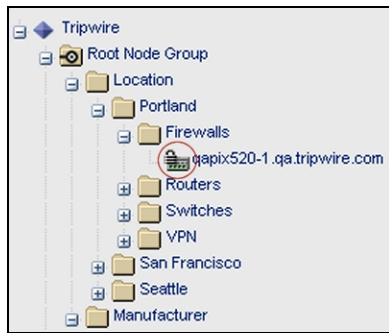
Since the node is now linked to two node groups, the link emblem  overlays the node's icon in both the **Firewall** node group (see [Figure 23](#)) and the **Cisco PIX** node group. If Jane then unlinks the node from the **Cisco PIX** node group, the node remains linked to the **Firewall** node group. However, the link emblem no longer overlays the node icon (see [Figure 24 below](#)).

Figure 24. Firewall node icon without link emblem



Importing and Exporting Tripwire Enterprise Objects

How Do I Import and Export Tripwire Enterprise Objects?

The Tripwire Web site provides a collection of XML files containing pre-configured rules, rule groups, policies, policy tests, and policy test groups. By importing these files to the Rule Manager and Policy Manager, you can use these Tripwire-crafted objects to initially configure your TE implementation. For more information, see:

- [What are Pre-Configured Rules and Policies? \(on page 219\)](#)
- [How Does Tripwire Enterprise Import an XML File? \(on page 222\)](#)

You can also export the TE objects in a Manager to an **XML file**. At a later date, the contents of the file can be imported to the same Manager in any TE installation. When an XML file is imported, the saved objects and data are re-created in the Manager.

User-created XML files serve three primary purposes:

- **Data backup.** XML files provide a reliable method for backing up your TE objects and data.
- **Data transfer between Tripwire Enterprise implementations.** XML files may be used to transfer TE objects from one TE implementation to another. By transferring TE objects, you can avoid the time-consuming task of re-creating identical objects in multiple implementations.
- **Data creation and editing.** In some cases, you can complete a procedure faster by directly editing the content of an XML file, rather than performing the same procedure in the TE interface. For instance, you can quickly create multiple nodes by editing an XML file and then importing the contents.

For further details about the XML import process, see [How Does Tripwire Enterprise Import an XML File? on page 222](#).

To export TE objects and data to an XML file, see:

- [Exporting Settings](#) (on page 277)
- [Exporting Home Pages](#) (on page 292)
- [Exporting Nodes and Node Groups](#) (on page 406)
- [Exporting Rules and Rule Groups](#) (on page 475)
- [Exporting Actions and Action Groups](#) (on page 505)
- [Exporting Tasks and Task Groups](#) (on page 527)
- [Exporting Policy Manager Objects](#) (on page 573)
- [Exporting Log Messages](#) (on page 582)
- [Exporting Reports, Report Groups, and Dashboards](#) (on page 599)

To import the contents of an XML file, see:

- [Importing Settings](#) (on page 276)
- [Importing Home Pages](#) (on page 292)
- [Importing Nodes and Node Groups](#) (on page 407)
- [Importing Rules and Rule Groups](#) (on page 476)
- [Importing Actions and Action Groups](#) (on page 506)
- [Importing Tasks and Task Groups](#) (on page 528)
- [Importing Policy Manager Objects](#) (on page 574)
- [Importing Reports, Report Groups, and Dashboards](#) (on page 600)

You can also export and import the content of an element version that represents a file. When you export an element version, Tripwire Enterprise saves the version's content in a binary or text file. For further instructions, see:

- [Exporting the Content of an Element Version](#) (on page 408)
- [Importing Element Version Content](#) (on page 409)

Order of Import for Multiple XML Files

If a Tripwire Enterprise object in an XML file references another TE object in a different XML file, an error may occur if you attempt to import the first object before the second object. For example, if you import a report with criteria that cites a node in a different XML file, you should import the node file before the report file.

To avoid errors when importing multiple XML files, you should import the files in the order indicated below. From start to finish, you should import XML files containing:

1. Settings
2. Nodes and node groups
3. Rules and rule groups
4. Actions and action groups
5. Policy tests, policies, and policy groups
6. Reports, report groups, and dashboards
7. Tasks and task groups
8. Home pages

What are Pre-Configured Rules and Policies?

For your convenience, Tripwire has developed a collection of pre-configured rules and TE policies. On the Tripwire Web site, you can create and download a zip file containing these objects. Each zip file contains XML files which can then be imported to the Rule Manager and Policy Manager. Once done, you can either use these objects with their default properties, or modify their properties to support your organization's needs.

To download pre-configured rules and TE policies with your License Agreement Card (provided with your Tripwire Enterprise license), go to:

<https://license.tripwire.com>

To download pre-configured rules and TE policies with a Tripwire Support Login, go to:

<https://tripwireinc.force.com/customers>

When you create a zip file on the Tripwire Web site, you specify the TE objects to be included in the zip file. A zip file includes one or more XML files containing:

- Pre-configured rules for change auditing, or
- Pre-configured TE policies for configuration assessment. In this case, the zip file also contains one or more XML files with pre-configured rules specified in the properties of the policy tests in each selected TE policy. Pre-configured TE policies and policy tests evaluate compliance of monitored systems with current guidelines and requirements established by industry standards organizations, such as the Payment Card Industry (PCI). For more information about TE policies and policy tests, see [What are Policy Manager Objects?](#) on page 131.

Tip Each zip file downloaded from the Tripwire Web site includes a readme file, which provides information about the pre-configured objects in the zip file. Prior to importing the XML files in a zip file, you should read the enclosed readme file.

Caution If you import TE policy XML files to update previously imported pre-configured policy objects, you should import all of the XML files in the related zip file at the same time. If you fail to do so, some policy tests may fail to run properly.

How Do I Manage User Access for Pre-Configured Rules and Policies?

To simplify user access, Tripwire applies access controls to some pre-configured TE objects in each XML file. [Table 64 \(on the next page\)](#) identifies those objects, along with the components of their access controls.

- For an explanation of how access controls work, see [What are Access Controls?](#) on page 208.
- For descriptions of the Rule Manager, Rule User, Policy Manager, and Policy User user roles, see [Table 61 on page 205](#).

The user groups listed in [Table 64](#) are created automatically when Tripwire Enterprise is installed. To grant a user access to pre-configured TE objects, simply add the user's account to these groups (see [Working with User Groups](#) on page 289).

- To grant someone full control over pre-configured rules and rule groups, add their user account to the Rule Manager user group.
- To grant someone the ability to use pre-configured rules in baseline operations and version checks, add their account to the Rule User group.
- To grant someone full control over pre-configured policies, policy tests, and policy test groups, add their user account to the Policy Manager user group.
- To grant someone the ability to run pre-configured policy tests, add their account to the Policy User group.

Table 64. Access controls for TE objects in pre-configured XML files

Pre-configured TE Object	Components of Access Control(s)
A rule group at the top level of the group hierarchy in a rule XML file	Access Control User group = Rule Manager Group User role = Rule Manager
A rule	Access Control #1 User group = Rule Manager Group User role = Rule Manager Access Control #2 User group = Rule User Group User role = Rule User
A policy test group at the top level of the group hierarchy in a policy XML file	Access Control User group = Policy Manager Group User role = Policy Manager
A policy test	Access Control #1 User group = Policy Manager Group User role = Policy Manager Access Control #2 User group = Policy User Group User role = Policy User

How Did Pre-Configured XML Files Change in Tripwire Enterprise 7.1?

In Tripwire Enterprise 7.1, Tripwire introduced TE policies, policy scores, waivers, weights, and scoring thresholds. To support these new Policy Manager features, Tripwire also upgraded the contents of the pre-configured **XML files** available on the Tripwire Web site (see [What are Pre-Configured Rules and Policies? on page 219](#)). If you upgraded to this version of TE from a version of TE earlier than 7.1 in which you imported pre-configured TE objects from Tripwire's XML files, you can update those objects by importing the new XML files.

- Each object in Tripwire's XML files now has a Tracking ID (see [What are Tracking Identifiers? on page 223](#)).
- Tripwire's policy XML files *can only* be imported to TE Console 7.1 and later.
- If you import a policy XML file created for an earlier version of Tripwire Enterprise, the imported policy objects will *not* support the new functionality introduced with TE 7.1.

How Does Tripwire Enterprise Import an XML File?

When you import an XML file to a Manager other than the Settings Manager, you select a **destination group** in the Manager's group hierarchy. Tripwire Enterprise will then import the contents of the file to the selected group.

If an XML file contains a hierarchy of groups, TE replicates the hierarchy in the destination group. TE first imports the TE objects on the top level of the XML file's group hierarchy, then the objects on the second level, and so on.

When importing a TE object from an XML file to a Manager, Tripwire Enterprise looks for a **matching object** in the Manager. A matching object must be the same type of object as the imported object, and it must share the same name and/or Tracking Identifier (see [What are Tracking Identifiers? on the next page](#)).

In some cases, Tripwire Enterprise may compare the **positions** of an imported object and matching object to determine the appropriate course of action. An object's position refers to the hierarchy of groups from which the object is descended. For example, consider an imported rule in the following sub-group of the XML root group:

```
XML Root Group
> Sub_Group_A
>> Sub_Group_B
```

If a matching rule is contained in the following sub-group in the Rule Manager, the imported rule and matching rule are said to occupy the same position.

```
Rule Manager Root Group
> Sub_Group_A
>> Sub_Group_B
```

Depending on the type of imported object, TE may also reference a matching object's import timestamp and modification timestamp.

- A TE object only has an **import timestamp** if the object was originally created by importing the contents of an XML file. In this case, the import timestamp indicates the date and time when the object was imported.
- A **modification timestamp** indicates the last time the object was changed in any way. If an object has not been altered since it was created or imported, the modification timestamp reflects the time of creation or import.

The process employed by TE to import an object from an XML file varies by object type. For further details, see:

- [XML-File Import of Settings \(on page 225\)](#)
- [XML-File Import of Home Pages \(on page 226\)](#)
- [XML-File Import of Groups \(on page 226\)](#)
- [XML-File Import of Nodes \(on page 227\)](#)
- [XML-File Import of VI Nodes and Node Groups \(on page 228\)](#)
- [XML-File Import of TE Policies \(on page 229\)](#)
- [XML-File Import of Rules, Actions, Tasks, Policy Tests, Reports, and Dashboards \(on page 230\)](#)

What are Tracking Identifiers?

A **Tracking Identifier** (TID) is a unique code that identifies a rule, rule group, TE policy, policy test, policy test group, or home page. When creating one of these TE objects, you have the option of assigning a **TID** to the object. If the object is later exported to another system, the object's TID remains the same. In addition, TE may refer to an object's TID to determine the appropriate steps when an XML file is imported to a TE installation (see [How Does Tripwire Enterprise Import an XML File? on the previous page](#)).

If you create a TE object with a TID, you can later remove the TID by clearing the **Enable Tracking Identifier** check box in the General tab of the object's properties dialog. Similarly, you can add a TID to an object by selecting the check box. To change this setting for an object, see:

- [Changing the Properties of a Rule \(on page 437\)](#)
- [Changing the Properties of a Rule Group \(on page 440\)](#)
- [Changing the Properties of a TE Policy \(on page 534\)](#)
- [Changing the Properties of a Policy Test \(on page 536\)](#)
- [Changing the Properties of a Policy Test Group \(on page 538\)](#)
- [Changing the Properties of a Home Page \(on page 291\)](#)

Every TE object in a pre-configured zip file has a TID that cannot be removed from the object. For more information about pre-configured zip files, see [What are Pre-Configured Rules and Policies? on page 219](#).

What are Import Conflicts?

A conflict indicates an unresolved discrepancy between the content of an imported XML file and the destination group (see [Table 65](#)). If one or more conflicts are detected during an import operation, TE presents a list of the conflicts when the import finishes. In the conflict dialog, you can then specify how TE should resolve each conflict.

Note Tripwire Enterprise only reports Removal and Clean Up conflicts if the imported object has a Tracking Identifier.

Table 65. Types of import conflicts

Conflict Type	Can occur with ...	Description
Update	Any TE object	Indicates an object that was created by a previous import operation and has since been modified. You have the option of retaining the object, or over-writing its properties with the properties of the XML object.
Removal	Rules Rule groups Policies Policy tests Policy test groups	Indicates an object in the destination group that has a Tracking Identifier but no counterpart in the XML file. You have the option of retaining or unlinking the object.
Scoring	Policies	Indicates a matching policy with a different scoring range from its imported XML counterpart. You have the option of retaining the existing scoring range, or over-writing it with the range defined for the XML policy.
Clean Up	Rules Rule groups Policy tests Policy test groups	Indicates an object in the destination group that lacks a Tracking Identifier. You have the option of retaining or unlinking the object. Note: In the Policy Manager, a Clean Up conflict can only occur with a policy test or policy test group descended from a policy.

XML-File Import of Settings

Note This section explains how Tripwire Enterprise imports an XML settings file with the Import Settings page in the Settings Manager. To learn how TE imports an XML file containing home pages, see [XML-File Import of Home Pages on the next page](#).

In the Settings Manager, each setting consists of either TE objects or a collection of specified values. For example, the Severity Ranges and Home Pages settings contain TE objects (either severity ranges or home pages), while the User Differences setting contains a set of defined values.

When importing a setting that consists of a **set of defined values**, TE assesses each value (for example, the **Table Page Size** value in User Differences). If a value differs between the XML file and the Settings Manager, TE over-writes the value in the Settings Manager. Otherwise, no action is taken.

In the Settings Manager, the following fields contain a list of text entries:

- **Integration hosts** in System Preferences
- **Binary attributes** in LDAP Directories
- **Binary attributes** and **security attributes** in Active Directories

When importing these lists, Tripwire Enterprise only imports entries that do *not* appear in the Settings Manager. If an entry exists in the Settings Manager but not the XML file, no action is taken.

When importing TE objects other than home pages to the Settings Manager, Tripwire Enterprise determines if the object has a matching object with the same name.

- If not, TE imports the object from the XML file.
- If so, TE overwrites the properties of the matching object, unless the properties of the two objects are identical.

XML-File Import of Home Pages

For an introduction to the XML import process and TIDs, see:

- [How Does Tripwire Enterprise Import an XML File? \(on page 222\)](#)
- [What are Tracking Identifiers? \(on page 223\)](#)

When importing a home page from an XML file to the Settings Manager, TE makes the following decisions to determine the appropriate action:

1. Does the XML home page have a **Tracking Identifier (TID)**?
 - If so, go to [step 2](#).
 - If not, TE imports the home page.
2. Does an existing home page have the same **TID** as the XML home page?
 - If so, TE over-writes the home page's properties with the properties of the XML home page.
 - If not, TE imports the home page.

XML-File Import of Groups

For an introduction to the XML import process and TIDs, see:

- [How Does Tripwire Enterprise Import an XML File? \(on page 222\)](#)
- [What are Tracking Identifiers? \(on page 223\)](#)

When importing a group from an XML file to a Manager, TE makes the following decisions to determine the appropriate action:

1. Does the XML group have a **Tracking Identifier (TID)**?
 - If so, go to [step 2](#).
 - If not, go to [step 3](#).
2. Does the destination group contain a matching group that has the same **TID** as the XML group?
 - If so, TE replaces the matching group's links with the links defined for the XML group in the XML file. TE then proceeds to [step 4](#).
 - If not, go to [step 3](#).
3. Does the destination group contain a matching group that has the same **name** and **position** as the XML group?
 - If so, go to [step 4](#).
 - If not, TE imports the XML group.

4. Does the matching group have an **import timestamp**?
 - If so, go to [step 5](#).
 - If not, TE presents the user with an Update conflict in the import conflict list (see [What are Import Conflicts? on page 224](#)).
5. Is the matching group's **modification timestamp** more recent than its import timestamp?
 - If so, TE presents the user with an Update conflict in the import conflict list (see [What are Import Conflicts? on page 224](#)).
 - If not, TE over-writes the matching group's properties with the properties of the XML group.

XML-File Import of Nodes

For an introduction to the XML import process, see [How Does Tripwire Enterprise Import an XML File? on page 222](#).

For information about the import of VI nodes, see [XML-File Import of VI Nodes and Node Groups on the next page](#).

When importing a node from an XML file to the Node Manager, Tripwire Enterprise makes the following decisions to determine the appropriate action:

1. In the Node Manager, does the destination group contain a **matching node** with the same name and type as the XML node?
 - If so, proceed to [step 2](#).
 - If not, proceed to [step 3](#).
2. Do the matching node and XML node have **identical properties**?
 - If so, TE retains the matching node.
 - If not, proceed to [step 3](#).
3. Do any matching nodes with identical properties exist in other node groups?
 - If so, TE creates a linked node that references one of the matching nodes (selected at random by TE). For more information, see [What are Links and Linked Objects? on page 213](#).
 - If not, TE imports the node.

XML-File Import of VI Nodes and Node Groups

For an introduction to VI nodes, see [Monitoring Virtual Systems with Tripwire Enterprise on page 59](#).

- To learn how Tripwire Enterprise imports a VI management node from an XML file, see [Import of VI Management Nodes](#) below.
- To learn how Tripwire Enterprise imports a VI node or node group that does not have a parent VI management node in the XML file, see [Import of VI Nodes and Node Groups without a VI Management Node](#) on the next page.

Note When importing VI nodes managed by a parent VI management node, make sure that the parent node is imported in the same XML file, or has previously been imported into Tripwire Enterprise.

Import of VI Management Nodes

If you export one or more VI management nodes (e.g. vCenter nodes), TE saves the properties of each selected node in the XML file. For each VI hypervisor node descended from a VI management node, TE also saves the following properties (as applicable):

- The username and password used by the hypervisor for HTTP connections
- The username, password, and SSH key file used by the hypervisor for SSH connections

When importing a VI management node from an XML file to the Node Manager, Tripwire Enterprise makes the following decisions to determine the appropriate action:

1. Does the Node Manager contain a matching VI management node that has the same **hostname** or **IP address** as the XML VI management node?
 - If so, go to [step 2](#).
 - If not, go to [step 3](#).
2. TE creates a link to the matching VI management node in the destination node group, and presents the user with an Update conflict in the import conflict list (see [What are Import Conflicts? on page 224](#)). Does the user elect to over-write the VI management node?
 - If so, TE replaces the properties of the VI management node and all descendant nodes with the properties defined in the XML file. However, the hierarchy of VI nodes remains unchanged.
 - If not, no further action is taken.
3. TE creates the VI management node and initiates the VI discovery process. If the discovery process results in the creation of a VI node with a matching node in the XML file, TE over-writes the VI node's properties with the properties of the matching node. For more information, see [Monitoring Virtual Systems with Tripwire Enterprise on page 59](#).

Import of VI Nodes and Node Groups without a VI Management Node

A **managed object ID** (MOID) is a unique identifier for each inventory object in a VMware virtual infrastructure. When a VMware VI management node (e.g. vCenter node) is created in the Node Manager, Tripwire Enterprise saves the MOID of each inventory object in the properties of the object's node or node group. When a VI node or node group is exported to an XML file, TE saves the object's MOID and the name of its vCenter (or VirtualCenter) in the XML file.

Note When importing VI nodes managed by a parent VI management node, make sure that the parent node is imported in the same XML file, or has previously been imported into Tripwire Enterprise.

When importing a VI node or node group that is not descended from a VMware VI management node in the XML file, Tripwire Enterprise makes the following decisions to determine the appropriate action:

1. Does the Node Manager contain a VI management node that has the same **hostname** or **IP address** as the XML object's VI management node?
 - If so, go to [step 2](#).
 - If not, Tripwire Enterprise presents the user with an error message.
2. Does the VI management node contain an object with a matching MOID?
 - If so, TE links the matching object to the destination group.
 - If not, Tripwire Enterprise creates an Error message in the Log Manager.

XML-File Import of TE Policies

For an introduction to the XML import process and TIDs, see:

- [How Does Tripwire Enterprise Import an XML File? \(on page 222\)](#)
- [What are Tracking Identifiers? \(on page 223\)](#)

When importing a TE policy from an XML file to the Policy Manager, Tripwire Enterprise makes the following decisions to determine the appropriate action:

1. Does the XML TE policy have a **Tracking Identifier (TID)**?
 - If so, go to [step 2](#).
 - If not, go to [step 3](#).
2. Does the destination group contain a matching TE policy that has the same **TID** as the XML TE policy?
 - If so, TE replaces the matching TE policy's links with the links defined for the XML TE policy in the XML file. TE then proceeds to [step 5](#).
 - If not, go to [step 3](#).

3. Does the destination group contain a matching TE policy or policy test group that has the **same name** and **position** as the XML TE policy?
 - If so, go to [step 4](#).
 - If not, TE imports the XML policy and its contents.
4. Is the matching object a **policy test group**?
 - If so, TE replaces the group with the XML TE policy.
 - If not, go to [step 5](#).
5. Does the matching TE policy have an **import timestamp**?
 - If so, go to [step 6](#).
 - If not, TE over-writes the matching TE policy's properties, but retains the TE policy's scoring range. TE then proceeds to [step 7](#).
6. Is the matching TE policy's **modification timestamp** more recent than its import timestamp?
 - If so, TE presents the user with an Update conflict in the import conflict list (see [What are Import Conflicts? on page 224](#)).
 - If not, TE over-writes the matching TE policy's properties, but retains the TE policy's scoring range. TE then proceeds to [step 7](#).
7. Are the **scoring ranges** of the XML TE policy and matching TE policy identical?
 - If so, no further action is taken.
 - If not, TE presents the user with a Scoring conflict in the import conflict list (see [What are Import Conflicts? on page 224](#)).

Next The policy tests under each imported TE policy will not run until you specify one or more nodes in the policy's scope properties. To define the scope for a TE policy, see [Changing the Properties of a TE Policy on page 534](#).

XML-File Import of Rules, Actions, Tasks, Policy Tests, Reports, and Dashboards

For an introduction to the XML import process and TIDs, see:

- [How Does Tripwire Enterprise Import an XML File? \(on page 222\)](#)
- [What are Tracking Identifiers? \(on page 223\)](#)

When importing a rule, action, task, policy test, report, or dashboard from an XML file to a Manager, Tripwire Enterprise makes the following decisions to determine the appropriate action:

1. Does the XML object have a **Tracking Identifier (TID)**?
 - If so, go to [step 2](#).
 - If not, go to [step 3](#).
2. Does the destination group contain a matching object that has the same **TID** as the XML object?
 - If so, TE replaces the matching object's links with the links defined for the XML object in the XML file. TE then proceeds to [step 5](#).
 - If not, go to [step 3](#).
3. Does the destination group contain a matching object that has the same **name** and **position** as the XML object?
 - If so, go to [step 5](#).
 - If not, go to [step 4](#).
4. Do any other groups in the Manager contain any matching objects that have a name and properties identical to the XML object?
 - If so, TE creates a linked object that references one of the matching objects (selected at random by TE). For more information, see [What are Links and Linked Objects? on page 213](#).
 - If not, TE imports the XML object.
5. Does the matching object have an **import timestamp**?
 - If so, go to [step 6](#).
 - If not, TE over-writes the matching object's properties with the properties of the XML object.
6. Is the matching object's modification timestamp more recent than its import timestamp?
 - If so, TE presents the user with an Update conflict in the import conflict list (see [What are Import Conflicts? on page 224](#)).
 - If not, TE over-writes the matching object's properties with the properties of the XML object.

Note If a policy test lacks a TID, and its properties are over-written by an XML policy test that has a TID, TE retains any excluded nodes specified in the test's properties.

Searching for Tripwire Enterprise Objects

How Do I Run a Search?

Tripwire Enterprise includes a robust search engine for the retrieval of data stored in the Tripwire Enterprise Console database. To run a search, you enter search criteria in a **search tab** in a Manager.

- [Table 66](#) identifies the search tabs in Tripwire Enterprise, along with the data that can be retrieved in each tab.
- Each search tab includes a unique set of search criteria. However, some features and functions are common to all search tabs. For further details, see [Table 67 on the next page](#).

Table 66. Search tabs

Search Tab	Searches for ...
Node Search	... nodes (see Searching for Nodes on page 355)
Element Search	... elements (see Searching for Elements on page 361)
Version Search	... element versions (see Searching for Element Versions on page 364)
Rule Search	... rules (see Searching for Rules on page 434)
Action Search	... actions (see Searching for Actions on page 480)
Task Search	... tasks (see Searching for Tasks on page 510)
Test Search	... policy tests (see Searching for Policy Tests on page 532)
Result Search	... policy test results (see Searching for Policy Test Results on page 559)
Waiver Search	... policy waivers (see Searching for Waivers on page 567)
Message Search	... TE log messages (see Searching for TE Log Messages on page 579)
Log Center Events	... TLC log messages (see Searching for TLC Log Messages on page 581)
Report Search	... reports (see Searching for Reports on page 587)



Table 67. Common search features

Feature	Description
wildcards	<p>If appropriate, you can enter wildcards in some search-criteria text fields.</p> <ul style="list-style-type: none"> • The ? wildcard represents a single character. • The * wildcard represents any number of characters (including zero). <p>For example, if you enter <code>Cisco*Configuration</code> in the Name field of the Rule Search tab, the search would return rules with the following names:</p> <ul style="list-style-type: none"> • Cisco CatOS Configuration Rule • Cisco IOS Configuration Rule • Cisco PIX Configuration Rule
text-field qualifiers	<p>A text-field qualifier determines how the search engine utilizes criteria entered in a text field. Users may select one of the following qualifiers from a drop-down menu adjacent to each search-criteria text field:</p> <ul style="list-style-type: none"> • Contains. This option retrieves all objects with any of the entered keywords. • Excludes. This option omits any objects with the entered keywords from search results. • Equals. This option retrieves only those objects that exactly match the entered keywords. • Not equal. This option omits any objects that exactly match the entered keywords.
saved searches	<p>For your convenience, entered search criteria can be stored as a saved search for future use. To create a saved search, you simply enter the desired search criteria in a search tab, and then save your entries. A saved search may be made available to all users or reserved exclusively for your own use.</p> <p>Once a saved search has been created, it may be loaded from the relevant search tab. When a saved search is loaded, the stored search criteria automatically populate the relevant search fields and menus.</p> <p>For related procedures, see:</p> <ul style="list-style-type: none"> • Creating a Saved Search (on the next page) • Loading a Saved Search (on the next page) • Deleting, Importing, and Exporting Saved Searches (on page 235) • Creating a Launch-in-Context URL (on page 235)

Creating a Saved Search

For an introduction to saved searches, see [How Do I Run a Search? on page 232](#).

To save a search:

1. Select a Manager search tab.
2. Enter search criteria. For field definitions, click  **Help**.
3. Click **Saved** >  **Save**.
4. In the Save Search dialog, enter a **Search name**.
5. (Optional) Select **Make search available to all users**. If this option is *not* selected, only the current user will have access to the saved search.


Note To make a search available to all users, you must have the **Manage system searches** permission assigned to your user account.

6. Click **OK**.


Loading a Saved Search

For an introduction to saved searches, see [How Do I Run a Search? on page 232](#).

To load a saved search:

1. Select a Manager search tab.
2. Click **Saved** >  **Load**.
3. In the Load Search dialog, select a saved search.


Tip Selected by default, the **Perform search** setting instructs the application to retrieve search results immediately after loading the search.

4. Click **OK**. The saved search criteria populates the search fields.
5. If appropriate, you can edit the loaded search criteria. For field definitions, click  **Help**.


Deleting, Importing, and Exporting Saved Searches

For an introduction to saved searches, see [How Do I Run a Search?](#) on page 232.

To delete, import, or export saved searches:

1. Select a Manager search tab.
2. Click **Saved** >  **Admin**.
3. To delete saved searches, select the check box of each search to be deleted and click **Delete**.

To import saved searches, click  **Import**.

To export saved searches, select the check box of each saved search to be exported and click  **Export**.



Tips For more information, click  **Help**.

The **Import** and **Export** buttons are not available for all types of saved searches.

Creating a Launch-in-Context URL

In any search tab of the Node Manager or Policy Manager, you may create a Launch-in-Context (LIC) URL for displayed search results. If another user enters one of these URLs in their Web browser, the same search tab opens with the specified search results.

To create a Launch-in-Context URL:

1. Select a Node or Policy Manager search tab.
2. Enter search criteria and click  **Search**.
3. Click **Saved** >  **URL**.

The Link dialog opens and presents the Launch-in-Context URL for the search results in the current view.

Using Launch-in-Context URLs

As specified in [Creating a Launch-in-Context URL on the previous page](#), you can create a Launch-in-Context (LIC) URL for a specific set of search criteria. This LIC URL will open Tripwire Enterprise to the same search tab with the results of the previous search criteria.

In addition, you can use LIC URLs to launch TE in the following ways:

To launch TE with the Node Search tab open to a node with a specific IP address:

```
https://<TE_Server>/rest/nodeManager/nodeSearch  
?q=ipAddress%3D%22<IP_address>%22
```

For example:

```
https://TEserver/rest/nodeManager/nodeSearch  
?q=ipAddress%3D%22192.168.0.123%22
```

To launch TE with the Node Search tab open to all nodes containing part of an IP address:

```
https://<TE_Server>/rest/nodeManager/nodeSearch  
?q=ipAddress%3D~%22<IP_Address_fragment>%22
```

For example:

```
https://TEserver/rest/nodeManager/nodeSearch?q=ipAddress%3D~%22.123%22
```

To launch TE with the Element Search tab open to an element with a specific OID:

```
https://<TE_Server>/rest/nodeManager/elementSearch  
?q=elementOid%3D%22<element_OID>%22
```

For example:

```
https://TEserver/rest/nodeManager/elementSearch  
?q=elementOid%3D%22-1y2p0ij32e8ci:-1y2p0ij32c297%22
```

Tip To determine an element's OID, click the element in the Node Manager to open the Property Editor dialog. The element's OID is listed in the URL for this dialog. OIDs are composed of two strings separated by a : character.

Integrating Tripwire Enterprise with Other Applications

What is the Tripwire Enterprise AAA Log Monitoring Tool?

The **Tripwire Enterprise AAA Log Monitoring Tool** is a Perl-based application that monitors log files created by a AAA (authentication, authorization, and accounting) server. Each AAA log file contains one or more log messages. As new entries are added to a AAA log file, the log monitoring tool periodically parses and forwards the entries to the Tripwire Enterprise Server.

- If a AAA log message was generated by activity on a monitored system, a new TE log message is created in the Log Manager.
- If you integrated TE with Tripwire Log Center (TLC), then TE will also forward AAA log messages to TLC.

Notes In the Log Manager, Tripwire Enterprise assigns a **Category** of TACACS+ or RADIUS to each TE log message originating with the Tripwire Enterprise AAA Log Monitoring Tool.

TACACS (Terminal Access Controller Access Control System) is a network-access protocol that authenticates users by allowing a remote access server to communicate with an authentication server. **RADIUS** (Remote Authentication Dial-In User Service) is an authentication protocol used in communications between a remote access server and an authentication server.

The Tripwire Enterprise AAA Log Monitoring Tool can parse log files created by the following auditing services:

- Cisco Secure ACS for Windows TACACS+ administration and accounting
- Cisco Secure ACS for Windows RADIUS accounting
- Cisco Secure ACS Appliance TACACS+ administration and accounting
- Cisco Secure ACS Appliance RADIUS accounting
- tac_plus
- RADIUS (with Livingston format logs)

For system requirements, installation instructions, and usage guidelines, see *Working with the Tripwire Enterprise AAA Log Monitoring Tool* in the *Tripwire Enterprise Reference Guide*.

What is the Command Line Interface?

The **Command Line Interface** (CLI) is a utility that allows you to run Tripwire Enterprise functions without using the TE interface. Once the CLI has been installed on a system, you can perform a number of Tripwire Enterprise operations from the command line of the CLI host machine. To complete an operation, the CLI host machine communicates with the Tripwire Enterprise Server over a secure network connection.

With the Command Line Interface, you can perform a variety of functions, including:

- Defining global and local variables
- Baselineing monitored objects
- Version checking monitored objects
- Promoting element versions to the baseline
- Setting values for custom properties
- Running actions and reports
- Importing XML files containing nodes, rules, or actions
- Creating launch in context URLs

You can also write a customized integration program with the Command Line Interface. A CLI-scripted program can automatically run a Tripwire Enterprise function when an event occurs in another application. For example, if a change request is authorized in a change management system (CMS), an integration program could instruct Tripwire Enterprise to promote the associated change versions.

The Command Line Interface is language- and platform-independent. Therefore, integration programs may be written in any programming language supported by the host operating system.

For CLI commands, options, and installation instructions, see *Working with the Command Line Interface* in the *Tripwire Enterprise Reference Guide*.

Chapter 4. Home Page Procedures

Viewing, Creating, and Deleting Objects in the Home Page Manager

Viewing Home Pages and Widgets

For an introduction to home pages and widgets, see [What are Home Pages and Widgets?](#) on page 189.

To view home pages in the Home Page Manager:

1. In the Manager bar, click **HOME**.

If your user account lacks the Manage home page permission and is not currently assigned to any home pages, the default Welcome page opens. To proceed further in the Home Page Manager, your account must be assigned to at least one home page.

2. The main pane contains a tab for each home page to which your user account is currently assigned, as well as the Create New Home Page tab.
 - To view the widgets in a home page, select the tab for the page.
 - To create a new home page, select the **Create New Home Page** tab. For further instructions, see [Creating a Home Page on the next page](#).
 - To edit an existing home page, see [Changing the Properties of a Home Page on page 242](#).

If your user account is not currently assigned to any home pages, the main pane displays the default Welcome tab.

[Table 68 \(below\)](#) describes each of the tabs in the Configuration pane.

Table 68. Tabs in the Configuration pane of the Home Page Manager

Tab	Description
Widgets	Includes links to add widgets to a home page selected in the main pane. For more information, see Adding a Widget to a Home Page on page 245 .
Home Pages	<p>If your user account has the Manage home page permission, the Home Pages tab lists all existing home pages in Tripwire Enterprise. In this case, you can assign/unassign your account to/from a home page by selecting/clearing the check box for the page. If no home pages exist, Tripwire Enterprise displays the default Welcome tab.</p> <p>If your account lacks the Manage home page permission, but has the Manage Own home page permission, the Home Pages tab lists all home pages to which your account is currently assigned. If your account is not assigned to any home pages, Tripwire Enterprise displays the default Welcome tab.</p>
Users	<p>If your user account has the Manage home page permission, the Users tab lists all existing user accounts in Tripwire Enterprise. In this case, you can assign/unassign a user account to/from the home page currently selected in the main pane by selecting/clearing the check box for the account.</p> <p>If your account lacks the Manage home page permission, but has the Manage Own home page permission, the Users tab lists all user accounts assigned to the home page currently selected in the main pane.</p>

Creating a Home Page

For an introduction to home pages, see [What are Home Pages and Widgets?](#) on page 189.

To create a new home page in the Settings Manager, see [Creating a Home Page](#) on page 290.

To create a new home page in the Home Page Manager:

1. In the Manager bar, click **HOME**.
2. In the main pane, select the **Create New Home Page** tab. Tripwire Enterprise opens a new tab labeled 'NEW Home Page.'
3. To name the new home page:
 - a. In the Configuration pane, select the **Home Pages** tab.
 - b. Click 'NEW home page' and enter a name for the page.
4. To add widgets to the new home page:
 - a. In the Configuration pane, select the **Widgets** tab.
 - b. In the Widgets tab, select a type of widget. TE adds the widget in the main pane.
 - c. To configure the new widget, refer to one of the following procedures:
 - [Changing the Properties of an Alert Widget](#) (on page 246)
 - [Changing the Properties of a Dashboard Widget](#) (on page 248)
 - [Changing the Properties of a Failing Tests Widget](#) (on page 250)
 - [Changing the Properties of a Log Center Event Widget](#) (on page 251)
 - [Changing the Properties of a Report Widget](#) (on page 251)
 - [Changing the Name of a Remediation Work Order Widget](#) (on page 254)
 - d. Repeat the steps above to add other widgets.
5. (Requires the Manage home page permission) To assign user accounts to the new home page:
 - a. In the Configuration pane, select the **Users** tab.
 - b. In the Users tab, select the check box of each user account.

Changing the Properties of a Home Page

For an introduction to home pages, see [What are Home Pages and Widgets? on page 189](#). To change the properties of a home page, see:

- [Changing the Name of a Home Page \(below\)](#)
- [Changing the Layout of Regions and Widgets in a Home Page \(below\)](#)
- [Changing the List of User Accounts Assigned to a Home Page \(on the next page\)](#)

Changing the Name of a Home Page

This procedure explains how to change the name of a home page in the Home Page Manager. To change the name of a home page in the Settings Manager, see [Changing the Properties of a Home Page on page 291](#).

To change the name of a home page:




1. In the Manager bar, click **HOME**.
2. In the Configuration pane, select the **Home Pages** tab.
3. In the Name column, click the home page.
4. Edit the name of the page and press **ENTER**.

Changing the Layout of Regions and Widgets in a Home Page

With this procedure, you can make the following changes to a home page:

- Show or hide the contents of the Top or Bottom region.
- Change the number of columns in a region.
- Re-arrange the home page's widgets.

To change the layout of an existing home page:

1. In the Manager bar, click **HOME**.
2. In the **Home Pages** tab of the Configuration pane, select the check box for the home page.
3. In the main pane, select the tab for the home page.
 - To show or hide the Top or Bottom Region, click the arrow button in the divider bar separating the region from the Middle Region.
 - To move a widget, click the widget's title bar and drag to the new position.
 - To conceal or display a widget's content, click  or  in the widget's title bar.
4. To change the number of columns in a region, click  (in the upper left corner of the region) and select the number of columns.

Note To change the properties of widgets in a home page, see:

- [Changing the Properties of an Alert Widget \(on page 246\)](#)
- [Changing the Properties of a Dashboard Widget \(on page 248\)](#)
- [Changing the Properties of a Failing Tests Widget \(on page 250\)](#)
- [Changing the Properties of a Log Center Event Widget \(on page 251\)](#)
- [Changing the Properties of a Report Widget \(on page 251\)](#)
- [Changing the Name of a Remediation Work Order Widget \(on page 254\)](#)

Changing the List of User Accounts Assigned to a Home Page

If your user account has the Manage home page permission, you can modify the list of user accounts assigned to any home page.

This procedure explains how to change the list of user accounts assigned to a home page in the Home Page Manager. To change the list of accounts for a home page in the Settings Manager, see [Changing the Properties of a Home Page on page 291](#).

To change the list of accounts for a home page:

1. In the Manager bar, click **HOME**.
2. In the Configuration pane, select the **Home Pages** tab and select the check box for the home page.
3. In the main pane, select the tab for the home page.
4. In the Configuration pane, select the **Users** tab.
5. Specify the user accounts for the page.
 - To assign a user account to the page, select the account's check box.
 - To unassign a user account, clear the account's check box.


To change the list of home pages to which your own user account is assigned:

1. In the Manager bar, click **HOME**.
2. In the Configuration pane, select the **Home Pages** tab.
3. Specify the home pages to which your user account will be assigned.
 - To assign your account to a home page, select the page's check box.
 - To unassign your account from a page, clear the page's check box.

Duplicating a Home Page

This procedure explains how to duplicate a home page in the Home Page Manager. To duplicate a home page in the Settings Manager, see [Duplicating a Home Page on page 290](#).

To duplicate an existing home page:

1. In the Manager bar, click **HOME**.
2. In the Configuration pane, select the **Home Pages** tab.
3. Click  **Actions** for the home page and select **Duplicate**.

Tripwire Enterprise adds a copy of the home page to the Home Pages tab. TE uses the following format to name the copy:

Copy of <Name_of_Original>


Where <Name_of_Original> is the name of the home page that was duplicated.

<p>Note A copy of a home page will lack any of the user accounts assigned to the original home page. The only exception is when a user with the Manage Own home page permission duplicates a page. In this case, TE automatically assigns the user's account to the copy.</p>
--

Deleting a Home Page

This procedure explains how to delete a home page in the Home Page Manager. To delete a home page in the Settings Manager, see [Deleting Home Pages on page 291](#).

To delete a home page:

1. In the Manager bar, click **HOME**.
2. In the Configuration pane, select the **Home Pages** tab.
3. Click  **Actions** for the home page and select **Delete**.
4. In the confirmation dialog, click **OK**.
5. If multiple users are currently assigned to the home page, a second confirmation dialog opens. Click **Continue**.

Tripwire Enterprise removes the page from the Home Pages tab.

Working with Widgets

Adding a Widget to a Home Page

For an introduction to widgets, see *What are Home Pages and Widgets?* on page 189.

To add a widget to an existing home page:

1. In the Manager bar, click **HOME**.
2. In the main pane, select the tab for the home page.
3. In the Configuration pane, select the **Widgets** tab.
4. In the Widgets tab, select a type of widget.

TE adds the widget in the main pane.

Next To configure the widget, see:

- *Changing the Properties of an Alert Widget* (on the next page)
- *Changing the Properties of a Dashboard Widget* (on page 248)
- *Changing the Properties of a Failing Tests Widget* (on page 250)
- *Changing the Properties of a Log Center Event Widget* (on page 251)
- *Changing the Properties of a Report Widget* (on page 251)
- *Changing the Name of a Remediation Work Order Widget* (on page 254)

Working with an Alert Widget

For an introduction to alert widgets and alert generators, see [How Do Alert Widgets and Alert Generators Work?](#) on page 192.

For information on working with alert data in an alert generator, see:


- [Reviewing Alert Data in an Alert Generator](#) (on the next page)
- [Clearing Alert Data from an Alert Generator](#) (on the next page)



Changing the Properties of an Alert Widget

To change the properties of an alert widget in a home page:

1. In the Manager bar, click **HOME**.
2. In the main pane, select the tab for the home page.
3. In the widget's panel in the main pane, configure alert generators for the widget.

To add an alert generator, click  and select the type of generator.

To delete an alert generator, click the generator's  **Actions** button and select **Delete**.

To change the scope of an alert generator, click the generator's  **Actions** button and select **Configure**. The generator's properties dialog opens. For more information, click  **Help**.

Note Since the scope of a discovered nodes alert generator is limited to the Discovered Nodes Group, the Configure option does not appear in the Actions drop-down menu.


Table 69. Actions for alert generators in an alert widget

Action	Available with ...	Description
Clear Alert Data	... all alert generators	Removes all existing alert data from the alert generator.
Configure	... all alert generators except Discovered Nodes	Opens a dialog in which the scope of the alert generator may be configured.
Delete	... all alert generators	Removes the alert generator from the widget.

Action	Available with ...	Description
Open in Log Search	... all alert generators except Waiver Expiration	Opens the Message Search tab, which contains TE log messages related to events in the alert generator's scope. For information about the Message Search tab, see Searching for TE Log Messages on page 579 .
Open in Node Search	... all alert generators	Opens the Node Search tab, which contains the nodes in the alert generator's scope. For information about the Node Search tab, see Searching for Nodes on page 355 .
Open in Waiver Search	... Waiver Expiration alert generators only	Opens the Waiver Search tab, which contains the waivers in the alert generator's scope. For information about the Waiver Search tab, see Searching for Waivers on page 567 .
View Report	... Remediation Messages alert generators only	Generates reports related to automated remediation, using the Approval ID(s) of the remediation runs that are selected in the widget. If (default) is selected, TE runs the selected report with the default criteria applied.

Reviewing Alert Data in an Alert Generator


To view the latest data for an alert generator in an alert widget:

1. In the Manager bar, click **HOME**.
2. In the main pane, select the tab for the widget's home page.
3. In the widget's panel in the main pane, click  to the left of the alert generator. TE displays the alert data below the generator's heading.

Tip By default, Tripwire Enterprise displays all alert generators in an alert widget. To limit your view to alert generators with alert data, clear the widget's **View All** check box.

Clearing Alert Data from an Alert Generator

To clear all data generated by an alert generator in an alert widget:

1. In the Manager bar, click **HOME**.
2. In the main pane, select the tab for the widget's home page.
3. In the widget's panel in the main pane, click  **Actions** for the alert generator and select **Clear Alert Data**.


Working with a Dashboard Widget

For an introduction to dashboards and dashboard widgets, see:

- [What are Home Pages and Widgets? \(on page 189\)](#)
- [What are Dashboards? \(on page 182\)](#)

Changing the Properties of a Dashboard Widget

To change the properties of a dashboard widget in a home page:

1. In the Manager bar, click **HOME**.
2. In the main pane, select the tab for the home page.
3. In the widget's panel in the main pane, click  .
4. In the Property Editor, change the name and/or dashboard for the widget and click **OK**.

Tip To edit the reports or layout of the dashboard assigned to the widget, see [Changing the Properties of a Dashboard on page 591](#).

Running a Report in a Dashboard Widget

To run a report in a dashboard widget in a home page:

1. In the Manager bar, click **HOME**.
2. In the main pane, select the tab for the home page.
3. In the widget's panel, click the graph of the report.

The report output opens in the Report Viewer. For descriptions of the buttons in the Report Viewer, see [Table 137 on page 602](#).

Working with a Failing Tests Widget

The failing tests widget presents a list of failed policy tests that meet specified criteria. This widget can be used to create remediation work orders for automated remediation.


For an introduction to policy tests, see [How Does a Policy Test Work? on page 135](#). For more information on automated remediation, see [How Does Automated Remediation Work? on page 151](#).

Note This widget is only available if an Automated Remediation license is installed on the Tripwire Enterprise Console. For more information on licenses, see [About Tripwire Enterprise Licenses on page 202](#).

Viewing and Filtering Failing Policy Tests

To view and filter the policy tests displayed in a failing tests widget:

1. In the Manager bar, click **HOME**.
2. In the main pane, select the tab for the home page that contains the widget.
3. In the widget, expand and contract the groups to view the nodes and failed policy tests. The columns in the widget display the following information for each node group, policy, or policy group:
 - **Tests** shows the number of unique failed policy tests that are descended from a policy group or associated with the nodes descended from a node group.
 - **Nodes** shows the number of nodes descended from a node group that have at least one failure, or the number of nodes that have failures associated with a policy test descended from a policy group.
 - **Failures** shows the number of unique combinations of nodes and failed policy test that are descended from a node or policy group.

Tip Click the link for a policy test with automated remediation  to see the specific actions that the remediation will perform.

To change the way that failed policy tests are displayed, use the **View by** drop-down. If **Node View** is selected, tests are organized based on their node and node group. If **Policy View** is selected, tests are organized based on their policy and policy group.

To filter the types of policy tests that are displayed, use the **Filter** drop-down. You can filter policy tests based on the type of remediation associated with the test, the actions that are required to complete the remediation, and whether the tests are already in an open work order.


Creating a Remediation Work Order with a Failing Tests Widget

To create a remediation work order using a failing tests widget:

1. In the Manager bar, click **HOME**.
2. In the main pane, select the tab for the home page that contains the widget.
3. In the widget, select the nodes or policies for which you want to create a remediation work order. All of the selected objects will be included in a single work order. For more information on automated remediation, see [How Does Automated Remediation Work? on page 151](#).
4. Click **New Work Order** to create a new remediation work order.


Note If you selected failing policy tests that are already part of an open work order (a work order with any state other than Closed), those tests will not be added to a new work order. You may need to complete remediation on these policy test failures, or close the existing work order(s) if remediation is complete.

5. Complete the fields in the Remediation Work Order dialog.

Tip For more information on the fields and settings in the Remediation Work Order dialog, click  **Help** in any tab.

Changing the Properties of a Failing Tests Widget

To change the properties of a failing tests widget:

1. In the Manager bar, click **HOME**.
2. In the main pane, select the tab for the home page that contains the failing tests widget.
3. In the widget's panel in the main pane, click  .
4. In the **Configuration** tab, you can edit the **Title** of the widget. You can also set the node and policy criteria that the widget displays.

Tip For more information on the fields in the **Configuration** tab, click  **Help**.


5. Click **OK**.

Working with a Log Center Event Widget

For an introduction to Tripwire Log Center (TLC) and log center event widgets, see [What are Home Pages and Widgets? \(on page 189\)](#).

Changing the Properties of a Log Center Event Widget

To change the properties of a log center event widget in a home page:

1. In the Manager bar, click **HOME**.
2. In the main pane, select the tab for the home page.
3. In the widget's panel in the main pane, click  .
4. In the **General** tab of the Property Editor, enter a **Title** for the widget along with the criteria that specifies the TLC log messages to be displayed by the widget.

Tip For more information, click  **Help** in any tab.

5. In the **Columns** tab, specify the event fields to be displayed by the widget.
To add an event field to the widget, double-click the event field in the **Available Event Fields** panel.
To remove an event field from the widget, double-click the event field in the **Assigned Event Fields** panel.
6. Click **OK**.


Working with a Report Widget

For an introduction to reports and report widgets, see:

- [What are Home Pages and Widgets? \(on page 189\)](#)
- [What are Reports and Report Types? \(on page 172\)](#)

Changing the Properties of a Report Widget

To change the properties of a report widget in a home page:

1. In the Manager bar, click **HOME**.
2. In the main pane, select the tab for the home page.
3. In the widget's panel in the main pane, click  .
4. In the Property Editor, change the name and/or list of reports for the widget.
To add a report to the widget, select the report in the left-hand panel and click the right arrow.

To remove a report from the widget, select the report in the right-hand panel and click the left arrow.

5. Click **OK**.

Changing the Properties of a Report in a Report Widget

To change the properties of a report in a report widget in a home page:

1. In the Manager bar, click **HOME**.
2. In the main pane, select the tab for the home page.
3. In the widget's panel in the main pane, select the report's link in the **Name** column. The report's properties dialog opens.
4. Edit the report's properties and click **OK**.

For information about report properties and criteria, see [Changing the Properties of a Report on page 589](#).

Running a Report in a Report Widget

To run a report in a report widget in a home page:

1. In the Manager bar, click **HOME**.
2. In the main pane, select the tab for the home page.
3. In the widget's panel, select the report's **Run** link. Tripwire Enterprise compiles the report output and opens the Report Viewer. For descriptions of the buttons in the Report Viewer, see [Table 137 on page 602](#).

Tips To open the properties dialog of a report, select the report's link in the widget's Name column. For information about report properties and criteria, see [Changing the Properties of a Report on page 589](#).

To access a report in the Report Manager, select the report's **View** link in the widget's panel. When Tripwire Enterprise opens the Report Manager, the report group containing the report is automatically selected in the tree pane.

Working with a Remediation Work Order Widget

The remediation work order widget displays a list of work orders for automated remediation. This widget is used to view and edit work orders for various remediation tasks. For more information on working with work orders, see:

- [Creating a Remediation Work Order](#) (on page 255)
- [Assigning a Work Order](#) (on page 257)
- [Approving or Denying Remediation Entries in a Work Order](#) (on page 258)
- [Running or Deferring Remediation in a Work Order](#) (on page 259)
- [Closing or Deleting a Work Order](#) (on page 260)

For more information, see [How Does Automated Remediation Work?](#) on page 151.

<p>Note This widget is only available if an Automated Remediation license is installed on the Tripwire Enterprise Console. For more information on licenses, see About Tripwire Enterprise Licenses on page 202.</p>

Viewing and Filtering Work Orders

To change the way that work orders are displayed in a remediation work order widget:

1. In the Manager bar, click **HOME**.
2. In the main pane, select the tab for the home page that contains the widget.
3. **To change the columns displayed in the widget**, mouse over any of the column headers. Click the drop-down in the header, select **Columns**, then select the columns you want to display.

To filter work orders based on their current state, use the **Filter** drop-down. Work orders have the following states:


- **Created.** The work order has been created, but not all of the remediation entries in the work order have been approved or denied.
- **Reviewed.** All of the remediation entries in the work order have either been approved or denied, and at least one entry has been approved. However, not all of the remediation entries have been remediated or deferred.
- **Completed.** All of the remediation entries in the work order have been successfully remediated, denied, or deferred.
- **Closed.** The work order is Completed and has been closed.

To filter work orders based on their creator or current owner, use the **Filter** drop-down. You can choose to display work orders owned by individual users, or by a user group. If you select one or more user groups and check **Include all members of the selected groups**, the work orders owned by the members of the selected group(s) are also displayed in the widget.

For more information on the automated remediation workflow, see [How Does Automated Remediation Work?](#) on page 151

Changing the Name of a Remediation Work Order Widget


To change the name of a remediation work order widget:

1. In the Manager bar, click **HOME**.
2. In the main pane, select the tab for the home page that contains the widget.
3. In the widget's panel in the main pane, click  .
4. In the **Configuration** tab, edit the **Title** of the widget.
5. Click **OK**.

Deleting a Widget

For an introduction to widgets, see [What are Home Pages and Widgets?](#) on page 189.

To delete a widget in an existing home page:

1. In the Manager bar, click **HOME**.
2. In the main pane, select the tab for the home page.
3. In the widget's panel in the main pane, click  .
4. In the confirmation dialog, click **OK**.
5. If multiple users are currently assigned to the home page, a second confirmation dialog opens. Click **Continue**.

Working with Remediation Work Orders

Creating a Remediation Work Order

Remediation work orders are used to manage automated remediation in Tripwire Enterprise. For more information, see [How Does Automated Remediation Work?](#) on page 151.

In order to view or edit a remediation work order after you have created it, you must have a remediation work orders widget on one of the home pages that is assigned to your user account. For information on adding a widget, see [Adding a Widget to a Home Page](#) on page 245

Tip This procedure explains how to create a remediation work order in the Policies tab of the Policy Manager. However, you can also create a remediation work order in:

- The Test Search tab of the Policy Manager (see [Searching for Policy Tests](#) on page 532)
- The Result Search tab of the Policy Manager (see [Searching for Policy Test Results](#) on page 559)
- The Test Results tab of a node properties dialog (see [Promoting Policy Test Results Generated for a Node](#) on page 337)
- The Policy Test Result Report Table View dialog (see [Running a Report Manually](#) on page 601)
- A failing tests widget on the Home Page Manager (see [Viewing and Filtering Failing Policy Tests](#) on page 249)

To create a remediation work order:

1. In the Manager bar, click **POLICIES**.
2. In the main pane, select the **Tests** tab.
3. In the tree pane, select the TE policy or policy test group containing the policy tests for which you want to create the work order.
4. To create a work order for all policy tests in the selected object that have current test results that failed, proceed to step 5.


To create a work order for specific policy tests, select the check box of each Policy Manager object in the main pane. (In this case, only objects on the same page of the Policy Manager can be selected in a single operation.)

5. Click  **New Work Order**.

Note If you selected failing policy tests that are already part of an open work order (a work order with any state other than Closed), those tests will not be added to a new work order. You may need to complete remediation on these policy test failures, or close the existing work order(s) if remediation is complete.

6. In the Remediation Work Order dialog, enter a **Work Order Approval ID**, **Reference URL**, and **Description** for the work order.

Tips TE assigns each work order a unique **Launch URL** that can be distributed via e-mail or using other methods. If a user browses to this URL while currently logged in to TE, the Work Order Editor will open to this work order. If the user is not logged into TE, they must first log in before viewing the work order.

For more information on the fields and settings in the Remediation Work Order dialog, click  **Help** in any tab.

7. (Optional) If desired, view or edit the information in the tabs of the work order:
 - The **Actions** tab lists the remediation entries in the work order, and displays the current disposition for each one. You can use the settings in the Filter Tests section of this tab to change the entries that are currently displayed in the work order.
 - The **Status** tab shows the history of changes to the work order, and lists remediation runs associated with the work order that have already been initiated.
 - The **Settings** tab enables you to specify actions that Tripwire Enterprise should take after running automated remediation (for example, executing a post-remediation or promoting changes made by the remediation). You can also specify reports that TE sends after each remediation run.
8. Click **Assign** to assign a new owner to the work order. Typically, the next owner would be a user with permission to approve the remediations in the work order.
9. Close the Remediation Work Order dialog. Changes to work orders are applied as they are made, so there is no **OK** or **Apply** button.

The new work order can now be viewed or edited in any remediation work orders widget.

For more information on working with work orders, see the following topics:

- [Assigning a Work Order \(on the next page\)](#)
- [Approving or Denying Remediation Entries in a Work Order \(on page 258\)](#)
- [Running or Deferring Remediation in a Work Order \(on page 259\)](#)
- [Closing or Deleting a Work Order \(on page 260\)](#)

Assigning a Work Order

When you assign a remediation work order to a user or user group, they become the owner of that work order. You can use a work order's Owner value to filter how work orders are displayed in widgets or reports.

For more information on the automated remediation workflow, see [How Does Automated Remediation Work?](#) on page 151.

Tip This procedure explains how to assign a remediation work order to a user or user group in a remediation work order widget. However, you can also assign a remediation work order with the **Assign** button in the Remediation Work Order dialog.

To assign a work order to a user:

1. In the Manager bar, click **HOME**.
2. In the main pane, select the tab for a home page that contains a remediation work order widget. For information on adding a widget, see [Adding a Widget to a Home Page](#) on page 245.
3. In the widget, select each work order that you want to assign.
4. Click **Assign**.
5. In the Assign Work Orders dialog, select the user or user group to which you want to assign the work orders.
6. Click **Assign**.

For more information on working with work orders, see the following topics:


- [Creating a Remediation Work Order](#) (on page 255)
- [Approving or Denying Remediation Entries in a Work Order](#) (on the next page)
- [Running or Deferring Remediation in a Work Order](#) (on page 259)
- [Closing or Deleting a Work Order](#) (on page 260)

Approving or Denying Remediation Entries in a Work Order

Before TE can carry out remediation on an entry in a work order, the remediation must be approved. For more information on the automated remediation workflow, see [How Does Automated Remediation Work? on page 151](#).

To approve or deny remediation for entries in a work order:

1. In the Manager bar, click **HOME**.
2. In the main pane, select the tab for a home page that contains a remediation work order widget. To add a widget, see [Adding a Widget to a Home Page on page 245](#).
3. In the widget, click the link for a work order in the **ID** field.
4. In the Remediation Work Order dialog, select the **Actions** tab.

Tip Use the **View By** drop-down and the settings in the Filter Tests section of the Actions tab to change how remediation entries are displayed in the work order. Click  on the left side of the Actions tab to display the Filter Tests settings.

5. Select one or more groups or entries and click **Approve** to approve remediation or click **Deny** to deny remediation.

Note You can also click **Drop** to remove a remediation entry from a work order. Dropped entries cannot be added back - you must create a new work order to remediate them.

6. (Optional) For approvals, enter a Work Order Approval ID and click **OK**.

Note If an Approval ID has already been specified for this work order, no additional Approval ID is necessary.

7. (Optional) Enter a Comment and click **OK**.
8. (Optional) Click the **Assign** button to change the owner of the work order. For example, you might want to assign the work order to a user who will perform the remediations that were just approved.
9. Close the Remediation Work Order dialog. Changes to work orders are applied as they are made, so there is no **OK** or **Apply** button.

For more information on working with work orders, see the following topics:

- [Creating a Remediation Work Order \(on page 255\)](#)
- [Assigning a Work Order \(on the previous page\)](#)
- [Running or Deferring Remediation in a Work Order \(on the next page\)](#)
- [Closing or Deleting a Work Order \(on page 260\)](#)


Running or Deferring Remediation in a Work Order

Before you can run automated remediation on an entry in a work order, the remediation must be approved. For more information, see [Approving or Denying Remediation Entries in a Work Order on the previous page](#).

For more information on the automated remediation workflow, see [How Does Automated Remediation Work? on page 151](#).

To run or defer automated remediation on entries in a work order:

1. In the Manager bar, click **HOME**.
2. In the main pane, select the tab for a home page that contains a remediation work order widget. For information on adding a widget, see [Adding a Widget to a Home Page on page 245](#).
3. In the widget, click the link for a work order in the **ID** field.
4. In the Remediation Work Order dialog, select the **Actions** tab.

Tip Use the **View By** drop-down and the settings in the Filter Tests section of the Actions tab to change how remediation entries are displayed in the work order. Click  on the left side of the Actions tab to display the Filter Tests settings.

5. Select one or more groups or entries and click **Remediate** to run automated remediation or click **Defer** to defer remediation.
6. (Optional) Enter a Comment and click **Execute** (to run remediation) or **OK** (to defer remediation).

Note After you remediate or defer a remediation entry, you can no longer drop it from the work order. Dropped remediation entries cannot be added back - you must create a new work order to remediate them.

7. (Optional) Click the **Assign** button to change the owner of the work order. For example, once remediation is completed, you might want to assign the work order back to the user who created it for review.
8. Close the Remediation Work Order dialog. Changes to work orders are applied as they are made, so there is no **OK** or **Apply** button.

For more information on working with work orders, see the following topics:

- [Creating a Remediation Work Order \(on page 255\)](#)
- [Assigning a Work Order \(on page 257\)](#)
- [Approving or Denying Remediation Entries in a Work Order \(on the previous page\)](#)
- [Closing or Deleting a Work Order \(on the next page\)](#)

Closing or Deleting a Work Order

You can close or delete a work order from a remediation work orders widget in a home page.

- A work order can only be **closed** when its state is Completed (that is, when all of the remediation entries in the work order have been successfully remediated, denied, or deferred). Tripwire Enterprise stores closed work orders for archival purposes. Closed work orders can be viewed like any other work order, but cannot be re-opened or changed in any way.
- A work order can be **deleted** at any time. Tripwire Enterprise removes all record of deleted work orders.

To close or delete a work order:

1. In the Manager bar, click **HOME**.
2. In the main pane, select the tab for the home page that contains a remediation work orders widget.
3. In the widget, select each work order that you want to close or delete.
4. To close a work order, click **Close**.
To delete a work order, click **Delete**.
5. In the confirmation dialog, click **Yes** to confirm your action.

For more information on working with work orders, see the following topics:

- [Creating a Remediation Work Order \(on page 255\)](#)
- [Assigning a Work Order \(on page 257\)](#)
- [Approving or Denying Remediation Entries in a Work Order \(on page 258\)](#)
- [Running or Deferring Remediation in a Work Order \(on the previous page\)](#)

Chapter 5. Settings Procedures

User Settings

Changing User Preference Settings

User Preferences control the behavior and display settings of the Tripwire Enterprise interface for the current user only.

To change user preference settings:


1. In the Manager bar, click **SETTINGS**.
2. Under the User folder, click  **Preferences**.
3. Edit the preference settings (see [Table 70](#)).
4. Click **Apply**.

Table 70. User preferences

Field	Definition
Table page size	<p>This setting establishes the maximum number of rows displayed on one page in any table. For example, if you set the table page size to 15, and then open the Rule Manager, the table in the Rules tab displays a maximum of 15 rules. If the number of rows in a table exceeds the table page size, Tripwire Enterprise provides navigation controls for review of additional table rows.</p> <p>Any value from 1 to 500 may be entered. One hundred fifty (150) is the default setting.</p>
Refresh rate	<p>This setting determines the frequency with which Tripwire Enterprise refreshes data displayed in the Node Manager and Task Manager.</p> <ul style="list-style-type: none">• To specify the number of seconds between data-refresh updates, enter a whole number from 5 to 3600. Thirty (30) is the default setting.• To disable this feature, enter zero (0). <p>Warning: Since each data refresh resets the session timeout clock, refresh rates may interfere with automatic session timeouts. If your refresh rate setting is less than the system session timeout setting, and you leave the application open to a page that automatically refreshes data, Tripwire Enterprise will <i>not</i> terminate the session after the specified period of inactivity. To adjust the timeout setting, see Changing System Preferences on page 266.</p>
Max version display	<p>This setting establishes the maximum size of element version content (in Kb) displayed in the Content tab of the element version dialog. If element version content exceeds the specified size, the content will not be displayed. 50 Kb is the default setting.</p> <p>Note: To view the content of an element version, see Changing the Properties of an Element Version on page 327.</p>

Field	Definition
Max element name display width	<p>This setting establishes the preferred number of characters in element names displayed in the Tripwire Enterprise interface. If an element name exceeds the specified number of characters, Tripwire Enterprise limits the element name to the specified number of characters by concealing characters in the middle of the name. In the displayed element name, the concealed characters are replaced by an ellipsis (...).</p> <p>This feature is disabled by default (a value of 0).</p> <p>Note: If this feature is enabled, the full name of an element can still be viewed in the element properties dialog (see Changing the Properties of an Element on page 326).</p>
Max description display width	<p>This setting establishes the preferred number of characters in Description columns displayed in tables. If the text of a description exceeds the specified number of characters, Tripwire Enterprise limits the column's text to the specified number of characters by concealing characters at the end of the description. In the displayed text, the concealed characters are replaced by an ellipsis (...).</p> <p>Notes: With the default value (0), TE displays only the first line of a description.</p> <p>This setting does not affect the display of content in Description fields in property dialogs.</p>
Always login to Home Page	<p>If this check box is enabled, the Home Page Manager opens when your user account logs on to Tripwire Enterprise. Otherwise, TE opens the last Manager accessed by your account.</p>
Display exact table count	<p>Note: The First Page (<<) and Last Page (>>) buttons are standard navigation controls that may appear at the bottom of any table displaying a collection of TE objects.</p> <p>For tables of TE objects, this setting determines if TE retrieves the objects from the TE Console database in batches.</p> <ul style="list-style-type: none"> • If this setting is enabled, TE retrieves all applicable objects from the database. In this case, the First Page and Last Page buttons open the first or last page of all retrieved objects. • If this setting is disabled, TE retrieves objects from the database in batches. In this case, the First Page and Last Page buttons open the first or last page of each successive batch.
Display elements	<p>This setting determines where elements may be viewed in the Tripwire Enterprise interface.</p> <ul style="list-style-type: none"> • Only within node property editors. With this option, Tripwire Enterprise presents elements in the Elements tab of a node properties dialog, but <i>not</i> in the Node Manager main pane. • Only within the Node Manager. This option displays elements in the Node Manager main pane, but <i>not</i> node property dialogs. With this option, Tripwire Enterprise omits the Elements tab from all node property dialogs. • In both locations. Selected by default, this option displays elements in both node property dialogs and the Node Manager main pane. <p>To view elements in a node properties dialog, see Changing the Properties of a Node on page 321.</p> <p>To view elements in the Node Manager main pane, see Viewing Nodes, Node Groups, and Elements on page 313.</p>

Field	Definition
Tree	<p>This setting controls the behavior of the tree pane in TE Managers.</p> <ul style="list-style-type: none"> • Animation. If this option is selected, and a user selects a group in the tree pane, TE uses an animated feature to display (or conceal) the contents of the group. • Disable Multi-Expand. If this option is selected, users will <i>not</i> be able to expand multiple groups simultaneously in a tree pane. • Enable Tree Filter Field. If this option is selected, TE displays a filter field at the top of each Manager's tree pane. Filter strings are case-insensitive regular expressions (see How Do Regular Expressions Work? on page 107). You can also toggle this setting in the Node Manager, using the Tree Options section of the tree pane. <p>If you enter a string in the filter field, TE limits the tree pane to branches containing nodes or node groups that match that string. After applying the tree filter, you may still need to manually expand the branches to find the highlighted objects that you're looking for.</p>
Detailed node view	<p>Select this check box to enable Detailed Node View. With this setting, you can view the following objects in the Node Manager and node property dialogs:</p> <ul style="list-style-type: none"> • All node groups • All nodes within each node group • The rules that have been used to baseline each node • The existing elements identified by each rule <p>In Standard Node View, rules <i>cannot</i> be viewed in the Node Manager and node property dialogs.</p> <p>To enable Standard Node Manager View, clear this check box. You can also toggle this setting in the Node Manager, using the Tree Options section of the tree pane.</p> <p>Caution: The Display elements setting may prevent Tripwire Enterprise from displaying elements and rules in the Node Manager and/or node property dialogs.</p>
Open property editors to the last sheet visited	<p>Select this check box to open property dialogs to the last tab you visited. If this check box is not selected, the first tab in a property dialog will open by default.</p> <p>Note: This setting is enabled by default.</p>
Display remediation disclaimer in popup	<p>Select this check box to have Tripwire Enterprise present a disclaimer pop-up message the next time you select the Remediation tab in the properties dialog of any policy test (see Changing the Properties of a Policy Test on page 536). The next time you access a Remediation tab, TE will present the disclaimer and automatically disable this setting (so the disclaimer does not appear again).</p>
Display automated remediation disclaimer in popup	<p>Select this check box to have Tripwire Enterprise present a disclaimer pop-up message the next time you select the Remediator tab in the properties dialog of any policy test (see Changing the Properties of a Policy Test on page 536). The next time you access a Remediator tab, TE will present the disclaimer and automatically disable this setting (so the disclaimer does not appear again).</p>

Changing User Difference Settings

Difference settings control the use of **context lines** when you compare two element versions in the Difference Viewer (see *Responding to Changes on page 46*). If difference settings are activated, the Difference Viewer only displays the lines that differ between the two versions, along with a specified number of lines before and after each change (context lines).

To change user differences settings:


1. In the Manager bar, click **SETTINGS**.
2. Under the User folder, click  **Differences**.
3. Edit the difference settings (see [Table 71](#)).
4. Click **Apply**.

Table 71. User differences

Field	Definition
Use on files exceeding	This setting determines the minimum size of element versions for which context lines will be displayed (in kilobytes). If you enter zero (0), context lines will be used with all element versions. Zero (0) is the default setting.
Lines of context	This setting establishes the number of context lines that will appear above and below each change. Three (3) is the default setting.
Max lines per block	This setting determines the maximum number of lines displayed for each detected difference in the two versions being compared. If the number of lines in a detected difference exceeds this value, only a portion of the change will be displayed in the Difference Viewer. In such cases, the application states that lines 'X through Y' have been omitted. Twenty (20) is the default setting.

System Settings

Changing System Preferences

System preferences apply to all users of your Tripwire Enterprise implementation. For a list of system preference settings, see [Table 72](#).

To change system preferences settings:


1. In the Manager bar, click **SETTINGS**.
2. Under the System folder, click  **Preferences**.
3. Edit the system preferences.
4. Click **Apply**.

Table 72. System preferences

Field	Definition
Session timeout	<p>This setting establishes the amount of time of user inactivity before a user is automatically logged out. Any value from one to 180 minutes may be entered. The default timeout is 30 minutes.</p> <p>Warning: If the refresh rate setting is less than the session timeout setting, and a user leaves the application open to a page that automatically refreshes data, Tripwire Enterprise will <i>not</i> terminate the user's session after the specified period of inactivity (because each data refresh resets the session timeout clock). To adjust the refresh rate, see Changing User Preference Settings on page 262.</p>
Web services timeout	<p>This setting establishes the amount of time of Web-services inactivity before a Web-services client session is automatically logged out. Any value from one to 999 minutes may be entered. The default timeout is 120 minutes.</p>
Maximum search results	<p>If the Display exact table count setting is selected in the User Preferences (Table 70 on page 262), this value determines the maximum number of objects or records that may be retrieved by any search run in Tripwire Enterprise. Any value from 100 to 1,000,000 may be entered (default = 10,000).</p>
Integration hosts	<p>This setting identifies the network systems that may communicate with Tripwire Enterprise via the Tripwire Enterprise AAA Log Monitoring Tool. The host name or IP address of each system should be entered on a separate line. If a system is not listed as an integration host, it will be denied access to the Tripwire Enterprise Server.</p> <p>For more information, see What is the Tripwire Enterprise AAA Log Monitoring Tool? (on page 237)</p>
Promote comment is required	<p>To require that users enter an explanatory comment when promoting an element version in the Node Manager, select this check box. If this setting is selected, a user will be unable to promote element versions unless he or she enters a comment.</p> <p>Note: This setting is enabled by default. To promote an element version in the Node Manager, see Promoting a Specific Element Version on page 393.</p>

Field	Definition
Allow promotion approval identifier	<p>Select this check box to display the Approval ID field in the Promote Versions dialog. When a user promotes an element version, he or she may enter an approval ID in this field.</p> <p>Note: This setting is enabled by default. To promote an element version, see Promoting a Specific Element Version on page 393.</p>
Show only applied report criteria	<p>By default, Tripwire Enterprise displays all report criteria values in the output generated for a report. If enabled, this setting limits displayed criteria to those for which a value(s) has been specified.</p>
Enable dynamic policy run	<p>If selected, when a tag is applied to an existing node and that tag causes the node to be included in the scope of a TE policy, TE will evaluate all existing elements for tests under the newly-associated policy.</p>
Enable Smart Node Groups	<p>If selected, Tripwire Enterprise enables smart node groups and displays them in the Nodes tab of the Node Manager. For more information about smart node groups, see About Node Groups and Smart Node Groups on page 57.</p> <p>Note: If you disable smart node groups, Tripwire Enterprise creates an Orphan Nodes group. This group contains nodes that only had smart node groups as parents. If desired, you can move nodes out of the Orphan Nodes group and delete it.</p>

Changing Log Management Settings

In the Log Management settings, you can configure Tripwire Enterprise to:

- Forward all new TE log messages to a syslog server, such as Tripwire Log Center (TLC) and/or
- Query TLC log messages from TLC (see [What are Log Messages?](#) on page 166).

To change log management settings:


1. In the Manager bar, click **SETTINGS**.
2. Under the System folder, click  **Log Management**.
3. Edit the log management settings (see [Table 73 below](#)).
4. Click **Apply**.

Table 73. Log management settings

Field	Definition
Forward TE log messages to syslog	<p>To send all new TE log messages to a syslog server, select this check box and complete the following fields:</p> <ul style="list-style-type: none"> • Transport protocol. The protocol (TCP, TLS, or UDP) used to send TE log messages. If TLS is selected, the syslog server must have a certificate with a certificate authority that is trusted by TE, or the syslog server's certificate must be added to the TE Console's customer keystore. For more information on importing certificates, see this Tripwire Knowledgebase article. • Host. The IP address or hostname of the syslog server. • Port. The port on which your syslog server will listen for log messages. <p>To test these settings, click Test Connection.</p>
Allow TE to use information from Tripwire Log Center	<p>To have TE query your TLC Server for TLC log messages, select this check box and complete the following fields:</p> <p>Service address. The URL of the TLC Server.</p> <p><code>https://<t1c_server>:8091/t1c</code></p> <p>where <t1c_server> is the hostname of your TLC Server.</p> <p>User name. The name of a valid TLC user account with the 'Allow REST API Logon' and 'View Databases' permissions. (TLC Administrators have this permission by default.)</p> <p>Password and Confirm. Enter and confirm the password for the account.</p> <p>To test these settings, click Test Connection.</p>


Recalculating Database Index Statistics

A **database index** is a data structure that improves the speed of operations in a database table. Like the index of a book, a database index contains entries that reference specific information in the database. A **query optimizer** is a database component that uses database index statistics to determine the most efficient way to execute a query.

To optimize system efficiency and speed, you should recalculate the database index statistics for your Tripwire Enterprise Console database on a weekly basis and following any large Tripwire Enterprise operation. To recalculate statistics, Tripwire Enterprise refreshes the database indices with the latest information in the Tripwire Enterprise Console database.

Caution Recalculating database-index statistics may take several hours, depending on the size of the database. No user activity will be possible during this time, and you should ensure that no tasks are scheduled to run at this time.

To recalculate index statistics for your TE Console database:

1. In the Manager bar, click **SETTINGS**.
2. Under the System folder, click  **Database**.
3. Select **Recalculate database index statistics**.
4. Click **Apply**.
5. In the confirmation dialog, click **OK**.



Working with Severity Ranges


For an overview of severity levels and severity ranges, see:

- [What are Severity Levels? \(on page 112\)](#)
- [What are Severity Ranges? \(on page 114\)](#)

Note When TE detects a change on a node without a Change Audit license, all change versions created on that node are assigned a severity level of zero (0). Because this severity level falls outside of any severity range, TE does not display a severity indicator for changes detected on nodes without a Change Audit license.


To create a new severity range:


1. In the Manager bar, click **SETTINGS**.
2. Under the System folder, click  **Severity Ranges**.
3. Click  **New Range**.
4. Enter a **Name** and **Description** (optional). Then, click **Next**.
5. Enter a **Level** (severity level) and **Color**.

Tip For field descriptions, click  **Help**.

6. Click **Finish**.



To edit a severity range:

1. In the Manager bar, click **SETTINGS**.
2. Under the System folder, click  **Severity Ranges**.
3. In the **Name** column, select the severity range to be edited.
4. In the Severity Range dialog, edit the **General** tab and/or **Details** tab.

Tip For field descriptions, click  **Help**.

5. Click **OK**.




To delete a severity range:

1. In the Manager bar, click **SETTINGS**.
2. Under the System folder, click  **Severity Ranges**.
3. Select the check box for each severity range to be deleted.
4. Click  **Delete**.
5. Click **OK** to confirm.

Working with Global Variables

Global variables include text variables and password variables. For an introduction to global variables, see [What are Global and Local Variables?](#) on page 196.

To create a new global variable:

1. In the Manager bar, click **SETTINGS**.
2. Under the System folder, click  **Global Variables**.
3. Click  **New Text** or  **New Password**.
4. Enter a **Name** and **Description** (optional) for the variable. Then, click **Next**.


Note To enter a variable, users will select the value entered in the **Name** field.

5. Enter a **Value** or enter and confirm the **Password**.

Note To include a literal \$ character in a variable value, precede it with another \$ character. For example, pa\$\$phrase should be expressed as pa\$\$\$\$phrase.



6. Click **Finish**.

To edit a global variable:

1. In the Manager bar, click **SETTINGS**.
2. Under the System folder, click  **Global Variables**.
3. In the **Variable** column, select the variable to be edited.
4. In the variable dialog, edit the **General** and **Details** tabs.
5. Click **OK**.

Note If you change a variable used in a start point or stop point of a file system rule, and the rule is used to monitor an Axon Agent node, you should manually run the Configure Axon Agents task to update the rules on all Axon Agent systems. Rules on TE Agent systems are updated automatically.

To delete a global variable:

1. In the Manager bar, click **SETTINGS**.
2. Under the System folder, click  **Global Variables**.
3. Select the check box for each variable to be deleted.
4. Click  **Delete**.
5. Click **OK** to confirm.



Caution If you delete a password variable that is in use, Tripwire Enterprise cannot log in to the associated monitored systems.


Working with E-mail Servers

The E-mail Servers setting defines the e-mail servers used to send Tripwire Enterprise e-mail notifications and report output. For more information, see:

- [How Does an E-mail Action Work? \(on page 120\)](#)
- [What are Reports and Report Types? \(on page 172\)](#)

To create an e-mail server:


1. In the Manager bar, click **SETTINGS**.
2. Under the System folder, click  **E-mail Servers**.
3. Click  **New E-mail Server**.
4. Enter a **Name** and **Description** (optional) for the server. Then, click **Next**.
5. Enter SMTP information and authentication credentials (optional).


Tip For field descriptions, click  **Help**.

6. Click **Finish**.

Next To assign the new e-mail server to an e-mail action, see [Creating an E-mail Action on page 492](#). To assign the new e-mail server to a report task, see [Creating a Report Task on page 519](#).



To edit an e-mail server:

1. In the Manager bar, click **SETTINGS**.
2. Under the System folder, click  **E-mail Servers**.
3. From the **Name** column, select the server to be edited.
4. In the server dialog, edit the **General** tab and **Details** tab.

Tip For field descriptions, click  **Help**.

5. Click **OK**.



To delete an e-mail server:

1. In the Manager bar, click **SETTINGS**.
2. Under the System folder, click  **E-mail Servers**.
3. Select the check box for each server to be deleted.
4. Click  **Delete**.
5. Click **OK** to confirm.

Working with Approval Templates

An **approval template** specifies an Approval ID and/or a comment. When you promote element versions in the Node Manager with the 'promote selected versions' method, you can select an approval template. If you do, TE saves the template's Approval ID and comment in each new baseline version created by the promotion **and** in each existing version of the element created since the last baseline version or version with an approval ID.


To create an approval template:

1. In the Manager bar, click **SETTINGS**.
2. Under the System folder, click  **Approval Templates**.
3. Click  **New Approval Template**.
4. Enter a **Name** and **Description** (optional) for the template. Then, click **Next**.
5. Enter a **Comment** and/or **Approval ID**.

Tips Approval templates support date and time macros. For example, to save the date and time of promotion in the properties of new baseline versions created with a template, you could enter the following values:

Comment: \${Date: DD, MMMM YYYY hh:mm}


Approval ID: 274B Approved on \${Date}


For field descriptions and macro formats, click  **Help**.

6. Click **Finish**.

Next To use the new approval template in a promotion with the 'promote specific versions' method, see [Promoting a Specific Element Version \(on page 393\)](#) and [Promoting All Current Versions for a Node or Node Group \(on page 395\)](#).


To edit an approval template:

1. In the Manager bar, click **SETTINGS**.
2. Under the System folder, click  **Approval Templates**.
3. From the **Name** column, select the template to be edited.
4. In the server dialog, edit the **General** tab and **Details** tab.

Tip For field descriptions, click  **Help**.

5. Click **OK**.

To delete an approval template:

1. In the Manager bar, click **SETTINGS**.
2. Under the System folder, click  **Approval Templates**.
3. Select the check box for each template to be deleted.
4. Click **✗ Delete**.
5. Click **OK** to confirm.

Configuring Tripwire Enterprise Console Properties

With this procedure, you can modify most of the system configuration properties for Tripwire Enterprise Console. For a complete list of property descriptions, see *Tripwire Enterprise Console Configuration Properties* in the *Tripwire Enterprise Reference Guide*.


Note If the `tw.disableConfigEditing` property in the Console properties file is set to true, any edits made to that properties file using the TE Console user interface will be ignored. You can still edit the file directly using a text editor.

Prior to configuring TE Console, complete the following steps:

- Disable all tasks (see [Disabling Tasks on page 524](#)).
- Ensure that no Agents are being started or re-started.
- Instruct all users to log out of the system.

Caution This procedure restarts Tripwire Enterprise Console. Therefore, the application will be unavailable for users during this time.

To configure Tripwire Enterprise Console properties:


1. In the Manager bar, click **SETTINGS**.
2. Under the System folder, click  **Configure TE Console**.
3. In the main pane, click **Configure**.
4. In the Configure Tripwire Enterprise Console dialog, edit the property values and click **OK**.
 - To assign the default value to a property, click the associated **Default** button.
 - To view the full names of all properties, select **Show full names of properties**.
 - To view the descriptions of all properties, select **Show detailed descriptions**.

Zeroize Critical Security Parameters

In this dialog, you can also zeroize critical security parameters. Zeroization writes zeroes to critical memory and shuts down the TE Console to prevent an attacker from capturing data that could be used to decrypt sensitive information.

Caution Zeroization will render your TE Console inoperable and unrecoverable!

To zeroize critical memory and shut down Tripwire Enterprise Console:


1. In the Manager bar, click **SETTINGS**.
2. Under the System folder, click  **Configure TE Console**.
3. In the main pane, click **Zeroize**.

Importing Settings

This procedure imports an XML settings file to your Tripwire Enterprise implementation.

- To create an XML settings file, see [Exporting Settings \(on the next page\)](#).
- For an overview of import guidelines, see [XML-File Import of Settings \(on page 225\)](#).

To import settings from an XML settings file:

1. In the Manager bar, click **SETTINGS**.
2. Under the System folder, click  **Import Settings**.
3. In the main pane, click **Import Settings**.
4. In the Import Settings dialog, click **Browse**.
5. To locate and select the XML file, complete the standard steps for your operating system.

Caution XML setting files may contain sensitive network information. Therefore, these files should be saved in a secure location or deleted following import.

6. In the Import Settings dialog, click **OK**.

Exporting Settings

This procedure exports and saves all Settings Manager data (with the exception of home pages) in an XML file. Exported data includes:

- User preferences and differences
- System preferences
- Log management settings
- Severity ranges
- Global variables
- Approval templates
- E-mail servers
- User accounts, user roles, and user groups
- Custom properties
- Custom nodes
- Monitoring preferences

As needed, the contents of the XML file may be re-imported at a later date (see [Importing Settings on the previous page](#)).

Note To export home pages, see [Exporting Home Pages on page 292](#).

To export Tripwire Enterprise settings to an XML file:


1. In the Manager bar, click **SETTINGS**.
2. Under the System folder, click  **Export Settings**.
3. In the main pane, click **Export Settings**.
4. In the Export Settings dialog, click **Save**.
5. To save the XML file, complete the standard steps for your operating system.


Creating Diagnostic Files for Tripwire Support


The Support Data feature creates a zip file containing diagnostic files for your Tripwire Enterprise Server and/or Agent systems. With these files, Tripwire Support can troubleshoot potential problems with your Tripwire Enterprise implementation.

Note You should only complete this procedure if Tripwire Support has requested that you do so. To submit a zip file to Tripwire Support, consult your Support representative.

To send diagnostic files to Tripwire support:

1. In the Manager bar, click **SETTINGS**.
2. Under the System folder, click  **Support Data**.
3. Click **Collect**.
4. In the Collect Data dialog:
 - a. If you received a trouble ticket for this issue from Tripwire Support, enter the **Trouble ticket number**.
 - b. (Optional) To submit diagnostic files for the TE Agent installed on the TE Console system, select **Include files from TE Server's Agent**.

Tip For field descriptions, click  **Help**.

5. (Optional) To add diagnostic files for one or more Agent systems:
 - a. Click  **Add**.
 - b. In the Chooser dialog, select an Agent node or node group.
 - c. Click **Add**.
 - d. For each Agent node or node group to be added, repeat steps **b** and **c** above. Then, click **OK**.
6. Click **Finish**.

Upgrading Agents

To upgrade a Tripwire Enterprise Agent or Axon Agent, complete the following steps:

Step 1. Upload Agent Updaters (below)

Step 2. Upgrade Agent Software (on page 281)

During an upgrade, Tripwire Enterprise will install either the 32-bit or 64-bit Agent software, matched to the operating system of the Agent system. If you want to upgrade 32-bit Agent software on a 64-bit OS, you must manually uninstall and re-install the Agent software.

Note You cannot use this procedure to upgrade an Agent on a platform that is not supported by the current version of Tripwire Enterprise. For a complete list of supported platforms for the current TE release, see <https://www.tripwire.com/products/tripwire-enterprise/tripwire-enterprise-platform-and-device-support-register>.

When upgrading a TE Agent older than version 8.5.0, you must first upgrade to TE Agent version 8.5.0 before upgrading to any later version.


Step 1. Upload Agent Updaters

To upgrade an Agent, you must first upload Agent updaters to the system where Tripwire Enterprise Console is installed, using the TE Console Settings Manager.

Note You can also upload Agent updaters for Tripwire Enterprise Agents using the command line. For more information, see [Uploading TE Agent Updaters from the Command Line on the next page](#).

Axon Agent updaters **must** be uploaded from TE Console using the steps below.

To upload Agent updaters:

1. Download the Agent updaters you want to install from the Tripwire Customer Center (<https://tripwireinc.force.com/customers>) and copy them to a location that is accessible from the TE Console system.
2. In the Manager bar, click **SETTINGS**.
3. Under the System folder, click  **Agent Updaters**.
4. In the main pane, click **Add Updater**.
5. In the Select Agent Updater Files dialog, click **Choose Files** and browse to the updaters you downloaded. Select one or more updaters and click **Open**.
6. Click **OK** when you are done selecting updaters.

After you have uploaded the Agent updaters to the TE Console system, proceed to [Step 2. Upgrade Agent Software on page 281](#).

Uploading TE Agent Updaters from the Command Line

Follow the steps below to upload TE Agent updaters without using the TE Console UI.

To upload Axon Agent updaters, you **must** use the process described in [Step 1. Upload Agent Updaters on the previous page](#).

To upload TE Agent updaters from the command line on a Linux TE Console:

1. Download the updaters you want to install from the Tripwire Customer Center (<https://tripwireinc.force.com/customers>).
2. Log in to the TE Console system as a privileged user.
3. If it doesn't exist already, create the following directory on the TE Console system:

```
mkdir /usr/local/tripwire/te/server/lib/updaters
chown tripwire:tripwire /usr/local/tripwire/te/server/lib/updaters
```

4. Copy the Agent updaters to the TE Console updaters directory:

```
cp -r updaters/* /usr/local/tripwire/te/server/lib/updaters
```

Do not unzip the files. They will be unzipped automatically during the update process.

5. Change directories to the Agent updaters directory:

```
cd /usr/local/tripwire/te/server/lib/updaters
```

6. To configure the user permissions for all contents of the directory, enter:

```
chmod 0444 *
chown tripwire:tripwire *
```

To upload TE Agent updaters from the command line on a Windows TE Server:

1. Download the updaters you want to install from the Tripwire Customer Center (<https://tripwireinc.force.com/customers>).
2. If it doesn't exist already, create the following directory on the TE Console system:

```
C:\Program Files\Tripwire\TE\Server\lib\updaters
```

3. Copy the Agent updaters to the new updaters directory on the TE Console system.

Do not unzip the files. They will be unzipped automatically during the update process.

4. To configure the user permissions for the updaters directory:

- a. In Windows Explorer, right-click the directory and select **Properties**.

- b. In the Properties dialog, clear (disable) the **read-only** attribute and verify that the Administrators user group has the **Full Control** permission.

Step 2. Upgrade Agent Software

Notes By default, the Event Generator software on TE Agent systems is updated at the same time as the Agent software. For more information, see [Upgrading Event Generator Software on TE Agents on the next page](#).


When upgrading a TE Agent on a Solaris system, the procedures in this section do not allow you to change the user account with which the Agent is running. For more information, see *Installing Tripwire Enterprise Agent on Solaris* in the *Tripwire Enterprise Installation & Maintenance Guide*.

To upgrade a TE Agent on a Solaris system, the upgrade must run as the root user, and root must be added as an authorized user to the `at.allow` file. If you edit this file, you may need to create a policy waiver for some Tripwire-published policies.

To upgrade Agent software on one or more Agent systems:

1. In the TE Console Manager bar, click **NODES**.
2. In the tree pane, select the node group with the Agent nodes to be upgraded.
3. **To upgrade specific Agents**, select the check box of each Agent node (or node group) in the main pane.

To upgrade all Agents in the selected node group, do not select any check boxes.

4. Click **Modify** >  **Upgrade**.
5. In the Upgrade Agents dialog, click **Next**.
6. (Optional) To upload a properties file for Linux or Windows TE Agents:
 - a. Click **Select**.
 - b. Click **Browse**.
 - c. In the Choose File dialog, select the file and click **Open**.
 - d. Click **Upload**.
7. Click **Finish**.

Tip If an error occurs, Tripwire Enterprise will generate an Error message in the Log Manager and the node will be tagged with a Health:Push Upgrade Error tag in Asset View. To begin troubleshooting, review these messages.

8. **For TE Agent upgrades on AIX systems only**, perform the following steps to enable real-time and Event Generator functionality:
 - a. Log into the AIX box with root privileges.
 - b. Run `<te root>/sup/rtm/teauditconfig`.
 - c. Start GES (`startsrc -s teges`).

Upgrading Event Generator Software on TE Agents

When upgrading a TE Agent running a platform that supports Event Generators, by default the upgrade also:

1. Installs an Event Generator on the Agent system,
2. Enables audit-event collection and real-time monitoring (RTM) for the Agent, and
3. Specifies port 1169 (TCP) as the port on the Agent system to be used by Tripwire Enterprise for all communications with the Event Generator.

On Linux and Windows TE Agents, you can override this default behavior by uploading a properties file (in [Step 2. Upgrade Agent Software on the previous page](#)) containing one or both of the following lines:

```
install_rtm=false  
rtm_port=<port_number>
```

where:

`install_rtm=false` prevents the installation of Event Generators, and
`<port_number>` specifies a port other than 1169.

On Solaris 10 systems, the `install_rtm` option cannot be used to prevent the installation of an Event Generator. An Event Generator is always installed.

On AIX systems, Tripwire does **not** recommend setting the `install_rtm` flag to `false` in the properties file, even if you do not intend to use real-time monitoring or Event Generator functionality with the TE Agent. If you do not want to use real-time monitoring, shut down the Event Generator (`stopsrc -s teeg`) after upgrading the TE Agent.



Administration Settings

Importing Post-Remediation Service Commands

For an introduction to post-remediation service commands, see [What are Post-Remediation Service Commands?](#) on page 164.

This procedure imports post-remediation service commands from an XML file to your Tripwire Enterprise implementation. You can download an XML file from the Tripwire Customer Center Web site (<https://tripwireinc.force.com/customers>) or create an XML file by exporting post-remediation service commands from another Tripwire Enterprise installation (see [Exporting Post-Remediation Service Commands](#) on the next page).


To import post-remediation service commands:


1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Post-Remediation Service Commands**.
3. Click  **Import**.
4. In the Select File dialog, click **Browse**.
5. To locate and select the XML file, complete the standard steps for your system.
6. In the Select File dialog, click **OK**.

Changing Post-Remediation Service Commands

For an introduction to post-remediation service commands, see [What are Post-Remediation Service Commands?](#) on page 164.

To change post-remediation service commands:

1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Post-Remediation Service Commands**.
3. In the **Name** column, select the post-remediation to be edited.
4. As appropriate, edit the **General** and **Post-Remediation Service Command** tabs in the properties dialog.

Notes	For further assistance, click  Help . If you have implemented whitelists on Agent systems, the post-remediation service command must exactly match a command in a whitelist file. For more information, see Restricting Commands on Agent Nodes with Whitelists on page 424.
--------------	---



5. Click **OK**.

Exporting Post-Remediation Service Commands

For an introduction to post-remediation service commands, see [What are Post-Remediation Service Commands? on page 164](#).

This procedure exports post-remediation service commands to an XML file. As needed, the contents of the XML file may be re-imported at a later date (see [Administration Settings on the previous page](#)).

To export post-remediation service commands to an XML file:


1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Post-Remediation Service Commands**.
3. (Optional) To export **specific** post-remediation service commands, select the appropriate check boxes.
4. Click  **Export**.
5. In the Export Post-Remediation Service Commands dialog, select one of the following options and click **OK**:
 - **All Post-Remediation Service Commands**. This option exports all post-remediation service commands in your TE implementation.
 - **Selected Post-Remediation Service Commands only**. This option exports the selected post-remediation service commands only.
6. To export the XML file to a local directory, complete the standard steps for your system.

Tip If your Web browser is an older version of Internet Explorer, you may need to manually add a **.xml** extension to the end of the file name.

Deleting Post-Remediation Service Commands

For an introduction to post-remediation service commands, see [What are Post-Remediation Service Commands? on page 164](#).

To delete post-remediation service commands:



1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Post-Remediation Service Commands**.
3. Select the check box for each post-remediation service command to be deleted.
4. Click **✗ Delete**.
5. Click **OK** to confirm.


Creating a User Account

For an overview of user access management in Tripwire Enterprise, see:

- [What are User Permissions and User Roles? \(on page 204\)](#)
- [What are User Accounts and User Groups? \(on page 206\)](#)

To create a user account:

1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Users**.
3. Click  **New User**.
4. Enter a **Username**, **E-mail address** (optional), and **Description** (optional). Then, click **Next**.

Tips For field descriptions, click  **Help**.

If your login method is LDAP/Active Directory, Tripwire Enterprise usernames must match the LDAP/Active Directory usernames. To define the login method, see [Configuring the Tripwire Enterprise Login Method on page 294](#).

5. Enter and confirm a **Password** for the user. Then, click **Next**.

Tip For security purposes, Tripwire requires that you create a password for every user account. This password is used if the Password login method is used for TE (see [Configuring the Tripwire Enterprise Login Method on page 294](#)).

6. Select a user role and click **Next**.

Caution Exercise caution when assigning the Power User and Administrator roles. These roles permit users to change TE objects, modify configuration files, and restore changed files.


7. (Optional) Assign the user account to one or more user groups, and click **Next**. (To assign the account to a user group, select the group's check box.)
8. (Optional) Assign one or more home pages to the user account, and click **Finish**. (To assign a home page, double-click the home page in the Available Home Pages panel.)


Changing User Account Properties

With this procedure, you can change the following properties of a user account:

- The user's name, e-mail address, and password
- The user role assigned to the user
- The list of user groups to which the user belongs
- The list of home pages assigned to the user

To change the properties of a user account:

1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Users**.
3. From the **Username** column, select the user account to be edited.
4. As appropriate, edit the tabs in the user account properties dialog.

Tip For field descriptions, click  **Help**.

5. Click **OK**.


Changing the Password for a User Account

Note For security purposes, Tripwire requires that you create a password for every user account. This password is used if the Password login method is used for TE (see [Configuring the Tripwire Enterprise Login Method on page 294](#)).

To change the password for the current user account:

1. In any Manager, click the user name in the status bar at the bottom of the screen.
2. In the user account properties dialog, select the **Password** tab.
3. Enter the current password for this account, then enter and confirm a new password.
4. Click **OK**.


To change the password for a user account from the Settings Manager:


1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Users**.
3. From the **Username** column, select the user account to be edited.
4. In the **Password** tab of the user account properties dialog, enter and confirm the new password.
5. Click **OK**.

Assigning a User Role to a User Account

For an introduction to user roles, see [What are User Permissions and User Roles?](#) on page 204.

To change the user role associated with a user account:

1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Users**.
3. From the **Username** column, select the user account to be edited.
4. In the **Role** tab of the user account properties dialog, select the desired user role.


Tip For field descriptions, click  **Help**.

5. Click **OK**.


Associating User Accounts with User Groups

With these procedures, you can associate (or disassociate) user accounts and user groups. For more information, see [What are User Accounts and User Groups?](#) on page 206.

To change the list of user groups to which a user account is assigned:

1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Users**.
3. From the **Username** column, select the user account.
4. In the **Groups** tab of the user account properties dialog, select the desired user groups.
 - To add the user account to a user group, select the check box for the group.
 - To remove the user account from a user group, clear the check box for the group.
5. Click **OK**.

To assign or remove user accounts to/from a user group:



1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **User Groups**.
3. From the **Group Name** column, select the group to be edited.
4. In the **Users** tab of the user group properties dialog, select the desired user accounts.
 - To add a user to the user group, select the user's check box.
 - To remove a user from the group, clear the user's check box.
5. Click **OK**.

Unlocking a User Account

Tripwire Enterprise can be configured to lock out user accounts after a specified number of failed login attempts (see *Configuring the Tripwire Enterprise Login Method* on page 294). Use this procedure to unlock a locked-out user account.

Note To immediately unlock **all** locked user accounts, restart the TE Console service:
`<te_root>\Server\bin\twservices restart`



To unlock a user account:

1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Users**.
3. From the **Username** column, select the user account to be unlocked.
4. Click  **Unlock**.

Deleting User Accounts

Note The default administrator user account cannot be deleted.

To delete user accounts:



1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Users**.
3. Select the check box for each account to be deleted.
4. Click  **Delete**.
5. Click **OK** to confirm.

Working with User Groups

For an overview of user access management in Tripwire Enterprise, see:

- [What are User Permissions and User Roles? \(on page 204\)](#)
- [What are User Accounts and User Groups? \(on page 206\)](#)


To create a user group:

1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **User Groups**.
3. Click  **New User Group**.
4. Enter a **Name** and **Description** (optional) for the new user group. Then, click **Next**.
5. (Optional) Select the check box for each user account to be included in the user group.


Note The default administrator user account cannot be added to a user group.

6. Click **Finish**.

To edit the properties of a user group:

1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **User Groups**.
3. From the **Group Name** column, select the group to be edited.
4. As appropriate, edit the **General** and **Users** tabs in the user group properties dialog.
5. Click **OK**.

To delete user groups:

1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **User Groups**.
3. Select the check box for each user group to be deleted.
4. Click **✗ Delete**.
5. Click **OK** to confirm.



Note When you delete a user group, the user accounts and user roles associated with the group remain intact. To delete user accounts or roles, see:


- [Deleting User Accounts \(on the previous page\)](#)
- [Working with User Roles \(on page 293\)](#)

Creating a Home Page

For an introduction to Tripwire Enterprise home pages, see [What are Home Pages and Widgets?](#) on page 189.

To create a home page:

1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Home Pages**.
3. Click  **New Home Page**.
4. In the New Home Page Wizard:
 - a. Enter a **Name** and **Description** (optional).
 - b. (Optional) To assign a Tracking Identifier to the home page, select **Enable update tracking** (see [What are Tracking Identifiers?](#) on page 223).
 - c. Click **Next**.



Tip For more information, click  **Help** in any wizard page.

5. Assign user accounts to the home page. To assign a user account, double-click the account in the Available Users menu.
6. Click **Finish**.

Duplicating a Home Page

With this procedure, you can duplicate one or more home pages.

To create copies of existing home pages:

1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Home Pages**.
3. (Optional) To duplicate specific home pages, select the check box of each home page.
4. Click  **Duplicate**.
5. Click **OK** in the confirmation dialog.

Tripwire Enterprise uses the following convention to name a duplicate home page:

Copy of <original_home_page>


where <original_home_page> is the name of the home page that was duplicated.


Note A copy of a home page includes all properties of the original home page, with the exception of the users assigned to the original.

Changing the Properties of a Home Page

For an introduction to Tripwire Enterprise home pages, see [What are Home Pages and Widgets?](#) on page 189.

To edit the properties of a home page:

1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Home Pages**.
3. In the **Name** column, select the home page to be edited.
4. As appropriate, edit the **General** and **Users** tabs in the home page properties dialog.



Tip For further assistance, click  **Help**.

5. Click **OK**.

Deleting Home Pages

For an introduction to Tripwire Enterprise home pages, see [What are Home Pages and Widgets?](#) on page 189.



To delete home pages:

1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Home Pages**.
3. Select the check box for each home page to be deleted.
4. Click  **Delete**.
5. Click **OK** to confirm.

Exporting Home Pages

This procedure exports selected home pages to an XML file. As needed, the contents of the XML file may be re-imported at a later date (see [Importing Home Pages](#) below).

To export home pages to an XML file:

1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Home Pages**.
3. (Optional) To export **specific** home pages, select the appropriate check boxes.
4. Click  **Export**.
5. In the Export Home Pages dialog, select one of the following options and click **OK**:
 - **All home pages**. This option exports all home pages in your TE implementation.
 - **Selected home pages only**. This option exports the selected home pages only.
6. To export the XML file to a local directory, complete the standard steps for your system.



Tip If your Web browser is an older version of Internet Explorer, you may need to manually add a **.xml** extension to the end of the file name.

Importing Home Pages

This procedure imports home pages from an XML file to your Tripwire Enterprise implementation. (To create an XML file containing home pages, see [Exporting Home Pages](#) above.)

Caution Prior to this procedure, you should first review the guidelines employed by Tripwire Enterprise when importing the contents of an XML file (see [How Do I Import and Export Tripwire Enterprise Objects?](#) on page 217).

To import the home pages in an XML file:

1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Home Pages**.
3. Click  **Import**.
4. In the Import Home Pages dialog, click **Browse**.
5. To locate and select the XML file, complete the standard steps for your system.
6. In the Import Home Pages dialog, click **OK**.



Working with User Roles

For an overview of user access management in Tripwire Enterprise, see:


- [What are User Permissions and User Roles? \(on page 204\)](#)
- [What are User Accounts and User Groups? \(on page 206\)](#)


Note The default user roles cannot be changed or deleted.

To create a user role:

1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Roles**.
3. Click  **New Role**.
4. Enter a **Role Name** and **Description** (optional). Then, click **Next**.
5. Select the permissions to be assigned to the user role.
6. Click **Finish**.


To change a user role:

1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Roles**.
3. From the **Role Name** column, select the user role to be edited.
4. As appropriate, edit the **General** and **Permissions** tabs in the user role properties dialog. (You cannot edit the Permissions tab for a default user role.)

Tip For field descriptions, click  **Help**.

5. Click **OK**.

To delete user roles:

1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Roles**.
3. Select the check box for each user role to be deleted.


Note If a user role is assigned to a user account, the role cannot be deleted. To delete the role, you must first assign another user role to the user account. For instructions, see [Assigning a User Role to a User Account on page 287](#).

4. Click  **Delete**.
5. Click **OK** to confirm.

Configuring the Tripwire Enterprise Login Method

For an overview of Tripwire Enterprise login methods, see [What are Login Methods? on page 207](#).

To set the system login method:

1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Login Method**.
3. Select the desired **System login method**.
 - **Password**. To log in with this method, users simply enter a username and password. If the login credentials are authenticated by Tripwire Enterprise, the user is granted access to the system.
 - **LDAP/Active Directory**. With this method, users also provide a username and password. However, the login credentials are authenticated by an LDAP or Active Directory server.

Tips If you select **Connect using SSL** with the LDAP/Active Directory method, you must add the root certificate of your directory server to the TE Console keystore. For more information on this process, see:

https://tripwireinc.force.com/customers/articles/Install_and_Upgrade/Tripwire-Enterprise-How-to-Set-Up-SSL-Communications-in-Tripwire-Enterprise-8-4-1

Changing the login method from LDAP/Active Directory to Password will allow all users to login with their Tripwire Enterprise passwords. Therefore, you should ensure that all user account passwords are strong.

4. If you selected the **LDAP/Active Directory** login method, enter the appropriate Server Configuration settings. For guidance, see [Table 74 on the next page](#).
5. If desired, configure the account lockout settings for the TE Console. For guidance, see [Table 75 on page 296](#).
6. Click **Apply**.

Table 74. LDAP/Active Directory server settings

Field	Definition
LDAP server	Enter the URL for the LDAP or Active Directory (AD) server to be used for authentication. ldap:// is the required prefix for both LDAP and Active Directory servers.
User template	<p>In accordance with your organization's configuration requirements, enter an LDAP login string.</p> <p>Example 1</p> <p>Typically, LDAP login strings are entered as Distinguished Names (DN), which are also known as X.500 formatted strings. The following text is an example of a Distinguished Name:</p> <p style="padding-left: 40px;">CN=Jeff Graves,CN=Users,DC=example,DC=com</p> <p>In this case, you would make the following entry in the User template field:</p> <p style="padding-left: 40px;">CN=\$user,CN=Users,DC=example,DC=com</p> <p>With this entry, Tripwire Enterprise replaces every instance of the string "\$user" with the login name being authenticated. Then, the application forwards this information to the LDAP/AD server for authentication.</p> <p>Example 2</p> <p>For authentication, Active Directory servers often use a "User logon name," which is typically the user's e-mail address in the following format:</p> <p style="padding-left: 40px;"><domain>\<user></p> <p>For example:</p> <p style="padding-left: 40px;">mydomain\jeff.graves</p> <p>Note: For successful authentication, the username for the user's Tripwire Enterprise account must be identical to the username for the LDAP/AD account. In the examples above, Tripwire Enterprise must contain user accounts for "Jeff Graves" and "jeff.graves," respectively.</p>
Connect using SSL	<p>Select this check box to use SSL to encrypt communications between the TE Server and the LDAP/AD server.</p> <p>If you select this option, you must add a certificate from your directory server to the TE Console keystore. For more information on this process, see:</p> <p>https://tripwireinc.force.com/customers/articles/Install_and_Upgrade/Tripwire-Enterprise-How-to-Set-Up-SSL-Communications-in-Tripwire-Enterprise-8-4-1?popup=true.</p>



Table 75. TE user lockout settings

Field	Definition
Enable Account Lockout Policy	If selected, TE will use the settings in this section to lock out user accounts after a specified number of failed login attempts.
Account lockout duration	<p>The number of minutes that a TE user account is locked out after exceeding the Account lockout threshold. To unlock a user account before this time, see Unlocking a User Account on page 288.</p> <p>Note: To immediately unlock all locked user accounts, restart the TE Console service: <code><te_root>\Server\bin\twservices restart</code></p>
Account lockout threshold	The number of failed login attempts allowed before TE locks out a user account. Each failed login attempt is logged, and can be viewed in the Log Manager.
Reset account lockout counter after	<p>The number of minutes after the last failed login attempt before TE resets the failed login counter to 0.</p> <p>Note: To immediately unlock all locked user accounts, restart the TE Console service: <code><te_root>\Server\bin\twservices restart</code></p>
Notify user on account lockout	<p>If selected, TE will send an e-mail notification to a user when their account is locked out. TE sends this notification to the e-mail address in the user account's properties.</p> <p>Use the CC field to select other TE users who should also receive the notification e-mail. If no e-mail address is associated with a TE user account, the user will not receive notification from TE. You should also ensure that the E-mail Server specified here is valid. For more information, see Working with E-mail Servers on page 272.</p> <p>Edit the Subject and Message Body to customize the notification e-mail. Message Body supports the following variables:</p> <ul style="list-style-type: none"> • <code>\$initiatedDateTime</code> is the date/time when TE initiated the lockout. • <code>\$expirationDateTime</code> is the date/time when the lockout will expire. • <code>\$locked-user</code> is the TE user name of the locked user.

Adding a License File

For an introduction to license files, see [About Tripwire Enterprise Licenses on page 202](#).



To add a license file:

1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Licenses**.
3. Click  **Add License**.
4. In the Add License dialog, click **Browse**.
5. Locate and select the license file. Then, click **Open**.
6. Click **OK**.

Deleting Licenses

If the licenses in a license file expire, only an Administrator can delete the file. However, an active license file can only be deleted (by an Administrator) if all nodes that use the file's Change Audit licenses have first been deleted from the Node Manager.

To delete a license file:


1. In the Manager bar, click **SETTINGS**.
2. Under the Administration folder, click  **Licenses**.
3. Select the check box for each license file to be deleted.
4. Click  **Delete**.
5. Click **OK** to confirm.


Custom Properties

Working with Custom Properties

For an introduction to custom properties, see [What are Custom Properties?](#) on page 197.

To create a custom property:

1. In the Manager bar, click **SETTINGS**.
2. Under the Custom Properties folder, select the type of property to be created.
3. Click  **New Property**.
4. In the New Custom Property Wizard, select a property type and click **OK**.
5. Complete the remaining wizard pages.

Tip For more information, click  **Help** in any wizard page.


To modify a custom property:

1. In the Manager bar, click **SETTINGS**.
2. Under the Custom Properties folder, select the type of property.
3. From the **Name** column, select the property to be edited.
4. As appropriate, edit the **General** and **Details** tabs in the custom properties dialog.

Tip For field descriptions, click  **Help**.

5. Click **OK**.

To delete a custom property:



1. In the Manager bar, click **SETTINGS**.
2. Under the Custom Properties folder, select the type of property.
3. Select the check box for each property to be deleted.
4. Click  **Delete**.
5. Click **OK** to confirm.

Monitoring Preferences


Working with Custom Node Types

A **custom node** is a user-created type of network device node.



To create a type of custom node:

1. In the Manager bar, click **SETTINGS**.
2. Under the Monitoring Preferences folder, click  **Custom Node Types**.
3. Click  **New Custom Node Type**.
4. In the New Custom Node Type Wizard, enter a **Name** and **Description** (optional).
5. Click **Finish**.

To change the name or description of a custom-node type:

1. In the Manager bar, click **SETTINGS**.
2. Under the Monitoring Preferences folder, click  **Custom Node Types**.
3. In the Name column of the main pane, select the link for the custom-node type.
4. In the properties dialog, edit the **Name** and/or **Description**.
5. Click **OK**.

To delete a custom-node type:

1. In the Manager bar, click **SETTINGS**.
2. Under the Monitoring Preferences folder, click  **Custom Node Types**.
3. In the main pane, select the check box of each node type to be deleted.
4. Click  **Delete**.



Tip If the Node Manager contains any nodes of the type to be deleted, you must first delete those nodes before you can delete the type (see [Deleting Nodes and Node Groups on page 377](#)).

5. Click **OK** to confirm.

Creating a Criteria Set for a File System Rule

When applied to a Windows or UNIX file system rule, a criteria set identifies the attributes to be checked on objects monitored by the rule. For more information, see [How Does a File System Rule Work?](#) on page 83.

To create a criteria set for a file system rule:

1. In the Manager bar, click **SETTINGS**.
2. Under the Monitoring Preferences folder, click  **Criteria Sets**.
3. Click  **New Criteria Set**.
4. In the Create Criteria Set dialog, select one of the following options and click **OK**:
 - **UNIX File Criteria Set**
 - **Windows File Criteria Set**

Tip For more information, click  **Help**.

5. In the New Criteria Set Wizard, enter a **Name** and **Description** (optional) for the criteria set. Then, click **Next**.
6. For a **UNIX** or **Windows file system rule**:
 - a. Select the file attributes for the criteria set, enter any **Severity Overrides** (optional), and click **Next**.
 - For UNIX attribute definitions, see [Table 76 on the next page](#).
 - For Windows attribute definitions, see [Table 77 on page 302](#).
 - b. Select the appropriate directory attributes and enter any **Severity Overrides** (optional). For attribute definitions, see [Table 76](#) and [Table 77](#).
7. Click **Finish**.

Table 76. File system attributes for UNIX

Attribute	Applies to ...	Description
ACL	... files & directories	The access control list for a file or directory
Access	... files & directories	The last date and time when a file or directory was accessed
Change	... files & directories	The last date and time when file or directory metadata was modified (or created)
Group	... files & directories	The UNIX user group that owns a file or directory
Growing	... files only	<p>The size and SHA-1 hash of a file</p> <p>In a version check, this attribute results in the creation of a change version if:</p> <ul style="list-style-type: none"> • The size of the file is smaller than the baseline, and/or • The hash of the original file content has changed (Note: If the only change in file content is an addition at the end of the file, and the file is equal to or larger than the baseline version, TE will not create a new change version.)
MD5	... files only	The MD5 hash for a file
Modify	... files & directories	The last time file or directory content was changed by a user
Package Data	... files only	<p>A hash that associates a file with a software-installation package</p> <p>Tip: To display package data in the property dialogs of element versions created by a file system rule, the following conditions must be met:</p> <ul style="list-style-type: none"> • The Package Data attribute must be included in the rule's criteria set. • The Enable installation package association setting must be enabled (see Setting File System Preferences on page 310).
Permissions	... files & directories	Permission and file mode bits
SHA-1	... files only	The SHA-1 hash for a file
SHA-256	... files only	The SHA-256 hash for a file
SHA-512	... files only	The SHA-512 hash for a file
Size	... files only	The size of a file
User	... files & directories	The owner of a file or directory

Table 77. File system attributes for Windows

Attribute	Applies to ...	Description
Access	... files & directories	The last time a file or directory was accessed by a user
Archive	... files & directories	Archive flag
Compressed	... files & directories	A flag that indicates whether a file or directory is compressed
Create	... files & directories	The date and time when a file or directory was created
DACL	... files & directories	A list that specifies the level of file or directory access granted to Windows users or user groups
Group	... files & directories	The Windows user group that owns a file or directory
Growing	... files only	<p>The size and SHA-1 hash of a file</p> <p>In a version check, this attribute results in the creation of a change version if:</p> <ul style="list-style-type: none"> • The size of the file is smaller than the baseline and/or • The hash of the original file content has changed (Note: If the only change in file content is an addition at the end of the file, and the file is equal to or larger than the baseline version, Tripwire Enterprise will not create a new change version.)
Hidden	... files & directories	Hidden flag
MD5	... files only	The MD5 hash of a file
Offline	... files & directories	Offline flag
Owner	... files & directories	The owner of the file

Attribute	Applies to ...	Description
Package Data	... files only	<p>A hash or version string that associates a file with a software-installation package</p> <ul style="list-style-type: none"> • If the file has Microsoft version information, Tripwire Enterprise stores the version string. • If the file lacks a version string, the application computes the MSI hash value. However, the hash is not computed for files larger than 10 MB. <p>Note: When reaping package information with this attribute, a Windows file system rule attempts to locate data to associate a file with a software-installation package.</p> <p>Tip: To display package data in the property dialogs of element versions created by a file system rule, the following conditions must be met:</p> <ul style="list-style-type: none"> • The Package Data attribute must be included in the rule's criteria set. • The Enable installation package association setting must be enabled (see Setting File System Preferences on page 310).
Read-Only	... files & directories	Read-only flag
SACL	... files & directories	A list that controls the generation of audit log entries for attempts to access a securable object.
SHA-1	... files only	The SHA-1 hash of a file
SHA-256	... files only	The SHA-256 hash of a file
SHA-512	... files only	The SHA-512 hash of a file
Size	... files only	The size of a file
Stream Count	... files & directories	<p>The number of data streams on a file or directory. Data streams may include:</p> <p>BACKUP_EA_DATA</p> <p>BACKUP_ALTERNATE_DATA</p> <p>BACKUP_LINK</p> <p>BACKUP_PROPERTY_DATA</p> <p>BACKUP_OBJECT_ID</p> <p>BACKUP_REPARSE_DATA</p> <p>BACKUP_SPARSE_BLOCK</p>
Stream MD5	... files & directories	The MD5 hash for the file or directory alternate data stream(s)
Stream SHA-1	... files & directories	The SHA-1 hash for the file or directory alternate data stream(s)
Stream SHA-256	... files & directories	The SHA-256 hash for the file or directory alternate data stream(s)

Attribute	Applies to ...	Description
Stream SHA-512	... files & directories	The SHA-512 hash for the file or directory alternate data stream(s)
System	... files & directories	System flag
Temp	... files & directories	Temp flag
Write	... files & directories	The date and time when file or directory content was last changed

Creating a Criteria Set for a Windows Registry Rule

In a Windows registry rule, a criteria set identifies the attributes of registry keys and entry values to be monitored by the rule. For more information, see [How Does a Windows Registry Rule Work? on page 85](#).

To create a criteria set for a Windows registry rule:



1. In the Manager bar, click **SETTINGS**.
2. Under the Monitoring Preferences folder, click  **Criteria Sets**.
3. Click  **New Criteria Set**.
4. In the Create Criteria Set dialog, select **Windows Registry Criteria Set**.
5. In the New Criteria Set Wizard, enter a **Name** and **Description** (optional) for the criteria set. Then, click **Next**.
6. Select the appropriate attributes for monitored **entry values** (see [Table 78 below](#)), enter any **Severity Overrides** (optional), and click **Next**.
7. Select the appropriate attributes for monitored **registry keys** (see [Table 78](#)), enter any **Severity Overrides** (optional), and click **Next**.
8. Click **Finish**.

Table 78. Registry attributes for Windows systems

Attribute	Applies to registry ...	Description
DACL	... keys	A list that specifies the level of access granted to Windows users or user groups
Data Type	... entry values	Indicates the type of data in an entry value; for data-type definitions, see Table 79 on page 306
Group	... keys	The Windows user or user group that owns a registry key

Attribute	Applies to registry ...	Description
MD5	... entry values	The MD5 hash of an entry value
Owner	... keys	The owner of a registry key
Package Data	... keys and entry values	<p>A string that associates a registry key or entry value with a software-installation package</p> <p>Tip: To display package data in the property dialogs of element versions created by a Windows registry rule, the following conditions must be met:</p> <ul style="list-style-type: none"> • The Package Data attribute must be included in the rule's criteria set. • The Enable installation package association setting must be enabled (see Setting File System Preferences on page 310).
SACL	... keys	A list that controls the generation of audit log entries for attempts to access a registry key
SHA-1	... entry values	The SHA-1 hash of an entry value
SHA-256	... entry values	The SHA-256 hash of an entry value
SHA-512	... entry values	The SHA-512 hash of an entry value
Size	... entry values	The size of data in an entry value
Write	... keys	The date and time when a key was last changed

Table 79. Registry data types

Data Type	Description
REG_BINARY	Binary data in any form
REG_DWORD	A 32-bit number
REG_DWORD_LITTLE_ENDIAN	A 32-bit number in little-endian format
REG_DWORD_BIG_ENDIAN	A 32-bit number in big-endian format
REG_EXPAND_SZ	Null-terminated string (Unicode or ANSI) that contains unexpanded references to environment variables (for example, "%PATH%")
REG_FULL_RESOURCE_DESCRIPTOR	A list of hardware resources that a physical device is using, detected and written into the \HardwareDescription tree by the monitored system
REG_LINK	Reserved for system use
REG_MULTI_SZ	An array of null-terminated strings, terminated by two null characters
REG_NONE	No defined value type
REG_QWORD	A 64-bit number
REG_QWORD_LITTLE_ENDIAN	A 64-bit number in little-endian format
REG_RESOURCE_LIST	A device driver's list of hardware resources, used by the driver or one of the physical devices it controls, in the \ResourceMap tree
REG_SZ	Null-terminated string (Unicode or ANSI)

Creating a Criteria Set for a Windows RSoP Rule

For an introduction to Windows RSoP rules, see [How Does a Windows RSoP Rule Work?](#) on page 88.

To create a criteria set for a Windows RSoP rule:



1. In the Manager bar, click **SETTINGS**.
2. Under the Monitoring Preferences folder, click  **Criteria Sets**.
3. Click  **New Criteria Set**.
4. In the Create Criteria Set dialog, select **Windows RSoP Criteria Set**.
5. In the New Criteria Set Wizard, enter a **Name** and **Description** (optional) for the criteria set. Then, click **Next**.
6. Select the appropriate **attributes** (see [Table 80 on the next page](#)) and enter any **Severity Overrides** (optional).
7. Click **Finish**.

Table 80. Attributes for Windows RSoP rules

Attribute	Description
MD5	This attribute identifies the MD5 hash of the Resultant Set of Policy for the monitored computer and user.
SHA-1	This attribute identifies the SHA-1 hash of the Resultant Set of Policy for the monitored computer and user.

Creating a Criteria Set for a Database Rule

For an introduction to database rules, see:

- [How Does a Database Metadata Rule Work? on page 89](#)
- [How Does a Database Query Rule Work? on page 92](#)

To create a criteria set for a database rule:



1. In the Manager bar, click **SETTINGS**.
2. Under the Monitoring Preferences folder, click  **Criteria Sets**.
3. Click  **New Criteria Set**.
4. In the Create Criteria Set dialog, select **Database Server Criteria Set**.
5. In the New Criteria Set Wizard, enter a **Name** and **Description** (optional) for the criteria set. Then, click **Next**.
6. Select the appropriate **attributes** (see [Table 81 below](#)) and enter any **Severity Overrides** (optional).
7. Click **Finish**.

Table 81. Attributes for database rules


Attribute	Description
MD5	In a database metadata rule, this attribute identifies the MD5 hash of the data definition language (DDL) statements used to create a database object. In a database query rule, this attribute identifies the MD5 hash of query results.
SHA-1, SHA-256, and SHA-512	In a database metadata rule, these attributes identify the hash of the data definition language (DDL) statements used to create a database object. In a database query rule, these attributes identify the hash of query results.


Changing Criteria Set Properties

In a file system rule, Windows registry rule, Windows RSoP rule, or database rule, a criteria set identifies the monitored object attributes to be checked by the rule. For more information, see:

- [How Does a File System Rule Work? \(on page 83\)](#)
- [How Does a Windows Registry Rule Work? \(on page 85\)](#)
- [How Does a Windows RSoP Rule Work? \(on page 88\)](#)
- [How Does a Database Metadata Rule Work? \(on page 89\)](#)
- [How Does a Database Query Rule Work? on page 92](#)

To change the name, description, or attributes of a criteria set:

1. In the Manager bar, click **SETTINGS**.
2. Under the Monitoring Preferences folder, click  **Criteria Sets**.
3. From the **Name** column, select the criteria set to be edited.



<p>Note If a checkmark overlays the upper right corner of a criteria set's icon () , the criteria set has one or more severity overrides. For more information, see What are Severity Levels? (on page 112).</p>
--

4. In the criteria set properties dialog, select and edit the desired tabs.
 - For definitions of attributes associated with **UNIX files and directories**, see [Table 76 on page 301](#).
 - For definitions of attributes associated with **Windows files and directories**, see [Table 77 on page 302](#).
 - For definitions of attributes associated with **Windows registry keys and entries**, see [Table 78 on page 304](#).
 - For definitions of attributes associated with a **Windows RSoP**, see [Table 80 on the previous page](#).
 - For definitions of attributes associated with **databases**, see [Table 81 on the previous page](#).
5. Click **OK**.

Duplicating Criteria Sets

With this procedure, you can duplicate one or more criteria sets.

To create copies of existing criteria sets:

1. In the Manager bar, click **SETTINGS**.
2. Under the Monitoring folder, click  **Criteria Sets**.
3. (Optional) To duplicate specific criteria sets, select the check box of each set.
4. Click  **Duplicate**.
5. Click **OK** in the confirmation dialog.

Tripwire Enterprise uses the following convention to name a duplicate criteria set:

```
<original_set>(<#>)
```

where:



<original_set> is the name of the criteria set that was duplicated.

<#> is a number that increments each time the original criteria set is duplicated (beginning with 1) - for example, set (1), set (2), etc.

Deleting Criteria Sets

Note You cannot delete a criteria set that is currently associated with a rule.


To delete a criteria set:

1. In the Manager bar, click **SETTINGS**.
2. Under the Monitoring Preferences folder, click  **Criteria Sets**.
3. Select the check box for each criteria set to be deleted.
4. Click  **Delete**.
5. Click **OK** to confirm.

Setting File System Preferences

With this procedure, you may configure settings used to monitor file systems.

To set preferences for your monitored file systems:

1. In the Manager bar, click **SETTINGS**.
2. Under the Monitoring Preferences folder, click  **File Systems**.
3. Select the check boxes for the desired settings (see [Table 82 below](#)).

Notes If selected, the **Enable installation package association** setting may significantly slow the first baseline or version check operation run on a file system.

To enable the collection of audit events from a file server, select the **Collect audit event information** check box in the properties dialog of the server's node (see [Changing the Properties of a Node on page 321](#)).

4. Click **Apply**.


Table 82. File system preference settings

Setting	Definition
Enable installation package association	<p>(Disabled by default) If enabled, this setting collects information about installed software packages on a monitored system. With this data, Tripwire Enterprise can associate elements and element versions with installed packages. Package associations may then be viewed in the Packages tab of both the element properties dialog and element version dialog.</p> <ul style="list-style-type: none"> • To view package information for an element, see Changing the Properties of an Element on page 326. • To view package information for an element version, see Changing the Properties of an Element Version on page 327. <p>Tip: To display package data in the property dialogs of element versions created by a file system rule, the following conditions must be met:</p> <ul style="list-style-type: none"> • The Package Data attribute must be included in the rule's criteria set (see Creating a Criteria Set for a File System Rule on page 300). • The Enable installation package association setting must be enabled.
Maximum size of archived content	<p>If the Archive Content setting is enabled for a start point, this setting determines if Tripwire Enterprise saves the content of text files identified by the start point.</p> <ul style="list-style-type: none"> • If a text file is smaller than the specified size (default = 1000 KB), the application saves the file's content in all new element versions. • If the size of a text file exceeds this setting, the file's content will not be saved. <p>Note: To enable or disable the Archive Content setting for a start point, see Changing or Deleting Start Points on page 466.</p>
Reset Windows access time	<p>(Disabled by default) This setting resets the access time when a Windows file system rule is run with a version check. If this setting is enabled, running a version check with Windows file system rules will <i>not</i> cause a modification of the access time for Windows files and directories.</p>

Setting LDAP Directory Preferences

With this procedure, you can define the binary attributes for your monitored LDAP directories. For more information, see [What are Binary Attributes and Security Attributes?](#) on page 97.

To set preferences for your monitored LDAP directories:


1. In the Manager bar, click **SETTINGS**.
2. Under the Monitoring Preferences folder, click  **LDAP Directories**.
3. As appropriate, edit the list of **Binary Attributes**.
 - To add an attribute, enter the attribute's name on a separate line.
 - To remove an attribute, delete the attribute's name.
4. Click **Apply**.

Setting Active Directory Preferences

With this procedure, you can:

- Enable the collection of audit events from security-event logs on monitored Active Directory servers. If enabled, Tripwire Enterprise will save relevant audit event information in any new element version that represents an Active Directory entry.
- Define the binary and security attributes for your monitored Active Directories. For more information, see [What are Binary Attributes and Security Attributes?](#) on page 97.

To set preferences for your monitored Active Directories:

1. In the Manager bar, click **SETTINGS**.
2. Under the Monitoring Preferences folder, click  **Active Directories**.
3. As appropriate, edit the list of **Binary Attributes** and **Security Attributes**.
 - To add an attribute, enter the attribute's name on a separate line.
 - To remove an attribute, delete the attribute's name.
4. To enable the collection of audit events, select **Collect audit event information**.

Note To collect audit events on an Active Directory node, a Change Audit license must be installed on that node. You can configure the licenses applied to a node on its **Licenses** tab. For more information on the functionality available with each type of license, see [About Tripwire Enterprise Licenses](#) on page 202.

5. If TE is collecting audit events, select **Ignore 'Open' audit events** to filter out Open and Object Operation events. Select this option to help reduce noise from events that don't correspond to actual changes.
6. Click **Apply**.

Chapter 6. Node Procedures

Viewing and Changing Objects in the Node Manager

Viewing Nodes, Node Groups, and Elements

To view nodes, node groups, and elements in the Node Manager:

1. In the Manager bar, click **NODES**.
2. In the tree pane, expand the Tree Options pane.
3. Select or clear the displayed Tree Options (see [Table 83 on the next page](#)).
4. In the tree pane, select a node group, node, or rule (available with Detailed Node View only).
5. In the Node Manager table, review the list of associated objects (see [Figure 25 on the next page](#)).
 - If you selected a node group in the tree pane, see [Table 84 \(on page 315\)](#) for column definitions.
 - If the main pane contains a list of elements, see [Table 85 \(on page 316\)](#).
 - If the main pane contains a list of rules, see [Table 86 \(on page 316\)](#).

Tips To sort the contents of the Node Manager table by the values in a column, click the column header. To reverse the order, click the column header a second time.

If the contents of the Node Manager table span multiple pages, use the navigation controls at the bottom of the table to scroll through the pages.

To adjust the number of items displayed on a single page in the main pane, adjust the Node Manager **table page size** setting (see [Changing User Preference Settings on page 262](#)).

Table 83. Tree Options

Option	Description
Changed Node View	Displays a flat list of all nodes with current change versions in the tree pane.
Detailed Node View	<p>Overrides the default Detailed Node View setting from the Settings Manager (see Changing User Preference Settings on page 262). Select or clear this check box to specify the hierarchy of Tripwire Enterprise objects displayed in the Node Manager table by default.</p> <p>Detailed Node View includes all rules and rule groups that have been used to baseline elements for each node. In descending order, this view displays the following TE objects:</p> <p style="padding-left: 40px;">node groups > nodes > rule groups > rules > elements</p> <p>Standard Node View displays the following objects (in descending order):</p> <p style="padding-left: 40px;">node groups > nodes > elements</p> <p>Note: The Detailed Node View settings also determine which TE objects are available in the Elements tab of a node properties dialog (see Changing the Properties of a Node on page 321).</p>
Enable Tree Filter Field	<p>Overrides the default Enable Tree Filter Field setting from the Settings Manager (see Changing User Preference Settings on page 262). If selected, this option displays a filter field at the top of the tree pane. Filter strings are case-insensitive regular expressions (see How Do Regular Expressions Work? on page 107).</p> <p>If you enter a string in the filter field, TE limits the tree pane to branches containing nodes or node groups that match that string. After applying the tree filter, you may still need to manually expand the branches to find the highlighted nodes that you're looking for.</p>

Figure 25. The Node Manager

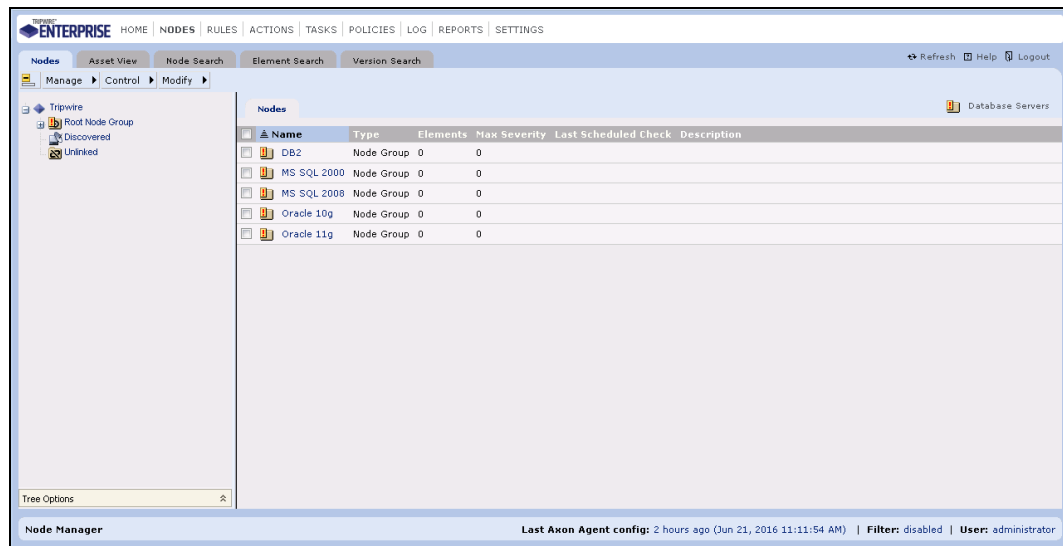


Table 84. Node Manager columns with a node group selected

Column	Description
Name	The Name column lists the names of nodes and node groups in the selected group. To view the properties of a node or node group, click a Name link. For more information, see: <ul style="list-style-type: none">• Changing the Properties of a Node on page 321• Changing the Properties of a Node Group on page 325
Type	This column identifies the type of Tripwire Enterprise object; either a type of node or "Node Group."
Elements	This column presents the number of elements that currently exist for each node or node group.
Max Severity	This column identifies the highest severity level among all element versions associated with each node or node group. For more information, see What are Severity Levels? on page 112 .
Last Scheduled Check	This column indicates the last time a version check was run on a node or node group. If none of the node or node group's elements have been checked, the entry is Never .
Description	This column provides an optional description of each node or node group. To add or edit descriptions, see: <ul style="list-style-type: none">• Changing the Properties of a Node on page 321• Changing the Properties of a Node Group on page 325

Table 85. Node Manager columns with elements displayed



Column	Description
Element	The Element column lists the names of elements associated with the selected node. To view the properties of an element, click an Element link.
Version Type	<p>If the current version of an element is a change version, this column identifies the type of change.</p> <ul style="list-style-type: none"> • Addition indicates that the element’s monitored object is new. • Modification indicates that the monitored object has changed. • Removal indicates that the monitored object has been deleted. <p>To compare a change version with the element’s current baseline in the Difference Viewer, select a Change Type link. For more information, see Comparing a Current Change Version with the Current Baseline on page 388.</p>
Current Version	<p>This column identifies the date and time when Tripwire Enterprise created the current version of each element.</p> <ul style="list-style-type: none"> •  The baseline icon indicates that the current version is the current baseline. •  The change version icon indicates that the current version is a change version. A severity indicator (!, +, or -) overlays the icon of each change version. For more information about severity indicators, see What are Severity Ranges? on page 114. <p>To open a current version of an element in the version properties dialog, select the Current Version link.</p>
Severity	<p>This column indicates the severity level associated with each current version. If the current version is a baseline, a severity level is not listed.</p> <p>For more information, see What are Severity Levels? on page 112.</p>
Rule	<p>This column identifies the rule used to baseline each element. To open a rule in the rule properties dialog, click a Rule link.</p> <p>To modify rule properties, see Changing the Properties of a Rule on page 437.</p>


Table 86. Node Manager columns with rules displayed (Detailed Node View only)

Column	Description
Rule	<p>The Rule column displays the name of each rule used to baseline elements associated with the selected node.</p> <p>To view the properties of a rule, click a Rule link. For more information, see Changing the Properties of a Rule on page 437.</p>
Elements	This column identifies the total number of elements baselined by each rule.
Max Severity	This column identifies the highest severity level assigned to any of the node’s element versions that were created by the rule. For more information, see What are Severity Levels? on page 112 .
Last Rule Run Date	This column indicates the last time a rule (or rule group) was used to baseline or version check a node.
Status	This column indicates if the last baseline operation or version check run with the rule completed successfully.

Monitoring the Health of Nodes and Resolving Errors

In Tripwire Enterprise, nodes are “healthy” if they can communicate with the TE Console without errors. TE monitors the health of a node each time that it attempts to communicate, for example during a version check, promotion, or baseline operation. Healthy nodes have a `Health:Healthy Assets` tag in the Asset View tab.


[Table 87 on the next page](#) lists the types of node errors tracked by Tripwire Enterprise. When TE detects an error for a node, it makes the following changes:


- The node's `Health` tag is changed to reflect the type of error.
- In the Asset View tab, the node has red shading in the Asset List pane, and details about the error are displayed in the Selection Information pane.
- In the Nodes tab, the node has an  error icon.
- The error is logged in the Log Manager.

You can resolve some errors from the Nodes tab, for example by restarting all of the nodes in the Out of Sync Errors smart node group. To resolve other errors, you may need to review details of the errors that are displayed in the Asset View tab.

To view and clear node errors in the Asset View tab:

1. (Optional) Use the `Health` filter to list assets with specific errors. You can also choose assets directly from the Nodes tab (see [Viewing Specific Nodes or Groups in Asset View on page 351](#)).
2. Click on an asset in the Asset List to see error information about the asset in the Selection Information pane. For each type of error, the ten most recent error messages that are less than two weeks old are displayed.
3. After resolving the cause of a node error, you may want to clear the asset's error messages. When you clear errors, the asset is restored to a healthy state in the Node Manager, but the error messages are retained in the Log Manager.

To clear all of the error messages for an asset, click  next to Asset Errors.

To clear all messages in a single category, click  next to the label for that category.

Tip To clear errors from multiple nodes at the same time, select the nodes in the Asset List, then click **Health Check** in the right-hand Selection Information pane and select **Dismiss Errors** from the dropdown menu.

Table 87. Types of errors for nodes

Error Type	Potential Causes and Solutions
<p>Connection Error</p>	<p>The Agent software is not running, or the system being monitored is not running.</p> <p>The username, password, port number, or other connection information specified for the node is incorrect.</p> <p>To resolve this type of error, first click the Test Connection button in the error dialog. If that doesn't fix the problem, make sure that all systems are running correctly, and that the connection information for the node is current.</p> <p>Tip: To test the connection for multiple nodes at the same time, select the nodes in the Asset List, then click Health Check in the right-hand Selection Information pane and select Test Connection from the dropdown menu.</p>
<p>Incompatible Agent Error</p>	<p>The TE Console software was upgraded, and is no longer compatible with the data on the node.</p> <p>To resolve this type of error, click the Restart Agent button in the error dialog and leave the Refresh agent data option selected in the confirmation dialog.</p>
<p>Event Generator Error</p>	<p>Communication between this Agent and the its Event Generator was disrupted, or there was another error with the Event Generator. This may affect the collection of audit events or real-time monitoring for this system.</p> <p>To resolve this error, first verify that the Event Generator service is running on the Agent system. For more information, see <i>Managing the Event Generator Service</i> in the <i>Tripwire Enterprise Installation & Maintenance Guide</i>.</p> <p>On Axon Agents, most Event Generator Errors will disappear automatically when the connection between the Agent and the Event Generator is restored. In some cases, you may need to manually dismiss the error.</p> <p>On TE Agents, restart the Agent after verifying that the Event Generator service is running.</p>
<p>Out of Sync Error</p>	<p>The connection between the Console and Agent was lost during a baseline or version check.</p> <p>To resolve this type of error, click the Restart Agent button in the error dialog and leave the Refresh agent data option selected in the confirmation dialog.</p>
<p>Push Upgrade Error</p>	<p>An error occurred when trying to upgrade this Agent node. For more information about the upgrade process, see Upgrading Agents on page 413.</p> <p>To resolve this type of error, select the asset in Asset View and review the details of the error in the Selection Information pane.</p> <p>Note: Messages about successful Agent upgrades and informational messages about upgrades are logged in the Log Manager.</p>
<p>Rule Run Error</p>	<p>A rule timed out during a baseline operation or version check. This can also happen if a rule attempts to query a database table that does not exist.</p> <p>To resolve this type of error, select the asset in Asset View and review the details of the error in the Selection Information pane.</p>
<p>Task Timeout Error</p>	<p>A task exceeded its maximum timeout setting.</p> <p>To resolve this type of error, increase the task timeout setting or split the task into several smaller tasks.</p>

Error Type	Potential Causes and Solutions
Uncategorized Error	<p>An error occurred that does not fit into any of the other error categories.</p> <p>To resolve this type of error, select the asset in Asset View and review the details of the error in the Selection Information pane.</p> <p>Note: After addressing the cause of an Uncategorized error, you must manually clear it as described in this section. TE does not automatically clear Uncategorized errors when they are resolved.</p>

Viewing Changed Nodes

To view a list of nodes with current changes:

1. In the Manager bar, click **NODES**.
2. In the tree pane, expand the Tree Options pane and select **Changed Node View**.

In the tree pane, Tripwire Enterprise presents a flat list of nodes with current change versions. For further details, see [Viewing Nodes, Node Groups, and Elements on page 313](#).

Filtering Elements in the Node Manager


Filter criteria determine which elements appear in the Node Manager table. To filter the contents of the Node Manager table, the filter function must be enabled. If filtering is disabled, the Node Manager displays all elements currently in the system.

To enable or disable filtering:

1. In the Manager bar, click **NODES**.
2. In the lower right-hand corner of the Node Manager, click the **Filter** link.
3. In the Node Filter dialog, select the **General** tab.
4. Select or clear the **Filter enabled** check box.
5. Click **OK**.

To change filter criteria for the Node Manager:

1. In the Manager bar, click **NODES**.
2. In the lower right-hand corner of the Node Manager, click the **Filter** link.
3. In the **Elements** tab of the Node Filter dialog, enter the appropriate filter settings.


Tip For more information, click  **Help** in any tab.

4. Click **OK**. The Node Filter dialog closes, and the Node Manager refreshes with the filtered elements.

Changing the Properties of a Node

To change the properties of a node:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the node group containing the node.
3. In the main pane, select the node in the **Name** column.
4. As needed, modify the tabs in the node properties dialog. For tab descriptions, see [Table 88 below](#).

Tip For more information, click  **Help** in any tab.

5. Click **OK**.

Table 88. Tabs in node properties

Tab	Available with	Description
Agent Logs	File server nodes	Downloads a text file containing log entries generated by the Agent software installed on the monitored system (see Downloading Agent Log Files on page 423).
Advanced	Custom nodes Network device nodes	Specifies settings for communication between the monitored system and your Tripwire Enterprise Server.
Connection	Custom nodes Database nodes Directory nodes Network device nodes VI management nodes	Sets the data-transfer and/or connection methods for communications between the monitored system and your TE Server.
Console Login	VI hypervisor nodes (only applies to VMware ESXi 5.0 & later)	Specifies authentication credentials and configuration properties for SSH connections between your TE Server and the monitored system. Note: If the Use Default Authentication check box is selected, TE uses the credentials and properties defined by the VI management node containing the hypervisor node (see the ESXi Console Login tab).
Delegated Agent	Database nodes Directory nodes VI management nodes	Specifies the delegated Agent for the node (see Assigning a Delegated Agent to a Node on page 411). Note: Only nodes with Tripwire Enterprise Agent installed can be a delegated Agent for a database, directory server, or VI management node. Nodes with Axon Agent installed cannot be used as a delegated Agent.

Tab	Available with	Description
Elements	All nodes with the exception of VI management nodes	Contains a list of elements created for the node. For more information, see Changing the Properties of an Element on page 326 . Note: This tab includes some of the same buttons that appear in the Node Manager. For guidance in using these buttons, refer to the corresponding Node Manager procedure in this chapter.
ESXi Console Login	VI management nodes	Specifies default authentication credentials and configuration properties for SSH connections between your TE Server and hypervisors administered by the node's VI management software. Note: TE establishes an SSH connection when running COHR commands on a hypervisor.
ESXi Web-Based Login	VI management nodes	Specifies default authentication credentials for HTTPS connections between your TE Server and hypervisors administered by the node's VI management software. Note: TE establishes an HTTPS connection to access configuration files and parameters identified by VI hypervisor rules.
Events	File server nodes Database nodes (except for PostgreSQL database nodes)	Enables audit event collection. For file server nodes, also enables real-time detection. For more information, see: <ul style="list-style-type: none"> • What is Audit Event Collection? (on page 63) • How Does Real-Time Monitoring Work? (on page 70) Notes: This tab does not contain any options for Axon Agent nodes that do not have an Event Generator installed. To collect information from an operating-system audit log, logging must be enabled on the monitored system.
General	All nodes	Identifies the monitored system.
Licensing	All nodes with the exception of: <ul style="list-style-type: none"> • VI management nodes • Virtual machine nodes • Virtual machine template nodes • Virtual switch nodes • Distributed virtual switch nodes 	Contains settings that apply or remove licenses to/from the node. For more information, see About Tripwire Enterprise Licenses on page 202 .

Tab	Available with	Description
Log Center Events	All nodes with the exception of: <ul style="list-style-type: none"> • VI management nodes • Virtual machine nodes • Virtual machine template nodes • Virtual switch nodes • Distributed virtual switch nodes 	Displays TLC log messages for events involving the node. Note: This tab does not appear in node property dialogs if the Allow TE to use information from Tripwire Log Center setting is disabled (see Changing Log Management Settings on page 268).
Login	Custom nodes Database nodes Directory nodes Network device nodes VI management nodes	Defines authentication credentials for Tripwire Enterprise to log in to the monitored system.
Login Script	Custom nodes	Defines a script to be run each time Tripwire Enterprise logs in to the monitored system.
Logout Script	Custom nodes	Defines a script to be run each time Tripwire Enterprise logs out of the monitored system.
Parent Groups	All nodes	Displays the full path of each node group to which the node is linked. <ul style="list-style-type: none"> • This tab includes some of the same buttons that appear in the Node Manager. For guidance in using these buttons, refer to the corresponding procedure in this chapter. • To view or edit the properties of a node group, select the group's link. (For more information, see Changing the Properties of a Node Group on page 325.)
Properties	All nodes with the exception of VI management nodes	Defines the values of custom properties assigned to the node (see Defining Values for Custom Properties on page 328).
Security	All nodes	Contains any access controls that have been created for the node. For more information, see Working with Node Access Controls on page 333 .

Tab	Available with	Description
Synchronization	VI management nodes	<p>Defines a schedule for Tripwire Enterprise to synchronize a VI management node with the current content of the node's VI management software (either a regular interval or specific times).</p> <p>Tip: To synchronize a VI management node at any time, click the Synchronize button in the node's properties dialog.</p>
Test Results	All nodes with the exception of VI management nodes	<p>Displays the hierarchy of all policies and policy tests that have a scope that includes the node. A test result indicator overlays each displayed object. To view or edit the properties of a displayed object, select the object's link.</p> <p>This tab also includes a collection of buttons that run selected policy tests, create waivers, and promote policy-test results. For more information, see:</p> <ul style="list-style-type: none"> • How Do I Monitor Compliance Statistics? (on page 137) • Working with Policy Test Results in a Node Properties Dialog (on page 335)
TFTP Script	Custom nodes	Defines a script to be run each time Tripwire Enterprise communicates with the device's TFTP client.
Variables	Database nodes Directory nodes File server nodes	Contains any local variables that have been created for the node. For more information, see What are Global and Local Variables? on page 196 .
Version	Custom nodes	Defines a regular expression to collect the make, model, and version number of the monitored system.
Web-Based Login	VI hypervisor nodes (only applies to VMware ESXi 5.0 & later)	<p>Specifies authentication credentials for HTTPS connections between your TE Server and the node.</p> <p>Note: If the Use Default Authentication check box is selected, TE uses the credentials defined by the VI management node containing the hypervisor node (see the ESXi Web-Based Login tab).</p>


Changing the Properties of a Node Group

Notes This procedure explains how to change the properties of a node group displayed in the main pane of the Node Manager. However, you can also change the properties of a node group in the **Parent Groups** tab of a node properties dialog (see [Changing the Properties of a Node on page 321](#)) or node group properties dialog (accessed below).

Under a VI management node, clusters and datacenters are represented by static node groups that lack any properties. If an Agent has been installed on a virtual machine, the virtual machine will also be represented by a static node group that contains the Agent node and virtual machine node. For more information, see [Discovering and Synchronizing a VMware Virtual Infrastructure on page 60](#).

To change the properties of a node group:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the group containing the node group.
3. In the **Name** column, select the node group.
4. As needed, modify the tabs in the node group properties dialog. For tab descriptions, see [Table 89](#).

Tip For more information, click  **Help** in any tab.

5. Click **OK**.

Table 89. Tabs in node group properties

Tab	Description
General	The name and description (optional) of the node group. Note: You can only change the name of a smart node group by renaming the corresponding tag set or saved filter in the Asset View tab. For more information, see Working with Tags and Tag Sets (on page 352) and Working with Saved Filters (on page 353)
Parent Groups	Displays the full path of each node group to which this node group is linked. <ul style="list-style-type: none">• This tab includes some of the same buttons that appear in the Node Manager. For guidance in using these buttons, refer to the corresponding procedure in this chapter.• To view or edit the properties of a node group, select the group's link.
Security	Contains any access controls that have been created for the node group. For more information, see Working with Node Access Controls on page 333 .

Changing the Properties of an Element


To change the properties of an element:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the group containing the element's node.
3. In the tree pane, click the node. Tripwire Enterprise displays the node's elements in the main pane.

Note If Detailed Node View is enabled, you must first select a rule to display elements in the main pane. To enable or disable Detailed Node View, see [Changing User Preference Settings on page 262](#).

4. In the **Element** column, click the desired element.
5. As needed, modify the tabs in the element properties dialog. For tab descriptions, see [Table 90 on the next page](#).

Tips You can also open an element properties dialog by selecting an element in the Elements tab of a node properties dialog (see [Changing the Properties of a Node on page 321](#)).

For more information, click  **Help** in any tab.

6. Click **OK**.

Table 90. Tabs in element properties

Tab	Available with any element that represents ...	Description
General	Any monitored object	Identifies the monitored object represented by the element, along with associated Tripwire Enterprise objects.
History	Any monitored object	Contains a list of versions created for the element. For more information, see Changing the Properties of an Element Version below . Note: This tab includes some of the same buttons that appear in the Node Manager. For guidance in using these buttons, refer to the corresponding Node Manager procedure in this chapter.
Log Center Events	Any monitored object	Displays TLC log messages for events involving the monitored object. Note: This tab does not appear in element property dialogs if the Allow TE to use information from Tripwire Log Center setting is disabled (see Changing Log Management Settings on page 268).
Packages	A file or directory (in a file system only) A registry key or entry	Identifies any software-installation packages associated with the monitored object. Note: To collect package information, select the Package Data attribute in the criteria set associated with the start point that identified the element (see Changing Criteria Set Properties on page 308).
Properties	Any monitored object	Defines the values of custom properties assigned to the element (see Defining Custom Property Values for an Element on page 330).

Changing the Properties of an Element Version

To change the properties of an element version:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the group containing the version's node.
3. In the tree pane, click the node. Tripwire Enterprise displays the node's elements in the main pane.

Note If Detailed Node View is enabled, you must first select a rule to display elements in the main pane. To enable or disable Detailed Node View, see [Changing User Preference Settings on page 262](#).

4. In the **Element** column, click the desired element.
5. In the element properties dialog, click the **History** tab and select the element version in the **Version** column.
6. As needed, modify the tabs in the version properties dialog and click **OK**. For tab descriptions, see [Table 91 on the next page](#).

Tip For more information, click  **Help** in any tab.

Table 91. Tabs in element version properties

Tab	Available with any version that represents ...	Description
Attributes	Any monitored object	Indicates the value of each of the version's attributes.
Content	A file A database object Query results	Displays the content of the monitored object. Note: If the version represents a file on a file server, the Content tab will only appear if the element was identified by a start point with the 'Archive element content' setting enabled (see Changing or Deleting Start Points on page 466).
General	Any monitored object	Identifies the version's element, creation date, severity level, and other properties.
Log	Any monitored object	Lists any TE log messages generated by events involving the element version. For definitions of log message categories, see Table 47 on page 167 .
Packages	A file or directory (in a file system only) A registry key or entry	Identifies any software-installation packages associated with the monitored object.
Permissions	A file or directory in a Windows file system A registry key or entry	Lists all Windows user accounts and groups with access to the monitored object, along with the permissions granted to each.
Properties	Any monitored object	Defines the values of custom properties assigned to the element version (see Defining Custom Property Values for an Element Version on page 331).

Defining Values for Custom Properties

Defining Custom Property Values for a Node

For an introduction to custom properties, see [What are Custom Properties? on page 197](#).

To change the custom properties for a node:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the node group containing the node.
3. In the main pane, select the node in the **Name** column.
4. In the node properties dialog, select the **Properties** tab.

- The Properties tab displays the node custom properties defined in the Settings Manager. For each property, the node has one of the following values:

- The property's **default value** (assigned in the Settings Manager)
- A **custom value** (a value previously defined in this tab)

If a custom value has *not* been defined for a property, the property's value is determined by its **Inherit the default if no value is specified** setting.

- If this setting is enabled, the property's default value applies to the node.
- Otherwise, the property does not apply to the node.

To modify this setting for a property, see [Working with Custom Properties on page 298](#).

Note In the Properties tab, default values appear in *italics*.

From the **Show properties that are** drop-down, select one of the following values:

- All** displays all node custom properties defined in the Settings Manager.
- Explicitly set** displays the properties for which a custom value has been defined for the node.
- Inherited** displays the properties for which the default value applies to the node.
- Not in use** displays the properties that do *not* apply to the node.

- As appropriate, edit the values of the displayed custom properties.

To define a custom value:

- In the drop-down list for the property, select **Change to**. Tripwire Enterprise presents additional fields for the property.
- In the new fields, define the custom value.

Tips If you cannot edit the value of a custom property, the property's **Editable in property editor** setting may be disabled. If a property's **Inherit the default if no value is specified** setting is enabled, a custom value can be null (no value). To adjust these settings, see [Working with Custom Properties on page 298](#).

To delete a custom value, select **Remove** from the property's drop-down list. (The Remove option is only available if the property currently has a custom value.)

- Click **OK**.

Defining Custom Property Values for an Element

For an introduction to custom properties, see [What are Custom Properties? on page 197](#).

Tip This procedure explains how to modify the custom properties of an element displayed in the main pane of the Node Manager. However, you can also modify the properties of elements in the **Elements** tab of a node properties dialog (see [Changing the Properties of a Node on page 321](#)).

To change the custom properties for an element:

1. In the Manager bar, click **NODES**.
2. In the tree pane, select the element's node.

Note If Detailed Node View is enabled, you must select the element's rule under the node in the tree pane. To enable or disable Detailed Node View, see [Changing User Preference Settings on page 262](#).

3. In the main pane, click the element in the **Element** column.
4. In the element properties dialog, select the **Properties** tab.
5. The Properties tab displays the element custom properties defined in the Settings Manager. For each property, the element has one of the following values:
 - The property's **default value** (assigned in the Settings Manager)
 - A **custom value** (a value previously defined in this tab)

If a custom value has *not* been defined for a property, the property's value is determined by its **Inherit the default if no value is specified** setting.

- If this setting is enabled, the property's default value applies to the element.
- Otherwise, the property does not apply to the element.

To modify this setting for a property, see [Working with Custom Properties on page 298](#).

Note In the Properties tab, default values appear in *italics*.

From the **Show properties that are** drop-down, select one of the following values:

- **All** displays all element custom properties defined in the Settings Manager.
 - **Explicitly set** displays the properties for which a custom value has been defined for the element.
 - **Inherited** displays the properties for which the default value applies to the element.
 - **Not in use** displays the properties that do *not* apply to the element.
6. As appropriate, edit the values of the displayed custom properties.

To define a custom value:

- a. In the drop-down list for the property, select **Change to**. Tripwire Enterprise presents additional fields for the property.
- b. In the new fields, define the custom value.

Tips If you cannot edit the value of a custom property, the property's **Editable in property editor** setting may be disabled. If a property's **Inherit the default if no value is specified** setting is enabled, a custom value can be null (no value). To adjust these settings, see [Working with Custom Properties on page 298](#).

To delete a custom value, select **Remove** from the property's drop-down list. (The Remove option is only available if the property currently has a custom value.)

7. Click **OK**.

Defining Custom Property Values for an Element Version

For an introduction to custom properties, see [What are Custom Properties? on page 197](#).

To change the custom properties for a version of an element:

1. In the Manager bar, click **NODES**.
2. In the tree pane, select the element's node.

Note If Detailed Node View is enabled, you must select the element's rule under the node in the tree pane. To enable or disable Detailed Node View, see [Changing User Preference Settings on page 262](#).

3. In the main pane, click the element in the **Element** column.
4. In the element properties dialog, select the **History** tab.
5. In the **Version** column, click the element version.
6. In the version properties dialog, select the **Properties** tab.
7. The Properties tab displays the version custom properties defined in the Settings Manager. For each property, the element version has one of the following values:
 - The property's **default value** (assigned in the Settings Manager)
 - A **custom value** (a value previously defined in this tab)

If a custom value has *not* been defined for a property, the property's value is determined by its **Inherit the default if no value is specified** setting.

- If this setting is enabled, the property's default value applies to the element version.
- Otherwise, the property does not apply to the version.

To modify this setting for a property, see [Working with Custom Properties on page 298](#).

Note In the Properties tab, default values appear in *italics*.

From the **Show properties that are** drop-down, select one of the following values:

- **All** displays all version custom properties defined in the Settings Manager.
- **Explicitly set** displays the properties for which a custom value has been defined for the element version.
- **Inherited** displays the properties for which the default value applies to the element version.
- **Not in use** displays the properties that do *not* apply to the element version.

8. As appropriate, edit the values of the displayed custom properties.

To define a custom value:

- a. In the drop-down list for the property, select **Change to**. Tripwire Enterprise presents additional fields for the property.
- b. In the new fields, define the custom value.

Tips If you cannot edit the value of a custom property, the property's **Editable in property editor** setting may be disabled. If a property's **Inherit the default if no value is specified** setting is enabled, a custom value can be null (no value). To adjust these settings, see [Working with Custom Properties on page 298](#).

To delete a custom value, select **Remove** from the property's drop-down list. (The Remove option is only available if the property currently has a custom value.)

9. Click **OK**.


Working with Node Access Controls

Creating an Access Control for a Node or Node Group

For an introduction to access controls, see [What are Access Controls? on page 208](#).

Note If one or more access controls have already been created for the node or node group, an additional access control can only be created by the default administrator account or a user account assigned to one of the existing access controls.

To set an access control for a node or node group:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the group containing the node or node group.
3. In the main pane, click the node or node group in the **Name** column.
4. In the properties dialog, click the **Security** tab.
5. Click  **Add Control**.
6. Select the check box of each **Principal** (user or user group) to be assigned to the access control and click **Next**.
7. Select the user role for the access control and click **Finish**.

Changing an Access Control for a Node or Node Group

For an introduction to access controls, see [What are Access Controls? on page 208](#).

Note An access control can only be changed by the default administrator account or a user account assigned to the control.

To change the user role assigned to an access control:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the group containing the node or node group associated with the access control.
3. In the main pane, click the node or node group in the **Name** column.
4. In the properties dialog, click the **Security** tab.
5. In the **Access Control** column, select the access control.
6. In the Access Control dialog, select the new user role and click **OK**.

Deleting Access Controls for a Node or Node Group

Note An access control can only be deleted by the default administrator account or a user account assigned to the control.

Caution With an access control, non-Administrators may be granted Administrator-level access to a particular node or node group. If the access control is deleted, the user will no longer be able to modify the properties of the node or node group.

To delete an access control from a node or node group:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the group containing the node or node group associated with the access control.
3. In the main pane, click the node or node group in the **Name** column.
4. In the properties dialog, select the **Security** tab.
5. Select the check box of each access control to be deleted.
6. Click **✕ Delete**.
7. Click **OK** to confirm.

Working with Policy Test Results in a Node Properties Dialog

Re-Running Policy Tests for a Single Node


For a single node, this procedure runs specified policy tests with effective scopes that include the node. When a test runs, TE generates a new test result for the specified node only.

If you specify a TE policy or policy test group with this procedure, TE will run each descendant policy test that meets the following criteria:

- The node must be included in the effective scope of the test.
- If the test exists under a TE policy, the policy cannot contain a waiver that specifies the test/node pair.

For more information, see [How Does a Policy Test Work? on page 135](#).

To re-run policy tests for a single node:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the node group containing the node.
3. In the main pane, select the node in the **Name** column.
4. In the node properties dialog, select the **Test Results** tab. This tab displays the hierarchy of Policy Manager objects.
5. In the tree pane of the Test Results tab, select the TE policy or policy test group containing the Policy Manager objects to be run.
6. To run all eligible policy tests in the selected TE policy or group, proceed to the next step. Otherwise, select the check box of each Policy Manager object to be run.
7. Click  **Re-Run Test**.
8. If a confirmation dialog opens, click **OK**.

Adding a Waiver to a TE Policy for a Single Node


With this procedure, you can create a waiver in the Test Results tab of a node's properties dialog. In the New Waiver Wizard, TE will only present test/node pairs that include the node.


For more information, see [What are Policy Scores? on page 138](#).


To create a waiver in the properties dialog of a node:



1. In the Manager bar, click **NODES**.
2. In the tree pane, click the node group containing the node.
3. In the main pane, select the node in the **Name** column.
4. In the node properties dialog, select the **Test Results** tab.
5. In the tree pane of the Test Results tab, select a TE policy or a policy test group.
6. To create a waiver for any policy tests descended from the selected policy or group, proceed to the next step.

To create a waiver for specific policy tests and/or groups, select the check box of each object in the main pane.

7. Click  **New Waiver**.
8. In the general waiver information page:
 - a. Enter a **Name** for the waiver.
 - b. Select a **TE Policy** for the waiver.
 - c. Complete the remaining fields and click **Next**.

Tip For more information, click  **Help** in any wizard page.

9. The wizard presents a list of the test/node pairs that include the node.
 - To include all displayed test/node pairs in the waiver, click **Next**.
 - To remove specific test/node pairs from the waiver, select the check box of each pair and click  **Delete**. Then, click **Next**.

Tip To add other test/node pairs to the waiver, use the following buttons:
Click  **Add tests with failures** to add test/node pairs for other TE policies or policy test groups.
Click  **Add nodes with failures** to add test/node pairs for other nodes.

10. The wizard presents a list of any specified test/node pairs that are not in the scope of the TE policy (if any). These pairs will be omitted from the waiver.


To complete the wizard, click **Finish**.

Promoting Policy Test Results Generated for a Node

With this procedure, you can modify the conditions that define the pass/fail criteria for one or more policy tests that have generated results for a specified node. Specifically, you can either modify a test's conditions based on values reflected in the most recent result generated by the test, or enter customized conditions of your choosing. For more information, see [What is Policy Test Promotion?](#) on page 146.

To modify the pass/fail conditions of policy tests that have generated results for a node:


1. In the Manager bar, click **NODES**.
2. In the tree pane, click the node group containing the node.
3. In the main pane, select the node in the **Name** column.
4. In the node properties dialog, select the **Test Results** tab. This tab displays the hierarchy of objects in the Policy Manager.
5. In the tree pane of the Test Results tab, select the TE policy or policy test group containing the policy tests to be modified.

Tips For more information, click  **Help** in any dialog or wizard page.

A test result indicator overlays the icon of each Policy Manager object in the Test Results tab. For further details, see [How Do I Review the Results of Policy Tests?](#) on page 144.

6. To modify the pass/fail conditions of any policy tests descended from the selected TE policy or group, proceed to the next step.

To modify the pass/fail conditions of specific policy tests, or all tests descended from specific TE policies or groups, select the check box of each object in the main pane.

7. Click  **Promote**.
8. The Promote Test Results dialog presents a complete list of all specified policy tests that have generated results for the node. For a description of each column in this dialog, see [Table 125](#) on page 563.

[Table 126](#) (on page 564) defines each of the promotion options that may be available from the Action drop-down for each test. By default, TE enters **Ignore** as the promotion option for each test. To change this setting for a test, select another option from the **Action** drop-down.

- If you select the **Customize** promotion option for a policy test, TE presents a dialog with the current pass/fail conditions of the test. Modify the conditions as needed, and click **OK**.
- The **Expand** and **Restrict** promotion options are only available if the current result of the test includes values that would support the option. For instance, if a test result does not include a value for which a new condition may be added to the test, TE excludes the Expand option from the Action drop-down menu.

9. When you finish specifying promotion methods for the listed policy tests, click **Next**.
10. (Optional) As a precautionary measure, you can now export the selected tests to an XML file. If your changes have undesirable or unintended consequences, you can simply re-import the XML file at a later time to return the policy tests to their original states.

To export the existing (i.e. pre-promotion) versions of the tests to an XML file:

- a. Click **Export**.
 - b. Complete the appropriate steps for your system.
11. In the Promote Test Results Wizard, click **Finish**.

Classifying Nodes with Tags

Getting Started with Tags

In Tripwire Enterprise you can use tags to classify the servers, network devices, and other systems that you monitor. This section introduces tags and related objects and walks you through the process of configuring them. You can follow these steps to configure tagging at any time, before or after you add nodes to your TE implementation. In addition, you can easily change your tag configuration later as your enterprise and processes change.

Tips To learn about best practices for using tags and smart node groups, see [Tagging Best Practices on page 342](#).

To automatically assign tags to new nodes, see [Using Tag Files to Assign Tags to New TE Agents and Step 3. \(Optional\) Create Tag Files to Assign Tags to New Axon Agents](#) in the *Tripwire Enterprise Installation & Maintenance Guide*.

To get started with tags in Tripwire Enterprise:

1. In the Manager bar, click **NODES** and select the **Asset View** tab.

The Asset View tab provides a complementary view of the objects in the Nodes tab of the Node Manager. Each node in the Nodes tab is represented by an **asset** in the Asset View tab. For an overview of Asset View components and features, see [Using the Asset View Tab on page 346](#).

2. To create tag sets and tags, click **Manage Tagging** in the upper left corner, then select **Tag Sets** in the left pane.

Tags are descriptors that you can create and assign to your assets. You can assign as many tags to an asset as you like and you can always rename or delete the tags later. Tags are organized using **tag sets**, which group a set of related tags. For example, a tag set named `Location` could include the tags `Portland`, `Chicago`, and `New York`. These tags would be represented in TE as `Location:Portland`, `Location:Chicago`, and `Location:New York`.

3. Create tag sets and tags to characterize and organize the assets that you want to monitor with Tripwire Enterprise.

Tag sets named `Location`, `Owner`, and `Platform Family` are created by default. You can create tags for these tag sets or create your own tag sets and tags. For more information, see [Working with Tags and Tag Sets on page 352](#).

4. After creating tags and tag sets, you can manually apply them to the assets in the Asset View tab. For details, see [Manually Applying Tags to Assets on page 350](#).

In addition to user-created tag sets, Tripwire Enterprise includes the following pre-defined tag sets:

- **system tag sets** organize your assets based on operating system, device type, or other criteria. These tags are automatically assigned to assets when you add them to TE. You can't edit or delete system tag sets or apply them to assets.
- **operational tag sets** help you to manage the health of your assets by identifying errors. Operational tags are applied to assets by TE, and can only be changed by clearing the error messages for an asset. For more information, see [Monitoring the Health of Nodes and Resolving Errors on page 317](#).

5. After creating and assigning tags in the Asset View tab, click the **Nodes** tab to see how tags are represented there.

In the Nodes tab, a **smart node group** corresponds to each tag set in the Asset View tab. When you add a new node, TE automatically links the node into one of more of these groups, depending on the system tags assigned to it.

Note Smart node groups are enabled by default in new installations of Tripwire Enterprise. If your Tripwire Enterprise installation was upgraded from an earlier version, click **Smart Node Groups: disabled** at the bottom of the Node Manager to enable them.

You can also enable smart node groups in the System Preferences section of the Settings Manager. For more information, see [Changing System Preferences on page 266](#).

6. Expand the **Smart Node Groups** group, then expand **System Tag Sets** and **Tag Sets**.

If you have already added nodes to Tripwire Enterprise, you will notice that those nodes are linked to groups in the System Tag Sets node group based on their operating system or device type. If you manually assigned tags to nodes, those nodes are linked to the corresponding groups in the Tag Sets node group. For more information on how smart node groups work, see [About Node Groups and Smart Node Groups on page 57](#).

7. Return to the Asset View tab, click **Manage Tagging** in the upper left corner, then select **Saved Filters** in the left pane.

You probably noticed the Saved Filters group in the Smart Node Group tree. **Saved filters** are defined collections of tags that you can use to classify sets of assets. For example, you could create a saved filter named **Portland Win2K3 PCI** that includes any asset with the following combination of tags:

- Location:Portland
- Operating System:Windows 2003 Server
- Policy:PCI

After creating this filter, you could use the smart node group associated with it to scope version checks or reports on compliance.

8. If desired, create saved filters to further classify your assets in TE. For more information, see [Working with Saved Filters on page 353](#).
9. After you are done with saved filters, click **Tagging Profiles** in the left pane.

With **tagging profiles**, you configure TE to apply tags automatically to assets that have specific characteristics. For example, you could create a profile to assign the tag `Owner:Windows Admin` to all Windows assets. Or you could assign `Dept:Finance` to all assets with "finance" in their hostname that are also within a specific IP address range. Tagging profiles enable you to apply tags to a large number of assets quickly and precisely, and to ensure that new assets are tagged properly.

10. If desired, create manual or automatic tagging profiles. For more information, see [Working with Tagging Profiles on page 354](#).

Tagging Best Practices

With tags in Tripwire Enterprise, you can manage more assets than ever before, in less time, and with fewer resources. Tags enable you to organize, view, and control assets using whatever criteria is important to you - business unit, operating system, policy, risk, owner, or applications installed. Since tags and filters are easy to change, you can quickly reconfigure and reorganize your assets as your business evolves.

For an overview of tagging functionality, see [Getting Started with Tags on page 339](#) and [About Node Groups and Smart Node Groups on page 57](#).

Note This section describes best practices developed by Tripwire Professional Services and early adopter customers, but the "state of the art" is always changing. For the latest information on using tags and smart node groups, see:

https://tripwireinc.force.com/customers/CommunitySiteLogin?startURL=/articles/Standard_Operations/Asset-Tagging-Best-Practices-and-Using-Smart-Node-Groups

Guidelines for Using Tags

Start small. Don't try to lay out your entire tag-based classification before you start applying tags. Choose a tag and apply it appropriately. See what you learned there, and then move on. You are going to see value in doing even a little bit of tagging, and you should feel free to iterate on your tagging at your own pace. For more information, see [Working with Tags and Tag Sets on page 352](#).

Use tag files to automatically apply tags when onboarding new nodes. A **tag file** is a text file on an Agent system that specifies tags to be assigned to the asset the first time it is added to a TE Console. For more information on tag files, see [Using Tag Files to Assign Tags to New TE Agents](#) and [Using Tag Files to Assign Tags to New Axon Agents](#) in the *Tripwire Enterprise Installation & Maintenance Guide*.

Use tagging profiles to automate the tagging process. If you can tell programmatically what tag should be applied for a given situation, create a tagging profile to apply it automatically. Tagging profiles will take much of the work out of applying tags, and ensure that you are up to date as new assets come online. For more information, see [Working with Tagging Profiles on page 354](#).

Tags and tag sets should represent a single group or type. Do not join concepts with 'and' or 'or' in a single tag or tag set. For example, avoid creating tags like `Location:Seattle&Portland` or `Application&Role:Exchange Server`. Instead, create `Location:Seattle` and `Location:Portland`. You can easily combine these tags while filtering if you do want to see assets that are either in Seattle or Portland, but it may be hard to make that distinction later if you report on a single combined tag.

All tags should have semantic value in themselves. Tags should mean something when read, even out of context. When creating tags, consider how they might appear on a report. Avoid tags like `Risk:2` or `Vulnerability:3` and instead use `Risk:Medium` or `Vulnerability:Low`.

Use affirmative tags whenever possible. Instead of creating tags like `Policy:Not PCI`, use the default `Untagged` tag to reflect the absence of a state. In some cases, it may be useful to have a tag like `Location:Unknown`, however.

Avoid abbreviations. Avoid tags like `Server Role:DC` and instead spell out `Server Role:Domain Controller`. When working with a single group or type, there is almost always room to write it out completely.

Avoid creating more than 2000 tags. Asset View currently performs best with 2000 or fewer tags, and will become less responsive as you approach and exceed the 2000 tag mark.

Tagging Tips and Tricks

Viewing the intersection between two or more tags from the same tag set.

To see assets that have the tags `Business Unit:Commercial` and `Business Unit:Sales`, filter in Asset View using one of the tags and then type the other tag in as a keyword search. You will always get the intersection between a tag and a keyword.

To add a third tag, save the previous tag and keyword combination as a saved filter and use that saved filter to filter assets. Then type in a third tag as a keyword search. You will always see the intersection between a tag and a saved filter, even if the tags in the saved filter come from the same tag set as the individual tag.

Use the counts in the filter pane to provide additional context to any tag selection.

As soon as you filter by a tag, all of the other tag counts update. That means that you only have to look at the counts next to the other tags to see how they relate to your selected tag.

For example, if you click on `Priority:Critical` and then look in the `Owner` tag set, you will immediately know which owners have critical assets, just by looking at the counts. The only caveat here is that tag counts will not provide interaction information for tags within the same tag set.

Use saved filters in Asset View as a shortcut for tag combinations that you filter on frequently.

Saved filters enable you to combine combinations of tags to schedule checks, filter reports, etc. However, you can also use saved filters in the Asset View tab to quickly view assets that you are interested in. For example, you could quickly identify all of the high priority assets in Portland that are in scope for PCI by creating a saved filter with `Priority:High`, `Location:Portland`, and `Policy:PCI` tags specified. For more information, see [Working with Saved Filters on page 353](#).

Tagging Strategies and Sample Tag Sets

With tags, you can organize your assets any way you want to, but the strategies below show some of the patterns that have worked well so far. [Table 92 on the next page](#) lists some suggested sample tag sets.

1. Tag for **policies** - this is typically based on operating system information and role.
2. Tag for **check rule tasks** - this is frequently done based on location and/or business unit, but it depends on how you segment your assets to time their checks.
3. Tag for **reports** - this will include tags like Priority and Owner, but it can include a many more. These tags give context to the results of your reports.
4. Tag for **asset management** - this can include tags like Priority and temporary tags like Status:Decommissioned or Status:New. You can use these tags when you need to work on an asset.

Table 92. Sample Tag Sets

Application:	Priority:
Microsoft SQL	Critical
Oracle	High
<i>Untagged</i>	Medium
	Low
	<i>Untagged</i>
Business Unit:	Risk:
Commercial	High
Consumer	Medium
Corporate	Low
HR	<i>Untagged</i>
Sales	
<i>Untagged</i>	
Location:	Server Role:
Corporate Office	Domain Controller
Portland	Domain Member
Store 125	Standalone (DMZ)
Unknown	Financial Reporting (Internal)
<i>Untagged</i>	Payment Card Gateway (Network)
	Web Server
	<i>Untagged</i>
Owner:	Vulnerability:
Bill	High
Ted	Medium
<i>Untagged</i>	Low
	<i>Untagged</i>
Platform Family:	Sample Saved Filters:
Windows	PCI - Critical Portland Windows assets
Linux	PCI – Domain Controller
Solaris	Bill’s Critical & High Priority assets
<i>Untagged</i>	PCI – Critical Disabled Corporate assets
	High Priority Corporate assets with
	Connection Errors
Policy:	
PCI	
CIS	
<i>Untagged</i>	

Using the Asset View Tab

In the Asset View tab of the Node Manager, you can view and manage your assets based on the tags assigned to them. For more information on tags and other components in the Asset View tab, see [Getting Started with Tags on page 339](#).

During normal use, the Asset View tab consists of three components (see [Figure 26 below](#)):

- The left pane is the **Asset Filter**, where you can apply filters to change the assets displayed in the Asset List. For more information, see [Filtering Assets on page 348](#).
- The middle pane is the **Asset List**, which displays assets that match the selected criteria. You can examine the properties of the assets displayed here, or add them to the current selection. For more information, see [Viewing and Selecting Assets on page 349](#).
- The right pane is the **Selection Information** pane, which displays a list of selected assets, or information about the currently selected asset. In this pane, you can also open the **Tags Drawer** to assign tags to assets or change the tags that are currently assigned. For more information, see [Manually Applying Tags to Assets on page 350](#).

To make changes to tags, saved filters, or tagging profiles you switch the Asset View tab to an editing mode (see [Figure 27 on the next page](#)). For more information on using Asset View in this mode, see:

- [Working with Tags and Tag Sets \(on page 352\)](#)
- [Working with Saved Filters \(on page 353\)](#)
- [Working with Tagging Profiles \(on page 354\)](#)

Figure 26. The Asset View tab

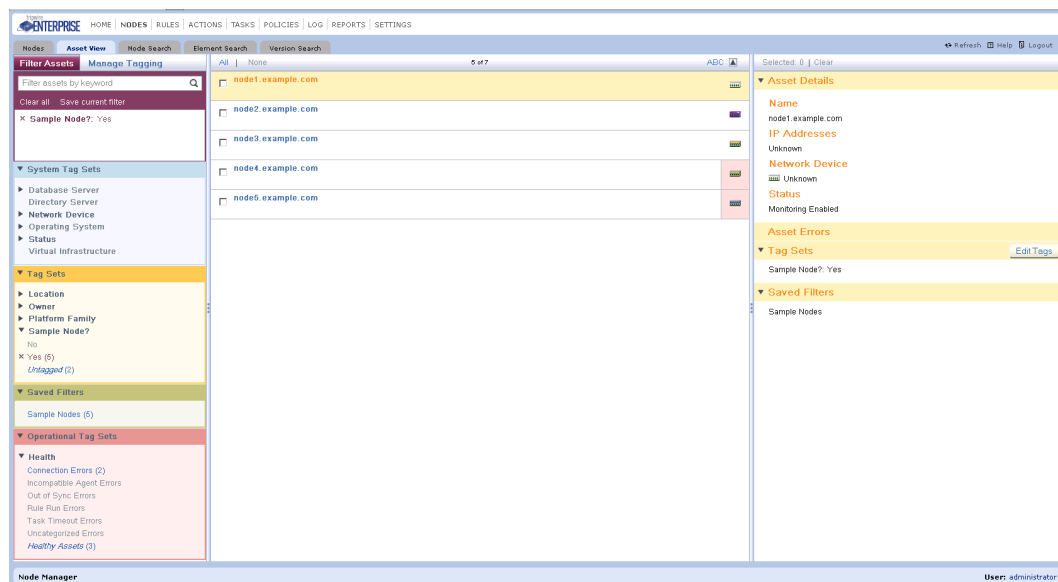
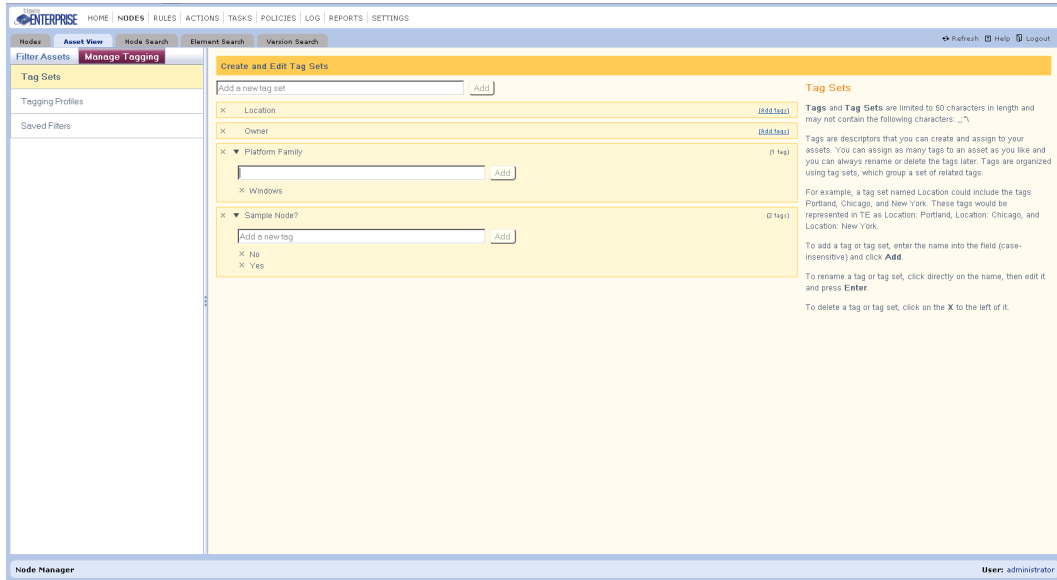


Figure 27. The Asset View tab when editing tags



Filtering Assets

The Asset Filter pane lists tag sets and saved filters that you can use to filter the assets in the Asset List. For more information on these objects, see:

- [Working with Tags and Tag Sets \(on page 352\)](#)
- [Working with Saved Filters \(on page 353\)](#)

The Asset Filter shows the number of assets associated with each tag. As you select tags to filter assets, these numbers change to reflect the currently displayed set of assets. If a tag isn't associated with any displayed assets, it is disabled.

Tip You can also view assets in Asset View by selecting nodes in the Nodes Manager and clicking **Manage > Tags**. For more information, see [Viewing Specific Nodes or Groups in Asset View on page 351](#).

To filter the assets displayed in the Asset List:

1. In the Asset Filter pane, filter assets using any combination of the following:
 - **To filter assets using keywords**, enter one or more strings in the keyword search field at the top of the pane. TE will display assets that contain **any** of the specified strings in their name, IP addresses, or in the tags associated with the assets.
 - **To filter assets using the tags assigned to them**, expand Tag Sets, System Tag Sets, or Operational Tag Sets and select one or more tags.
 - **To filter assets using saved filters**, expand Saved Filters and select one or more saved filters.

Note When you specify multiple filter criteria, TE interprets criteria in the same tag set, system tag set, or saved filter using a logical OR operator. Criteria from different tag sets or saved filters are interpreted using an AND operator. For example, if you select `Location:Portland`, `Location:Seattle`, and `Owner:Bob`, the Asset List displays all assets that Bob owns **and** that are in either Portland **or** Seattle.

2. TE lists the filters that are currently being used at the top of the Asset Filter pane. To clear all of the current filters, click **Clear all**. To clear a single filter, click **×** in front of the item that you want to clear.

Tip To save the current filtering criteria as a saved filter, click **Save current filter** at the top of the Asset Filter pane. For more information, see [Working with Saved Filters on page 353](#).

Viewing and Selecting Assets

To see the properties of an asset:

1. (Optional) Use the Asset Filter pane to refine the list of assets in the Asset List, or choose assets to be displayed directly from the Nodes tab (see [Viewing Specific Nodes or Groups in Asset View on page 351](#)).
2. Click on (**don't** select the checkbox for) an asset in the Asset List.

TE displays information about the asset in the Selection Information pane. You can also clear the errors for this asset from this pane. For more information, see [Monitoring the Health of Nodes and Resolving Errors on page 317](#).

Tip If you have assets selected in the Asset List and you use the process above to view the properties of an asset, click the **Selected:** link at the top of the Selection Information pane to switch back to the list of selected assets.

To select assets:

1. (Optional) Use the Asset Filter pane to refine the list of assets in the Asset List, or choose assets directly from the Nodes tab (see [Viewing Specific Nodes or Groups in Asset View on page 351](#)).
2. In the Asset List, click the checkbox for each asset that you want to select.
 - Use the **All** or **None** selectors at the top of the Asset List to select or clear all assets currently displayed in the list.
 - Assets in the Asset List are sorted by name. Use the **ABC** selector to toggle between ascending and descending sort order for assets.

As you select each asset, it is added to the list in the Selection Information pane. This list persists even if you change the filters to display different assets in the Asset List.

Tip The Selection Information pane only displays the first 500 selected assets. Additional assets are still included in the selection, but are not displayed individually.

To remove assets from the current selection:

To remove a single asset from the list, click **×** in front of that asset in the Selection Information pane.

To remove all assets from the list, click **Clear** at the top of the Selection Information pane.

Manually Applying Tags to Assets

To edit the tags for a list of assets:

1. (Optional) Use the Asset Filter pane to refine the list of assets in the Asset List, or choose assets directly from the Nodes tab (see [Viewing Specific Nodes or Groups in Asset View on the next page](#)).
2. In the Asset List, click the checkbox for each asset whose tags you want to edit.
3. In the Selection Information pane, click **Edit Tags** to open the Tags Drawer.

Tip You can also click **Dismiss Errors** to clear the errors for all selected assets. For more information on errors, see [Monitoring the Health of Nodes and Resolving Errors on page 317](#).

4. In the Tags Drawer, select or clear the tags that are applied to the asset. AM uses the following states for the checkboxes in this dialog:
 - means that the tag is applied to all of the selected assets
 - means that the tag is not applied to any of the selected assets
 - means that the tag is applied to some of the selected assets.
5. Click **Close** to apply your changes and close the Tags Drawer.


Note If **Enable dynamic policy run** is selected in the System Preferences section of the Settings Manager, when a tag is applied to an existing node and that tag causes the node to be included in the scope of a TE policy, TE will evaluate all existing elements for tests under the newly-associated policy.

For more information, see [Changing System Preferences on page 266](#).

Viewing Specific Nodes or Groups in Asset View

With the Tag button, you can select nodes or node groups in the Nodes tab and then view the selected items in the Asset View tab. This makes it easier to apply tags that reflect your existing node hierarchy.

To view nodes or node groups in Asset View:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the group containing the node or node group you want to open in Asset View.
3. In the main pane, select the check box of each node or node group.
4. Click **Manage** >  **Tag**.

The Asset View tab opens with the selected nodes (and any nodes in the selected groups) selected in the Asset List pane.

To apply tags to the selected assets, see [Manually Applying Tags to Assets on the previous page](#).

Working with Tags and Tag Sets

Tags are descriptors that you can create and assign to your assets. You can assign as many tags to an asset as you like and you can always rename or delete the tags later. Tags are organized using **tag sets**, which group a set of related tags. For example, a tag set named Location could include the tags Portland, Chicago, and New York. These tags would be represented in TE as Location:Portland, Location:Chicago, and Location:New York.

Tip To automatically assign tags to new nodes, see *Using Tag Files to Assign Tags to New TE Agents* and *Using Tag Files to Assign Tags to New Axon Agents* in the *Tripwire Enterprise Installation & Maintenance Guide*.

In addition to user-created tag sets, Tripwire Enterprise includes the following pre-defined tag sets:

- **system tag sets** organize your assets based on operating system, device type, or other criteria. These tags are automatically assigned to assets when you add them to TE. You can't edit or delete system tag sets or apply them to assets.
- **operational tag sets** help you to manage the health of your assets by identifying errors. Operational tags are applied to assets by TE, and can only be changed by clearing the error messages for an asset. For more information, see [Monitoring the Health of Nodes and Resolving Errors on page 317](#).

Tag sets and system tag sets are represented by smart node groups in the Nodes tab of the Node Manager. For more information, see [About Node Groups and Smart Node Groups on page 57](#).

To manage tags and tag sets:

1. In the Manager bar, click **NODES** and select the **Asset View** tab.
2. In the upper left corner, select **Manage Tagging**.
3. In the left pane, select **Tag Sets**.

To add a tag set, enter the name of the new tag set (case-insensitive) and click **Add**.

To rename a tag set, click the set's name, then edit it and click **Enter**.

To delete a tag set, click **x** in front of the set. Review the system objects associated with the tag set, then click **Yes** to confirm.

4. To manage the tags in a tag set, first expand the set to see the tags that it contains.

To add a tag to a set, enter the name of the tag and click **Add**. The same tag name can be used in multiple tag sets.

To rename a tag, click the tag's name, then edit it and click **Enter**. The tag is renamed in the tag set, and also in every asset where the tag is applied.

To delete a tag, click **x** in front of the tag. Review system objects associated with the tag, then click **Yes** to confirm.

5. Click **Filter Assets** to return to the main Asset View dialog.

Working with Saved Filters

Saved filters are defined collections of tags that you can use to classify sets of assets. For example, you could create a saved filter named **Portland Win2K3 PCI** that includes any asset with the following combination of tags:

- Location:Portland
- Operating System:Windows 2003 Server
- Policy:PCI

After creating this filter, you could use it to scope version checks using an appropriate set of rules. Saved filters are represented by smart node groups in the Nodes tab of the Node Manager. For more information, see [About Node Groups and Smart Node Groups on page 57](#).

To manage saved filters:

1. In the Manager bar, click **NODES** and select the **Asset View** tab.
2. In the upper left corner, select **Manage Tagging**.
3. In the left pane, select **Saved Filters**.

To add a saved filter:

- a. Click **New Saved Filter**.
- b. Enter a name for the saved filter.
- c. (Optional) Specify a keyword and tags that the filter will use to select assets.
- d. Click **Save** to create the new saved filter.

To edit an existing saved filter, select the filter and click **Edit Saved Filter**.

To delete a saved filter, select the filter and click **Delete Saved Filter**. Review the system objects associated with the filter, then click **Yes** to confirm.

4. Click **Filter Assets** to return to the main Asset View dialog.

Working with Tagging Profiles

TE automatically applies **system tags** to assets based on their operating system, device type, the Agent version installed, or other criteria. With **tagging profiles**, you can configure TE to apply additional tags automatically to assets that have specific characteristics.

For example, you could create a profile to assign the tag `Owner:Windows Admin` to all Windows assets. Or you could assign `Dept:Finance` to all assets with "finance" in their hostname that are also within a specific IP address range.

Tagging profiles can apply tags automatically when new assets are added to TE, or you can run them manually to quickly apply tags to existing assets in TE.

To manage tagging profiles:

1. In the Manager bar, click **NODES** and select the **Asset View** tab.
2. In the upper left corner, select **Manage Tagging**.
3. In the left pane, select **Tagging Profiles**.

To add a tagging profile:

- a. Click **New Profile**.
- b. Enter a name for the profile and specify whether you want to run the profile manually or automatically. Automatic tagging profiles evaluate all existing assets when the profile is created, and also evaluate new assets when they are added to TE. Manual tagging profiles only evaluate assets when they are run from the Manage Tags dialog.
- c. In the **Choose Conditions** section, specify the conditions that the profile will use to select assets.

Tips

You can use the **Matches** and **Does Not Match** selectors to select assets by hostname or IP address using regular expressions. Choose one of these selectors and click **Regex Help** for information and examples.

Click **Refresh Preview** to see assets selected by the current conditions.

- d. In the **Choose Tags to Apply** section, specify the tags that the profile will assign to selected assets.
- e. Click **Save** to create the new profile. If you chose to run the profile automatically, TE will run the profile and list the number of assets matched.

To manually run an existing profile, select the profile and click **Run Profile Now**.

To edit an existing profile, select the profile and click **Edit Profile**.

To delete a profile, select the profile and click **Delete Profile**.

4. Click **Filter Assets** to return to the main Asset View dialog.


Searching for Nodes, Elements, and Versions

Searching for Nodes

Notes For an introduction to common search features such as wildcards, text-field qualifiers, and saved searches, see [How Do I Run a Search?](#) on page 232.



In the Node Search tab, the button bar contains many of the same buttons available in the Nodes tab. To use these buttons, refer to the procedures in [Chapter 6: Node Procedures](#) (on page 312).








To search for nodes:



1. In the Manager bar, click **NODES**.
2. Select the **Node Search** tab.
3. From the **Type** list, select **(any node)** or a specific node type. The available search fields vary by node type.
4. Enter search criteria. For guidance, see [Table 93 on the next page](#).
 - Some of the search criteria are based on values that can be edited in node property dialogs (see [Changing the Properties of a Node](#) on page 321).
 - The following search criteria only appear for custom node types: **Automatically append newlines, Command to execute, Make Pattern, Model Pattern, Pager prompt, Regular expression, Use DOS style line endings, Version identification method, and Version Pattern**.
 - All text-field entries are case-insensitive. For example, ‘Node’ and ‘node’ will return the same results.
 - Any string may be entered in a text field. For example, if you enter a string in the **Node name** field and select **Contains** as the text-field qualifier, search results will include any node with a name that includes the string.
5. Click  **Search**



Next If desired, you can save the entered search criteria for future use. For instructions, see [Creating a Saved Search](#) on page 234.

Table 93. Node search criteria

Search Criteria	To limit search results to ...
Additional configuration files	<p>... monitored systems with configuration files that have specific names (other than <code>running-config</code> and <code>startup-config</code>):</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial file name in the text field.
Alternative TFTP return address	<p>... monitored systems that receive returning TFTP communications through a firewall:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial firewall IP address in the text field.
Automatically append newlines	<p>... custom nodes that have the Automatically append newlines option enabled, select Yes.</p> <p>... custom nodes that do not have the Automatically append newlines option enabled, select No.</p> <p>Note: If enabled in the properties of a custom node, the Automatically append newlines setting directs TE to append a newline character to each value sent to the system represented by the custom node.</p>
Change time	<p>... monitored systems that have changed within a specific time period:</p> <ol style="list-style-type: none"> 1. Click  Time Chooser. 2. Complete the Time Chooser dialog and click OK. <p>Tip: Click  Help for more information.</p>
Command to execute	<p>... nodes with specified content in the command run to identify the monitored system's version:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a search string in the text field.
Communication timeout	<p>... monitored systems with specific communication timeouts:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a timeout value in the text field. <p>Note: A system's communication timeout is the amount of time of communication inactivity before Tripwire Enterprise Console terminates a connection with the system.</p>
Configuration file name(s)	<p>... monitored systems with configuration files that have specific names:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial file name in the text field.
Conforms to baselines	<p>... nodes with at least one element that varies from its current baseline, select No.</p> <p>... nodes for which all elements are in their current baseline state, select Yes.</p>
Connection method	<p>... network devices for which the Tripwire Enterprise Server employs Telnet or SSH to establish a connection, select Telnet or SSH.</p>

Search Criteria	To limit search results to ...
Current version content	<p>... nodes with specific content in at least one current version:</p> <ol style="list-style-type: none"> 1. Click  Content Criteria Chooser. 2. Complete the Current Version Content dialog and click OK. <p>Tip: Click  Help for more information.</p>
Descends from node group	<p>... nodes that descend from a specific node group:</p> <ol style="list-style-type: none"> 1. Click  Chooser. 2. Select the node group and click OK.
Element custom properties	<p>... nodes with at least one element that has specified values for element custom properties:</p> <ol style="list-style-type: none"> 1. Click  Custom Properties Chooser. 2. Complete the Custom Properties dialog and click OK. <p>Tip: Click  Help for more information.</p>
Element name	<p>... nodes with elements that have specific names:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial element name in the text field.
Enable username	<p>... monitored systems for which Enable Mode is activated by a specific username:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial username in the text field.
FTP port	<p>... network devices that listen on a specified port for FTP communications from the Tripwire Enterprise Server:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial port number in the text field.
Has failures	<p>... monitored systems that experienced a failure when your TE Server last attempted communication, select Yes.</p> <p>... monitored systems that did <i>not</i> experience a communication failure, select No.</p>
IP address	<p>... monitored systems with a specific IP address(es):</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial IP address in the text field.
Last registration time	<p>... Agent systems that registered with the Tripwire Enterprise Server within a specified time range.</p>
Latest version properties	<p>... nodes with at least one element with a current version that has specified values for version custom properties:</p> <ol style="list-style-type: none"> 1. Click  Custom Properties Chooser. 2. Complete the Custom Properties dialog and click OK. <p>Tip: Click  Help for more information.</p>

Search Criteria	To limit search results to ...
Make Pattern	<p>... custom nodes that use a specified regular expression to identify the monitored system's make or manufacturer:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a search string in the text field.
Manager username	<p>... monitored systems for which Manager Mode is activated by a specific username:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial username in the text field.
Model Pattern	<p>... custom nodes that use a specified regular expression to identify the monitored system's model:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial model number in the text field.
Node custom properties	<p>... nodes that have specified values for node custom properties:</p> <ol style="list-style-type: none"> 1. Click  Custom Properties Chooser. 2. Complete the Custom Properties dialog and click OK. <p>Tip: Click  Help for more information.</p>
Node description	<p>... nodes with specific user-entered descriptions:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial node description in the text field.
Node make	<p>... monitored systems with a specified make or manufacturer:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a search string in the text field.
Node model	<p>... monitored systems with specific model numbers:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial model number in the text field.
Node name	<p>... nodes with specific names:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial node name in the text field.
Node version	<p>... monitored systems with specific version numbers:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial version number in the text field.
Pager prompt	<p>... nodes with a specific pager prompt:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a search string in the text field.

Search Criteria	To limit search results to ...
Regular expression	<p>... custom nodes with specified content in the regular expression used to identify the monitored system's make, model, and version:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a search string in the text field.
Saved searches in Log Manager	<p>... nodes associated with a saved search defined in the Log Manager:</p> <ol style="list-style-type: none"> 1. Click  Chooser. 2. Select the saved search and click OK. <p>Tip: Click  Help for more information.</p>
Select Catalyst OS version	<p>... monitored systems with a specific version(s) of Cisco CatOS, select a version number from the drop-down list.</p>
SSH Cipher	<p>... monitored systems that use a specific encryption method for SSH communication, select an option from the drop-down list.</p>
SSH port	<p>... network devices that listen on a specified port for SSH communications from the Tripwire Enterprise Server:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial port number in the text field.
SSH private key file	<p>... monitored systems with specific SSH private key file names:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial file name in the text field.
TE Agent version	<p>... monitored systems with a specific TE Agent version(s) installed:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial TE Agent version number in the text field.
Telnet port	<p>... network devices that listen on a specific port for Telnet communications from the Tripwire Enterprise Server:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial port number in the text field.
Transfer method	<p>... network devices that communicate with your Tripwire Enterprise Server via a specific protocol, select FTP, TFTP, SFTP, or SCP.</p> <p>Note: The protocols available in this drop-down depend upon the type of node selected in the Type drop-down.</p>
Type	<p>... nodes of a specific type, select a type from the drop-down list. Otherwise, accept the default value (any node).</p>
Use : in TFTP command	<p>... Cisco IOS systems that use the "tftp:" (as opposed to "tftp") syntax in copy commands, select Yes.</p> <p>... Cisco IOS systems that do not use the "tftp:" (as opposed to "tftp") syntax in copy commands, select No.</p>
Use DOS style line endings	<p>... nodes that require a carriage return and line feed as an end of line marker (as opposed to just a line feed).</p>


Search Criteria	To limit search results to ...
Use interactive communication mode	<p>... Cisco IOS systems that use interactive communication mode, select Yes.</p> <p>... Cisco IOS systems that do not use interactive communication mode, select No.</p> <p>Note: In interactive communication mode, Tripwire Enterprise Console uses a more precise method to communicate with a monitored system. This mode is more robust, but communication with the system is also measurably slower.</p>
Use PASV mode for FTP transfers	<p>... network devices for which the Tripwire Enterprise Server uses passive mode (PASV) to communicate via FTP, select Yes.</p> <p>... network devices for which the TE Server does <i>not</i> use passive mode (PASV) to communicate via FTP, select No.</p>
Username	<p>... network devices for which a specific username is used for login:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial username in the text field.
Version identification method	<p>... nodes that use a specified method to determine the version of the node's monitored system.</p>
Version Pattern	<p>... custom nodes that use a specified regular expression to identify the monitored system's version number:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial version number in the text field.
VLAN	<p>... network devices that use a specific VLAN to communicate with the Tripwire Enterprise Server:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial VLAN identifier in the text field.

Searching for Elements

Notes For an introduction to common search features such as wildcards, text-field qualifiers, and saved searches, see [How Do I Run a Search? on page 232](#).







In the Element Search tab, the button bar contains many of the same buttons available in the Nodes tab. To use these buttons, refer to the procedures in [Chapter 6: Node Procedures \(on page 312\)](#).







To search for elements:

1. In the Manager bar, click **NODES**.
2. Select the **Element Search** tab.
3. Enter search criteria. For guidance, see [Table 94 on the next page](#).
 - Some of the search criteria are based on values that can be edited in element property dialogs (see [Changing the Properties of an Element on page 326](#)).
 - Unless otherwise specified in [Table 94](#), all text-field entries are case-insensitive. For example, 'File' and 'file' will return the same results.
 - Any string may be entered in a text field. For example, if you enter a string in the **Element name** field, and select **Contains** as the text-field qualifier, search results will include any element with a name that includes the string.
4. Click  **Search**

Next If desired, you can save the entered search criteria for future use. For instructions, see [Creating a Saved Search on page 234](#).

Table 94. Element search criteria

Search Criteria	To limit search results to ...
Audit event username	<p>... elements identified by Audit Event TE log messages for audit events initiated by specified users:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial user name in the text field. <p>Notes: Audit Event log messages are generated when audit events are received from an external auditing utility or an Event Generator (see What is Audit Event Collection? on page 63).</p> <p>Character strings entered with the Equals and Not Equals options are case sensitive.</p> <p>The Excludes and Contains options support the ? and * wildcard characters. The ? wildcard represents a single character, while the * wildcard represents any number of characters (including zero).</p>
Change time	<p>... elements that have changed within a specified time period:</p> <ol style="list-style-type: none"> 1. Click  Time Chooser. 2. Complete the Time Chooser dialog and click OK. <p>Tip: Click  Help for more information.</p>
Current version	<p>... elements with a specific type of current version, select an option from the list. For example, select Addition to search for elements with a current version that indicates the addition of a new monitored object.</p> <p>Tip: To select multiple options, use the standard selection convention for your operating system. For example, in Windows, hold the CTRL key while making your selections.</p>
Current version content	<p>... elements with specific content in their current version:</p> <ol style="list-style-type: none"> 1. Click  Content Criteria Chooser. 2. Complete the Current Version Content dialog and click OK. <p>Tip: Click  Help for more information.</p>
Currently checked	<p>... elements that were checked the last time TE used the element's rule to version check its node, select Yes.</p>
Element custom properties	<p>... elements that have specified values for element custom properties:</p> <ol style="list-style-type: none"> 1. Click  Custom Properties Chooser. 2. Complete the Custom Properties dialog and click OK. <p>Tip: Click  Help for more information.</p>
Element name	<p>... elements with specific names:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial element name in the text field.
Exists	<p>... elements that represent monitored objects that currently exist, select Yes.</p> <p>... elements that represent monitored objects that do not currently exist, select No.</p>


Search Criteria	To limit search results to ...
Has current policy test failures	<p>... elements that currently have at least one failed policy test result, select Yes.</p> <p>... elements that have no failed policy test results, select No.</p>
Latest version properties	<p>... elements with a current version that has specified values for version custom properties:</p> <ol style="list-style-type: none"> 1. Click  Custom Properties Chooser. 2. Complete the Custom Properties dialog and click OK. <p>Tip: Click  Help for more information.</p>
Node custom properties	<p>... elements of nodes that have specified values for node custom properties:</p> <ol style="list-style-type: none"> 1. Click  Custom Properties Chooser. 2. Complete the Custom Properties dialog and click OK. <p>Tip: Click  Help for more information.</p>
Node name	<p>... elements associated with nodes that have specific names:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial node name in the text field.
Node or node group	<p>... elements associated with a specific node or node group:</p> <ol style="list-style-type: none"> 1. Click  Chooser. 2. Select the node or group, and click OK.
Rule or rule group	<p>... elements that represent monitored objects identified by a specific rule or rule group:</p> <ol style="list-style-type: none"> 1. Click  Chooser. 2. Select the rule or group, and click OK.

Searching for Element Versions

Notes For an introduction to common search features such as wildcards, text-field qualifiers, and saved searches, see [How Do I Run a Search?](#) on page 232.







In the Version Search tab, the button bar contains many of the same buttons available in the Nodes tab. To use these buttons, refer to the procedures in [Chapter 6: Node Procedures](#) (on page 312).







To search for element versions:

1. In the Manager bar, click **NODES**.
2. Click the **Version Search** tab.
3. Enter search criteria. For guidance, see [Table 95 on the next page](#).
 - Some of the search criteria are based on values that can be edited in version property dialogs (see [Changing the Properties of an Element Version](#) on page 327).
 - Unless otherwise specified in [Table 95](#), all text-field entries are case-insensitive. For example, 'File' and 'file' will return the same results.
 - Any string may be entered in a text field. For example, if you enter a string in the **Element name** field, and select **Contains** as the text-field qualifier, search results will include any version of an element with a name that includes the string.
4. Click  **Search**.

Next If desired, you can save the entered search criteria for future use. For instructions, see [Creating a Saved Search](#) on page 234.

Table 95. Element version search criteria

Search Criteria	To limit search results to ...
Audit event username	<p>... element versions identified by Audit Event TE log messages for audit events initiated by specified users:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial user name in the text field. <p>Note: Audit Event log messages are generated when audit events are received from an external auditing utility or an Event Generator (see What is Audit Event Collection? on page 63).</p> <p>Character strings entered with the Equals and Not Equals options are case sensitive.</p> <p>The Excludes and Contains options support the ? and * wildcard characters. The ? wildcard represents a single character, while the * wildcard represents any number of characters (including zero).</p>
Change window	<p>... change versions created inside or outside of the currently defined change window, select Inside Window or Outside Window. (For more information about change windows, see How Does the Outside Change Window Action Work? on page 122.)</p>
Comment	<p>... element versions with specific user-entered comments:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial comment in the text field.
Creation time	<p>... element versions created within a specified time period:</p> <ol style="list-style-type: none"> 1. Click  Time Chooser. 2. Complete the Time Chooser dialog and click OK. <p>Tip: Click  Help for more information.</p>
Current element versions only	<p>... current versions only, select Yes.</p> <p>... all element versions, select No.</p>
Current version content	<p>... element versions with specific content:</p> <ol style="list-style-type: none"> 1. Click  Content Criteria Chooser. 2. Complete the Current Version Content dialog and click OK. <p>Tip: Click  Help for more information.</p>
Element custom properties	<p>... versions of elements that have specified values for element custom properties:</p> <ol style="list-style-type: none"> 1. Click  Custom Properties Chooser. 2. Complete the Custom Properties dialog and click OK. <p>Tip: Click  Help for more information.</p>
Element name	<p>... versions associated with elements that have specific names:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial element name in the text field.

Search Criteria	To limit search results to ...
Exists	<p>... element versions that represent monitored objects that exist, select Yes.</p> <p>... element versions that represent monitored objects that do not exist, select No.</p>
Has audit events	<p>... element versions currently identified by one or more Audit Event TE log messages, select Yes.</p> <p>... element versions that are not currently associated with any Audit Event TE log messages, select No.</p> <p>Note: Audit Event log messages are generated when audit events are received from an external auditing utility or an Event Generator (see What is Audit Event Collection? on page 63).</p>
Has current policy test failures	<p>... elements with a current version that has at least one failed policy test result, select Yes.</p> <p>... elements with a current version that has no failed policy test results, select No.</p>
Has promotion approval identity	<p>... element versions that have an associated promotion approval ID number, select Yes.</p> <p>... element versions lacking an associated promotion approval ID number, select No.</p>
Node custom properties	<p>... element versions of nodes that have specified values for node custom properties:</p> <ol style="list-style-type: none"> 1. Click  Custom Properties Chooser. 2. Complete the Custom Properties dialog and click OK. <p>Tip: Click  Help for more information.</p>
Node name	<p>... element versions associated with nodes that have specific names:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial node name in the text field.
Node or node group	<p>... element versions of a specific node or node group:</p> <ol style="list-style-type: none"> 1. Click  Chooser. 2. Select the node or group, and click OK.
Promotion approval identity	<p>... element versions with specific promotion approval ID values:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial ID number in the text field.
Rule or rule group	<p>... element versions that represent monitored objects identified by a specific rule or rule group:</p> <ol style="list-style-type: none"> 1. Click  Chooser. 2. Select the rule or group, and click OK.
Version custom properties	<p>... element versions that have specified values for version custom properties:</p> <ol style="list-style-type: none"> 1. Click  Custom Properties Chooser. 2. Complete the Custom Properties dialog and click OK. <p>Tip: Click  Help for more information.</p>


Search Criteria	To limit search results to ...
Version type	... element versions of a specific type, select an option from the list. For example, select Modification to search for change versions that indicate a modification made to a monitored object. Tip: To select multiple options, use the standard selection convention for your operating system. For example, in Windows, hold the CTRL key while making your selections.

Creating and Deleting Objects in the Node Manager

Creating a Node Group

In addition to regular groups in the Node Manager, you can also create smart node groups, which reflect tags and other elements in the Asset View tab. For more information, see [About Node Groups and Smart Node Groups on page 57](#). For information on regular node groups, see [About Groups on page 29](#).

To create a node group:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the node group in which to create the new node group.
3. Click **Manage** >  **New Group**.
4. In the New Node Group Wizard, enter a **Name** and **Description** (optional) for the new node group.
5. Click **Finish**.


Next To add existing nodes to a node group, see:


- [Moving Nodes and Node Groups \(on page 379\)](#)
- [Linking Nodes and Node Groups \(on page 380\)](#)

Creating a Custom Node

Note To create a custom node, you must first create a custom type for the node (see [Working with Custom Node Types on page 299](#)).

To create a custom node:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the node group in which the new node will be created.
3. Click **Manage** >  **New Node**.
4. In the Create Node dialog, select a custom-node type in the **Network Device** > **Custom** folder and click **OK**.
5. Complete the New Node Wizard.

Tip For further instructions, click  **Help** in any wizard page.

Creating a Directory Server Node

For an introduction to directory server nodes, see *What are Node Types?* on page 51.

For a list of LDAP directory products officially supported by Tripwire Enterprise, see the following URL:


<https://www.tripwire.com/products/tripwire-enterprise/tripwire-enterprise-platform-and-device-support-register>


Note To monitor a directory node you must specify a **delegated Agent**, a system with Tripwire Enterprise Agent software installed that processes some Tripwire Enterprise functions for the directory node.

Tripwire strongly recommends that you install TE Agent on the directory server, and use that Agent both to monitor the server's file system, and as the delegated Agent used to monitor the directory itself.

Before completing the process below, make sure that TE Agent is installed on the directory server that you want to monitor. Nodes with Axon Agent installed cannot be used as a delegated Agent.

To create a directory server node:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the node group in which the new node will be created.
3. Click **Manage** >  **New Node**.
4. In the Create Node dialog, select a node type in the **Directory Server** folder and click **OK**.
5. Complete the New Node Wizard.

Tip For further instructions, click  **Help** in any wizard page.

Creating a Database Node


For an introduction to database nodes, see [What are Node Types?](#) on page 51.


Note To monitor a database node you must specify a **delegated Agent**, a system with Tripwire Enterprise Agent software installed that processes some Tripwire Enterprise functions for the database node.

Tripwire strongly recommends that you install TE Agent on the database server, and use that Agent both to monitor the server's file system, and as the delegated Agent used to monitor the database itself.

Before completing the process below, make sure that TE Agent is installed on the database server that you want to monitor. Nodes with Axon Agent installed cannot be used as a delegated Agent.

To create a database node:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the node group in which the new node will be created.
3. Click **Manage** >  **New Node**.
4. In the Create Node dialog, select a node type in the **Database Server** folder and click **OK**.
5. Complete the New Node Wizard.

Tips For further details, click  **Help** in any wizard page.

Select the **Collect audit-event information** check box to save audit events (if available) in new element versions. For more information on the source for audit events, see [Table 96 on the next page](#). Tripwire Enterprise does not collect audit events on PostgreSQL databases.

Next In the New Node Wizard, you specified a database user account. When Tripwire Enterprise attempts to access the database server, the server will authenticate the application with the credentials of the user account. However, to successfully baseline and version check the database server, you must first grant appropriate permissions to the user account. For instructions, see [Configuring a Database User Account \(or Login\)](#) on the next page.

Table 96. Audit event sources for monitored databases

Database type	Audit Event Source
DB2	One of the following sources: <ul style="list-style-type: none">• the AUDIT.OBJMAINT table• the AUDIT.SECMAINT table
Microsoft SQL Server	One of the following sources: <ul style="list-style-type: none">• a security event log (on Windows systems)• an audit log (on UNIX systems)• a database audit log
Oracle	One of the following sources: <ul style="list-style-type: none">• a security event log (on Windows systems)• an audit log (on UNIX systems)• a database audit log <p>Note: If the fine-grained auditing feature is enabled for a monitored Oracle database, Tripwire Enterprise will not collect events identified by fine-grained auditing.</p>
PostgreSQL	Tripwire Enterprise does not monitor audit events on PostgreSQL databases.

Configuring a Database User Account (or Login)

To successfully monitor a database, you must configure the database user account (or login) that is assigned to the database's node.

For a Microsoft SQL Server 2008 or 2012 database server, complete the following steps in the login's properties dialog.

1. On the User Mapping page:
 - Select each database to be monitored by TE.
 - Select **db_datareader** from the list of database roles.
2. On the Securables page:
 - a. Click **Search** to add the database server.
 - b. If you want to enable audit event collection on the database node, the user account needs to have the **alter trace** permissions for the database server.
 - c. If you want to monitor all logins, add the **View any definition** permission.

For an Oracle database server, enter the following SQL statement at a command prompt:

```
GRANT CREATE SESSION, SELECT ANY TABLE, SELECT ANY DICTIONARY TO <username>;  
where <username> is the name of the Oracle user account.
```

Note For some database query rules, additional privileges may be required. For example, if an Oracle query rule calls for a user-defined function, then the EXECUTE ANY PROCEDURE privilege must be granted to the Oracle user account.

For a DB2 database server, complete the following steps in a command editor:

1. Enter the following command:

```
GRANT CONNECT ON DATABASE TO USER <user_account_name>;
```

2. With the following format, enter a command for each of the privileges listed below.

```
GRANT SELECT ON <privilege> TO USER <user_account_name>;
```

Privileges:

AUDIT.OBJMAINT	SYSCAT.INDEXEXTENSIONMETHODS
AUDIT.SECMAINT	SYSCAT.KEYCOLUSE
SYSCAT.ATTRIBUTES	SYSCAT.LIBRARYAUTH
SYSCAT.AUDITPOLICIES	SYSCAT.PACKAGEAUTH
SYSCAT.BUFFERPOOLS	SYSCAT.PACKAGES
SYSCAT.CHECKS	SYSCAT.PASSTHROUGH
SYSCAT.COLAUTH	SYSCAT.PREDICATESPECS
SYSCAT.COLCHECKS	SYSCAT.PROCEDURES
SYSCAT.COLIDENTATTRIBUTES	SYSCAT.PROCPARMS
SYSCAT.COLUMNS	SYSCAT.REFERENCES
SYSCAT.COLUSE	SYSCAT.ROUTINEAUTH
SYSCAT.DATATYPES	SYSCAT.ROUTINES
SYSCAT.DBAUTH	SYSCAT.SCHEMAAUTH
SYSCAT.DBPARTITIONGROUPDEF	SYSCAT.SCHEMATA
SYSCAT.DBPARTITIONGROUPS	SYSCAT.SEQUENCEAUTH
SYSCAT.EVENTMONITORS	SYSCAT.SEQUENCES
SYSCAT.EVENTS	SYSCAT.TABAUTH
SYSCAT.EVENTTABLES	SYSCAT.TABCONST
SYSCAT.FUNCPARMS	SYSCAT.TABLES
SYSCAT.FUNCTIONS	SYSCAT.TABLESPACES
SYSCAT.HIERARCHIES	SYSCAT.TBSPACEAUTH
SYSCAT.INDEXAUTH	SYSCAT.TRIGGERS
SYSCAT.INDEXCOLUSE	SYSCAT.VIEWS
SYSCAT.INDEXES	SYSIBM.SYSDUMMY1
SYSCAT.INDEXEXPLOITRULES	

3. Enter a command for each of the following privileges using the format specified in [step 2 on the previous page](#).

SYSCAT.DATAPARTITIONEXPRESSION	SYSCAT.VARIABLEAUTH
SYSCAT.DATAPARTITIONS	SYSCAT.VARIABLES
SYSCAT.HISTOGRAMTEMPLATEBINS	SYSCAT.WORKACTIONS
SYSCAT.HISTOGRAMTEMPLATES	SYSCAT.WORKACTIONSETS
SYSCAT.HISTOGRAMTEMPLATEUSE	SYSCAT.WORKCLASSES
SYSCAT.INDEXXMLPATTERNS	SYSCAT.WORKCLASSSETS
SYSCAT.NICKNAMES	SYSCAT.WORKLOADAUTH
SYSCAT.ROLEAUTH	SYSCAT.WORKLOADCONNATTR
SYSCAT.ROLES	SYSCAT.WORKLOADS
SYSCAT.SECURITYLABELCOMPONENTELEMENTS	SYSCAT.XSROBJECTAUTH
SYSCAT.SECURITYLABELCOMPONENTS	SYSIBMADM.DBCFG
SYSCAT.SECURITYPOLICIES	SYSIBMADM.DBMCFG
SYSCAT.SERVICECLASSES	SYSIBMADM.SNAPCONTAINER
SYSCAT.THRESHOLDS	SYSIBMADM.SNAPTbsp
	SYSIBMADM.SNAPTbsp_PART

For a PostgreSQL database server, enter the following SQL statements at a command prompt:

```
CREATE USER <username> WITH LOGIN NOSUPERUSER NOINHERIT NOCREATEDB
NOCREATEROLE NOREPLICATION CONNECTION LIMIT 30;

GRANT SELECT ON ALL TABLES IN SCHEMA pg_catalog TO <username>;

GRANT EXECUTE ON FUNCTION pg_catalog.pg_get_functiondef(oid) TO <username>;

GRANT EXECUTE ON FUNCTION pg_catalog.pg_get_function_identity_arguments(oid)
TO <username>;
```


where <username> is the name of the PostgreSQL user account.


The permissions above will enable the specified user to monitor PostgreSQL database objects with database metadata rules. To monitor specific objects with database query rules, the user account must also have SELECT permission on the database objects that are to be monitored.

Creating a Network Device Node

For an introduction to network device nodes, see [What are Node Types?](#) on page 51.

To create a network device node:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the node group in which the new node will be created.
3. Click **Manage** >  **New Node**.
4. In the Create Node dialog, select a node type in the **Network Device** folder and click **OK**.
5. Complete the New Node Wizard.

Tip For further instructions, click  **Help** in any wizard page.

Creating a VI Management Node

For an introduction to VI management nodes, see [Monitoring Virtual Systems with Tripwire Enterprise \(on page 59\)](#)


Notes You can create no more than one VI management node for a single host system.


To monitor a VI management node you must specify a **delegated Agent**, a system with Tripwire Enterprise Agent software installed that processes some Tripwire Enterprise functions for the VI management node.

Tripwire strongly recommends that you install TE Agent on the VI management server, and use that Agent both to monitor the server's file system, and as the delegated Agent used to monitor the VI manager itself.

Before completing the process below, make sure that TE Agent is installed on the VI management server that you want to monitor. Nodes with Axon Agent installed cannot be a used as a delegated Agent.

To create a VI management node:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the node group in which the new node will be created.
3. Click **Manage** >  **New Node**.
4. In the Create Node dialog, select a type of VI management node (for example, VMware vCenter) from the **Virtual Infrastructure** folder and click **OK**.
5. Complete the New Node Wizard.

Tips For further instructions, click  **Help** in any wizard page.


In the New Node Wizard, you can create a new check rule task for the VI management node. If you do so, TE will add the new task to the Task Manager. For more information, see [About Version Checks on page 44](#).

Duplicating Nodes

With this procedure, you can either duplicate specified nodes in a selected node group, or all nodes in a selected node group.

Note VI nodes descended from a VI management node cannot be duplicated.

To create copies of existing nodes:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the node group containing the nodes to be duplicated.
3. (Optional) To duplicate specific nodes, select the check box of each node.
4. Click **Manage** >  **Duplicate**.
5. Click **OK** in the confirmation dialog.

Deleting Nodes and Node Groups

This procedure permanently deletes all instances of selected nodes and/or node groups. To remove an instance of a node or node group from another node group *without* deletion, see [Unlinking Nodes and Node Groups on page 381](#).

If you delete a node group, the nodes within the group are *not* deleted from the system. If the deleted group contains the only instance of an Agent node, TE moves the node to the **Discovered** group. If the group contains the only instance of a non-Agent node, TE moves the node to the **Unlinked** folder.

Tips To delete an object, your user account must have Delete permissions for that object, and (for groups) all objects descended from that object. For more information, see [What are User Permissions and User Roles? on page 204](#).

VI nodes and node groups descended from a VI management node cannot be deleted. You can only delete a smart node group by deleting the corresponding tag set or saved filter in the Asset View tab. For more information, see [Working with Tags and Tag Sets \(on page 352\)](#) and [Working with Saved Filters \(on page 353\)](#)

This procedure explains how to delete node groups displayed in the main pane of the Nodes tab in the Node Manager. However, you can also delete node groups in:

- The **Parent Groups** tab of a node properties dialog (see [Changing the Properties of a Node on page 321](#))
- The **Parent Groups** tab of a node group properties dialog (see [Changing the Properties of a Node Group on page 325](#))
- The **Node Search** tab of the Node Manager (see [Searching for Nodes on page 355](#))

To delete nodes and/or node groups:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the node group containing the objects to be deleted.
3. In the main pane, select the check box for each object to be deleted.
4. Click **Manage > X Delete**.
5. Specify whether or not to run the Clear Unlinked Groups task on all Unlinked groups in TE. For more information on this task, see [What are Task Types? on page 127](#).
6. Click **OK**.

Note If you get an error message when trying to delete objects, an access control (see [What are Access Controls? on page 208](#)) is preventing you from deleting a descendant object. To determine which objects have access controls, check the Objects tab for the Error log message associated with this operation.

Deleting Elements

Tip This procedure explains how to delete elements displayed in the main pane of the Nodes tab in the Node Manager. However, you can also delete elements in:

- The **Elements** tab of a node properties dialog (see [Changing the Properties of a Node on page 321](#))
- The **Element Search** tab of the Node Manager (see [Searching for Elements on page 361](#))

To delete elements:

1. In the Manager bar, click **NODES**.
2. In the tree pane, select the elements' node.

Note If Detailed Node View is enabled, you must select the elements' rule under the node in the tree pane. To enable or disable Detailed Node View, see [Changing User Preference Settings on page 262](#).

3. In the main pane, select the check box of each element to be deleted.
4. Click **✖ Delete**.
5. Click **OK** to confirm.

Moving, Linking, and Unlinking Objects in the Node Manager

Moving Nodes and Node Groups

With this procedure, you can move a node (or node group) from one node group to another. For example, you can move a node from the **Unlinked** group to another node group.

Notes


VI nodes and node groups descended from a VI management node cannot be moved.

Smart node groups cannot be moved, and you can't move nodes into a smart node group. To add a node to a smart node group, you must change the tags associated with the node in the Asset View tab. For more information, see [Using the Asset View Tab on page 346](#).

If you move a node (or node group) to a node group that is currently associated with a check rule task, you may need to initialize new baselines for the task. For instructions, see [Creating Current Baselines for a Check Rule Task on page 522](#).

If you move a node (or node group) from a node group associated with a rule task to another group that is unrelated to the task, the rule task will no longer run on the moved object.

To move nodes and node groups:


1. In the Manager bar, click **NODES**.
2. In the tree pane, click the group containing the objects to be moved.
3. In the main pane, select the check box of each node (or node group) to be moved.
4. Click **Manage** >  **Move**.
5. In the Move Nodes dialog, select the destination node group and click **OK**.


Linking Nodes and Node Groups

When you create a node or node group, the object is linked to the node group in which it was created. As needed, the object may also be linked to other node groups. For more information, see [What are Links and Linked Objects?](#) on page 213.

Notes	<p>Smart node groups cannot be linked to any other group. For more information, see About Node Groups and Smart Node Groups on page 57.</p> <p>If you link a node in the Discovered or Unlinked node groups, Tripwire Enterprise <i>moves</i> the node to the destination node group.</p> <p>This procedure explains how to link nodes and node groups displayed in the main pane of the Nodes tab in the Node Manager. However, you can also link:</p> <ul style="list-style-type: none">• Nodes in the Report Viewer for some reports (see Running a Report Manually on page 601)• Nodes in the Node Search tab of the Node Manager (see Searching for Nodes on page 355)• Node groups in the Parent Groups tab of a node properties dialog (see Changing the Properties of a Node on page 321)• Node groups in the Parent Groups tab of a node group properties dialog (see Changing the Properties of a Node Group on page 325)
--------------	--

To link nodes and node groups to another node group:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the group containing the objects to be linked.
3. Select the check box of each node (or node group) to be linked.
4. Click **Manage** >  **Link**.
5. Select the destination node group and click **OK**.

Note	In the Node Manager, a link  emblem overlays the icon of each node or node group that is currently linked to more than one node group.
-------------	---

Unlinking Nodes and Node Groups

This procedure unlinks a node (or node group) from a node group. For more information, see [What are Links and Linked Objects? on page 213](#).

If you unlink a **file server node** from the only node group with which it is linked, Tripwire Enterprise moves the node to the **Discovered** node group. If you unlink **any other node** from the only node group with which it is linked, Tripwire Enterprise moves the node to the **Unlinked** node group. To retrieve a node or node group from the **Unlinked** or **Discovered** groups, see [Moving Nodes and Node Groups on page 379](#).


Notes To unlink an object, your user account must have Delete and Link permissions for that object, and (for groups) all objects descended from that object. For more information, see [What are User Permissions and User Roles? on page 204](#).

Smart node groups cannot be unlinked from any other group. For more information, see [About Node Groups and Smart Node Groups on page 57](#).

VI nodes and node groups descended from a VI management node cannot be unlinked.

This procedure explains how to unlink nodes and node groups displayed in the main pane of the Node Manager. However, in the properties dialog of a node (or node group), you can unlink the node (or node group) from any node group displayed in the **Parent Groups** tab. For more information, see [Changing the Properties of a Node \(on page 321\)](#) and [Changing the Properties of a Node Group \(on page 325\)](#).

To unlink a node or node group:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the group containing the node or node group to be unlinked.
3. In the main pane, select the check box for each node or node group to be unlinked.
4. Click **Manage** >  **Unlink**.
5. Specify whether or not to run the Clear Unlinked Groups task on all Unlinked groups in TE. For more information on this task, see [What are Task Types? on page 127](#).
6. Click **OK**.

Note If you get an error message when trying to unlink objects, an access control (see [What are Access Controls? on page 208](#)) is preventing you from unlinking a descendant object. To determine which objects have access controls, check the Objects tab for the Error log message associated with this operation.

Baselining and Version Checking Monitored Objects

Initial Baselining of Monitored Objects

To monitor a system for change, you must first create current baselines for the objects to be monitored. To do so, you baseline the system with a rule or rule group. The selected rules identify the monitored objects for which current baselines will be created (see [About Baselines on page 43](#)).

With this procedure, you can either:

- Baseline monitored systems with a rule or rule group for the first time.
- Baseline monitored systems with a rule or rule group that was previously used to baseline the systems. In this case, Tripwire Enterprise creates a current baseline for each monitored object created since the rule or rule group was last run. In addition, you have the option of re-baselining the monitored objects that were previously baselined with the rule or rule group.


To baseline monitored objects, your account must have the **Use Rules** and **Update Elements** permissions. By default, only Administrators and Power Users have these permissions. For more information, see [What are User Permissions and User Roles? on page 204](#).

Caution You should only baseline monitored objects that are in a known-good state.

Tip This procedure explains how to baseline nodes and node groups displayed in the main pane of the Nodes tab of the Node Manager. However, you can also baseline:

- Nodes in the **Node Search** tab of the Node Manager (see [Searching for Nodes on page 355](#))
- Node groups in the **Parent Groups** tab of a node properties dialog (see [Changing the Properties of a Node on page 321](#))
- Node groups in the **Parent Groups** tab of a node group properties dialog (see [Changing the Properties of a Node Group on page 325](#))

To create initial baselines for monitored objects:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the group containing the node or node group for the monitored system(s) to be baselined.
3. In the main pane, select the check box of each node or node group to be baselined.
4. Click **Control** >  **Baseline**.
5. In the Baseline dialog:

- a. Select **Selected nodes with rule or rule group**.
- b. From the rule menu, select the rule or rule group with which to baseline the selected nodes.
- c. (Optional) To create new baseline versions for all elements, select **All elements** in the **Create baselines for** section of the dialog.

Note When baselining monitored systems with a rule or rule group for the first time, the setting in the **Create baselines for** section has no effect.

6. Click **OK**.

Re-baselining Monitored Systems


With this procedure, you can re-baseline monitored objects on one or more systems with the rule or rule group that was originally used to generate the baselines. For more information, see [About Baselines on page 43](#).

To baseline monitored objects, your account must have the **Create Rules** and **Update Elements** permissions. By default, only Administrators and Power Users have these permissions. For more information, see [What are User Permissions and User Roles? \(on page 204\)](#).

Tip This procedure explains how to baseline nodes and node groups displayed in the main pane of the Nodes tab of the Node Manager. However, you can also baseline:

- Nodes in the Report Viewer for some reports (see [Running a Report Manually on page 601](#))
- Nodes in the **Node Search** tab of the Node Manager (see [Searching for Nodes on page 355](#))
- Node groups in the **Parent Groups** tab of a node properties dialog (see [Changing the Properties of a Node on page 321](#))
- Node groups in the **Parent Groups** tab of a node group properties dialog (see [Changing the Properties of a Node Group on page 325](#))

To re-baseline monitored objects for one or more systems:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the group containing the node or node group for the monitored system(s) to be re-baselined.
3. In the main pane, select the check box of each node or node group.
4. Click **Control** >  **Baseline**.

5. In the Baseline dialog, select **Selected nodes with currently associated rules**. With this option, Tripwire Enterprise re-baselines the specified monitored systems with all rules (and rule groups) previously used to generate baselines.

Note This option is only available if at least one element exists for the selected systems.

6. Select the **New elements only** in the **Create baselines for** section of the Baseline dialog.
7. Click **OK**.

Re-baselining Specific Monitored Objects

With this procedure, you can re-baseline specific monitored objects on a single system. For more information, see [About Baselines on page 43](#). To baseline monitored objects for the first time, see [Initial Baseline of Monitored Objects \(on page 382\)](#).

Tip This procedure explains how to baseline elements displayed in the main pane of the Nodes tab of the Node Manager. However, you can also baseline elements in:

- The **Elements** tab of a node properties dialog (see [Changing the Properties of a Node on page 321](#))
- The **Element Search** tab of the Node Manager (see [Searching for Elements on page 361](#))
- The **Version Search** tab of the Node Manager (see [Searching for Element Versions on page 364](#))


To baseline specific objects on a single monitored system:

1. In the Manager bar, click **NODES**.
2. In the tree pane, select the node for the monitored system.

Note If Detailed Node View is enabled, you must also select a rule in the tree pane. To enable or disable Detailed Node View, see [Changing User Preference Settings on page 262](#).

3. The main pane displays an element for each monitored object that has been baselined. Select the check box of each element to be re-baselined.

Caution If you do **not** select a check box, Tripwire Enterprise will re-baseline all of the node's elements.

4. Click **Control** >  **Baseline**.
5. In the Baseline dialog, **Baseline selected elements** is selected by default. Click **OK**.

Version Checking Monitored Systems


With this procedure, you can version check monitored objects for one or more monitored systems. For an introduction to version checking, see [About Version Checks on page 44](#).

To version check specific monitored objects for a single system, see [Version Checking Specific Monitored Objects on the next page](#).

Tip This procedure explains how to version check nodes and node groups displayed in the main pane of the Nodes tab of the Node Manager. However, you can also check:

- Nodes in the Report Viewer for some reports (see [Running a Report Manually on page 601](#))
- Nodes in the **Node Search** tab of the Node Manager (see [Searching for Nodes on page 355](#))
- Node groups in the **Parent Groups** tab of a node or node group properties dialog (see [Changing the Properties of a Node on page 321](#) and [Changing the Properties of a Node Group on page 325](#))

To run a version check of one or more monitored systems:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the group containing the node or node group for the monitored system(s) to be checked.
3. In the main pane, select the check box for each node or node group to be checked.
4. Click **Control** >  **Check**.
5. In the Check for Changes dialog, specify the rules to be used in the version check.
 - **Selected nodes with currently associated rules.** With this option, Tripwire Enterprise checks the selected systems with all rules (and rule groups) used to baseline the systems. In this case, Tripwire Enterprise checks each monitored object with the rule used to baseline the object.

Note This option is only available if at least one element exists for the selected systems.

- **Selected nodes with rule or rule group.** With this option, you specify a rule or rule group to check the selected systems. In this case, Tripwire Enterprise only checks monitored objects that were baselined with one of the selected rules.
6. Click **OK**.

Next If the version check resulted in the creation of a new change version(s), you can compare the new version with the current baseline to determine if the version should be promoted. For instructions, see [Comparing a Current Change Version with the Current Baseline on page 388](#).

Version Checking Specific Monitored Objects

With this procedure, you can run a version check of specific elements associated with a single monitored system. For more information, see [About Version Checks on page 44](#).

To version check multiple systems for changes, see [Version Checking Monitored Systems on the previous page](#).

Note Axon Agents do not support running version checks on specific elements. Instead, the whole rule used to monitor the element should be re-run.


Tip This procedure explains how to version check elements displayed in the main pane of the Nodes tab of the Node Manager. However, you can also check elements in:

- The **Elements** tab of a node properties dialog (see [Changing the Properties of a Node on page 321](#))
- The **Element Search** tab of the Node Manager (see [Searching for Elements on page 361](#))
- The **Version Search** tab of the Node Manager (see [Searching for Element Versions on page 364](#))

To version check specific elements for a single system:

1. In the Manager bar, click **NODES**.
2. In the tree pane, select the node for the monitored system.

Note If Detailed Node View is enabled, you must also select a rule in the tree pane. To enable or disable Detailed Node View, see [Changing User Preference Settings on page 262](#).

3. The main pane displays an element for each monitored object that has been baselined. Select the check box of each element to be version checked.
4. Click **Control** >  **Check**.
5. In the Check for Changes dialog, **Perform check on selected elements** is selected by default.
6. Click **OK**.

Next If the version check created a new change version, you can compare the new version with the current baseline to determine if the version should be promoted. For instructions, see [Comparing a Current Change Version with the Current Baseline on page 388](#).

Temporarily Disabling Checks and Baselines on a Node

Sometimes you may want to temporarily suspend version checks or baselines for a node without affecting the other nodes in the group. For example, if you take a system offline for maintenance, you should first disable that node to prevent TE from reporting a connection error.

When you disable a node,

- checks and baseline operations for the node are suspended until you re-enable the node.
- TE displays (disabled) after the name of each unlicensed node in the Node Manager.
- The Status:Monitoring Disabled system tag is applied to the node. For more information, see [Working with Tags and Tag Sets on page 352](#).

Tip If smart node groups are enabled, you can see all currently disabled nodes in:

**Root Node Group > Smart Node Groups > System Tag Sets > Status
> Monitoring Disabled**

For more information, see [About Node Groups and Smart Node Groups on page 57](#).


To temporarily disable or enable checks and baselines in the Asset View tab:

1. (Optional) Use the Asset Filter pane to refine the list of assets in the Asset List.

To disable or enable a single asset, select it in the Asset List and click **Disable** or **Enable** in the right-hand Selection Information pane.

To disable or enable multiple assets:

- a. In the Asset List, click the checkbox for each asset to add it to the list in the Selection Information pane.
- b. Click **Health Check** at the top of the list.
- c. Select **Enable Assets** or **Disable Assets** from the dropdown menu.

Tip You can also disable or enable checks and baselines from the Nodes tab of the Node Manager. Select the appropriate nodes or node groups in the main pane, then click **Modify** >  **Status**.

Comparing Element Versions

Comparing a Current Change Version with the Current Baseline

If the current version of an element is a change version, you can use the Difference Viewer to compare the current version with the element's current baseline. This is when determining the appropriate response to a detected change.

Notes To use the Difference Viewer to evaluate changes on a node, a Change Audit license must be installed on that node. For more information, see [About Tripwire Enterprise Licenses on page 202](#).

You can also access the Difference Viewer from:

- The **Elements** tab of a node properties dialog (see [Changing the Properties of a Node on page 321](#))
- The **Element Search** tab of the Node Manager ([Searching for Elements on page 361](#))

To compare an element's current baseline with the latest change version:

1. In the Manager bar, click **NODES**.
2. In the tree pane, select the element's node.

Note If Detailed Node View is enabled, you must also select a rule in the tree pane. To enable or disable Detailed Node View, see [Changing User Preference Settings on page 262](#).

3. In the main pane, select the **Version Type** link for the element. (If the element does not have a Version Type link, the element's current version is the current baseline.)
4. In the Difference Viewer, compare the change version with the current baseline.
 - The **Content** tab shows changes in the monitored object's content (if applicable).
 - The **Attributes** tab shows changes in the monitored object's attributes.

Tip For more information, click  **Help**.

5. Click **Close**.

Next If you approve of the changes reflected in the change version, you can promote the change version to the baseline. For instructions, see [Promoting a Specific Element Version on page 393](#).

If you do not approve of the change version, and the element represents a file on a network device, you may be able to restore the file to its baseline state. For instructions, see [Restoring a Changed File with the Run Actions Feature on page 404](#).

Comparing an Element Version with the Current Baseline


Notes To use the Difference Viewer to evaluate changes on a node, a Change Audit license must be installed on that node. For more information, see [About Tripwire Enterprise Licenses on page 202](#).

You can also compare versions of an element in the **Elements** tab of a node properties dialog (see [Changing the Properties of a Node on page 321](#)).

To compare an element's current baseline with another version of the element:

1. In the Manager bar, click **NODES**.
2. In the tree pane, select the element's node.

Note If Detailed Node View is enabled, you must also select a rule in the tree pane. To enable or disable Detailed Node View, see [Changing User Preference Settings on page 262](#).

3. In the main pane, click the element in the **Element** column.
4. In the element properties dialog, select the **History** tab.
5. Select the check box for the element version to be compared with the current baseline.
6. Click  **Differences**.
7. In the Difference Viewer, compare the element version with the current baseline.
 - The **Content** tab shows the differences in the monitored object's content (if applicable).
 - The **Attributes** tab shows the differences in the monitored object's attributes.

Tip For more information, click  **Help**.

8. Click **Close**.

Next If you approve of the element version's content and attributes, you can promote the version to the baseline. For instructions, see [Promoting a Specific Element Version on page 393](#).


Comparing Any Two Versions of the Same Element

Note To use the Difference Viewer to evaluate changes on a node, a Change Audit license must be installed on that node. For more information, see [About Tripwire Enterprise Licenses on page 202](#).

To compare any two versions of the same element:

1. In the Manager bar, click **NODES**.
2. In the tree pane, select the element's node.

Note If Detailed Node View is enabled, you must also select a rule in the tree pane. To enable or disable Detailed Node View, see [Changing User Preference Settings on page 262](#).

3. In the main pane, click the element in the **Element** column.
4. In the element properties dialog, select the **History** tab.
5. Select the check boxes of the two element versions to be compared.
6. Click  **Differences**.
7. Compare the two element versions in the Difference Viewer.

Tip For more information, click  **Help**.

8. Click **Close**.

Comparing Any Two Versions of Different Elements

This procedure compares a version of one element with a version of another element. The first element version selected is known as the **base version**, while the second version is the **compare version**.


To specify a new base version, existing selections must first be cleared. For instructions, see [Clearing Mark for Compare Selections on the next page](#).

Note To use the Difference Viewer to evaluate changes on a node, a Change Audit license must be installed on that node. For more information, see [About Tripwire Enterprise Licenses on page 202](#).

To compare two versions for different elements:

1. In the Manager bar, click **NODES**.
2. In the tree pane, select the base version's node.

Note If Detailed Node View is enabled, you must also select a rule in the tree pane. To enable or disable Detailed Node View, see [Changing User Preference Settings on page 262](#).

3. In the main pane, click the element in the **Element** column.
4. In the element properties dialog, select the **History** tab.
5. Select the check box for the base version.
6. Click  **Mark for Compare**.
7. In the Versions to Compare dialog, verify that your selection is now marked as the **base version**. Also, the **Compare Version** region should indicate that the second element version has yet to be selected.
8. Close all open dialogs, and specify the compare version by repeating the steps above.
9. In the Versions to Compare dialog, verify that the second selection is now marked as the **compare version**.

Note Your selection will remain as the compare version until you select another element version by repeating steps 2-7.

10. Click **View**. The Difference Viewer opens.
 - If the two element versions are identical, a message states **No differences found**.
 - If the two element versions differ, the differences are highlighted in gray and color-coded by type.

Tip For more information, click  **Help**.

Clearing Mark for Compare Selections


Comparing Any Two Versions of Different Elements (on the previous page) outlines the process for comparing any two versions of different elements. In that procedure, you designate one element version as the **base version**, while the second version is the **compare version**. With this procedure, you can erase the current settings for the base and compare versions.

Note To use the Difference Viewer to evaluate changes on a node, a Change Audit license must be installed on that node. For more information, see *About Tripwire Enterprise Licenses* on page 202.

To clear the current mark for compare selections:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click any node.

Note If Detailed Node View is enabled, you must also select a rule in the tree pane. To enable or disable Detailed Node View, see *Changing User Preference Settings* on page 262.

3. In the main pane, click any element in the **Element** column.
4. In the element properties dialog, select the **History** tab.
5. Select the check box for any element version.
6. Click  **Mark for Compare**.
7. Click **Clear**, then click **Cancel**.

Next To compare a new base version with another element version, see *Comparing Any Two Versions of Different Elements* (on the previous page).

Promoting Element Versions

Promoting a Specific Element Version

This procedure promotes a single element version to the baseline.

- For an introduction to promotion, see [What is Promotion? on page 47](#).
- To promote an element version, the Update Elements permission must be assigned to your user account (see [What are User Permissions and User Roles? on page 204](#)).
- To promote all current versions associated with a node or node group, see [Promoting All Current Versions for a Node or Node Group on page 395](#).


Tip In this procedure, you promote a version of an element displayed in the main pane of the Node Manager. However, you can also promote a version of an element in:

- The **Elements** tab of a node properties dialog (see [Changing the Properties of a Node on page 321](#))
- The **Element Search** tab of the Node Manager ([Searching for Elements on page 361](#))


To promote a single element version:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the element's node.


Note If Detailed Node View is enabled, you must also select a rule in the tree pane. To enable or disable Detailed Node View, see [Changing User Preference Settings on page 262](#).


3. The main pane displays all of the node's elements. In the **Current Version** column:
 - The baseline icon  indicates that an element's current baseline is the current version.
 - A severity indicator indicates that an element's current version is a change version (known as a *current change version*). (For descriptions of severity indicators, see [What are Severity Ranges? on page 114](#).)

To promote a current change version:

- a. Select the element's check box.
- b. Click **Control** >  **Promote**.

To promote an element version other than the current version:

- a. In the **Element** column, click the element.
 - b. In the element properties dialog, select the **History** tab.
 - c. Select the check box for the element version to be promoted.
 - d. Click  **Promote**.
4. In the Promote Wizard, accept the default setting (**Promote selected versions**) and click **Next**.
 5. Complete the remaining wizard pages.

Tip For further instructions, click  **Help** in any wizard page.

Promoting All Current Versions for a Node or Node Group

This procedure promotes all current versions associated with one or more specified nodes. However, if the latest version of an element is a current baseline, no action is taken for the element.

- For an introduction to promotion, see [What is Promotion? on page 47](#).
- To promote an element version, the Update Elements permission must be assigned to your user account (see [What are User Permissions and User Roles? on page 204](#)).
- To promote a specific element version, see [Promoting a Specific Element Version on page 393](#).


Tip In this procedure, you can promote all current versions for a node group displayed in the main pane of the Nodes tab of the Node Manager. However, you can also do this with:


- Nodes in the **Report Viewer** for some reports (see [Running a Report Manually on page 601](#))
- Nodes in the **Node Search** tab of the Node Manager (see [Searching for Nodes on page 355](#))
- Node groups in the **Parent Groups** tab of a node properties dialog (see [Changing the Properties of a Node on page 321](#)) or node group properties dialog (see [Changing the Properties of a Node Group on page 325](#))

To promote all current versions for one or more nodes:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the group containing the node(s) and/or node group(s) to be promoted.
3. In the main pane, select the check box of each node or node group to be promoted.

Note Only nodes and node groups marked with a severity indicator may be promoted. For descriptions of severity indicators, see [What are Severity Ranges? on page 114](#).

4. Click **Control** >  **Promote**.
5. In the Promote Wizard, select **Promote selected versions** and click **Next**.
6. Complete the remaining wizard pages.

Tip For further details, click  **Help** in any wizard page.

Promoting by Match

With the promote-by-match method, Tripwire Enterprise only promotes current versions that meet the criteria specified by a user-defined matching strategy.


- For an introduction to this promotion method, see [What is the By-Match Selection Method? on page 73](#).
- To promote element versions, the Update Elements permission must be assigned to your user account. For more information, see [What are User Permissions and User Roles? on page 204](#).
- To complete this procedure, your match file must be in a directory that can be accessed by your Web browser.


Tip In this procedure, you can run a promote-by-match operation for a node group displayed in the main pane of the Node Manager. However, you can also do this in the **Parent Groups** tab of a node properties dialog (see [Changing the Properties of a Node on page 321](#)) or node group properties dialog (see [Changing the Properties of a Node Group on page 325](#)).

To promote element versions with a matching strategy:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the group containing the node(s) and/or node group(s) to be promoted.
3. In the main pane, select the check box of each node or node group to be promoted.

Note Only nodes and node groups marked with a severity indicator may be promoted. For more information, see [What are Severity Ranges? on page 114](#).

4. Click **Control** >  **Promote**.
5. In the Promote Wizard, select **Promote-by-match** and click **Next**.
6. Complete the remaining wizard pages.

Tip For further instructions, click  **Help** in any wizard page.


Promoting by Reference

For an introduction to the **promote-by-reference** method, see [What is the By-Reference Selection Method? \(on page 76\)](#)

To promote element versions, the Update Elements permission must be assigned to your user account. For more information, see [What are User Permissions and User Roles? on page 204](#).

Tip In this procedure, you can run a promote-by-reference for a node group displayed in the main pane of the Node Manager. However, you can also do this in the **Parent Groups** tab of a node properties dialog (see [Changing the Properties of a Node on page 321](#)) or node group properties dialog (see [Changing the Properties of a Node Group on page 325](#)).

To promote element versions using promote-by-reference:


1. In the Manager bar, click **NODES**.
2. In the tree pane, click the group containing the nodes and/or groups to be promoted.
3. In the main pane, select the check box of each node or node group to be promoted.
4. Click **Control** >  **Promote**.
5. In the Promote Wizard, select **Promote-by-reference** and click **OK**.
6. Enter a comment and click **Next**.

Notes A comment is required if the **Promote comment is required** check box is selected in the Settings Manager.

This page also includes an **Approval Identifier** field if the **Allow promotion approval identifier** setting is enabled.

For more information on these settings, see [Changing System Preferences on page 266](#).

7. Complete the remaining wizard pages.

Tip For further instructions, click  **Help** in any wizard page.

Changing Rules with the Adjust Rule Feature

Adding a Start Point with the Adjust Rule Feature

With this procedure, you use the Adjust Rule button to add a start point to a file system rule, Windows registry rule, or directory rule. For an introduction to this feature, see [What is the Adjust Rule Feature?](#) on page 84.


Tip This procedure explains how to add a start point to an element displayed in the main pane of the Node Manager. However, you can also add start points with the Adjust Rule button in:


- The **Elements** tab of a node properties dialog (see [Changing the Properties of a Node](#) on page 321)
- The **Element Search** tab of the Node Manager ([Searching for Elements](#) on page 361)
- The **Report Viewer** of some reports (see [Running a Report Manually](#) on page 601)

To create a single start point for an element with the Adjust Rule feature:

1. In the Manager bar, click **NODES**.
2. In the tree pane, select the element's node.

Note If Detailed Node View is enabled, you must also select a rule in the tree pane. To enable or disable Detailed Node View, see [Changing User Preference Settings](#) on page 262.

3. In the main pane, select the check box of any element that is *not* already a start point.
4. Click **Modify** >  **Adjust Rule**.
5. In the Adjust Associated Rule dialog, select **Create a start point for the selected element** and click **OK**. (If the rule already has a start point for the selected element, this option will not appear.)
6. Complete the New Start Point Wizard. For guidance, see [Adding a Start Point to a Rule](#) on page 462.

Tip For field definitions, click  **Help**.

Editing a Start Point with the Adjust Rule Feature

With this procedure, you use the Adjust Rule button to edit a start point in a file system rule, Windows registry rule, directory rule, or database metadata rule. For an introduction to this feature, see [What is the Adjust Rule Feature? on page 84](#).


Tip This procedure explains how to edit a start point for an element displayed in the main pane of the Node Manager. However, you can also edit start points with the Adjust Rule button in:

- The **Elements** tab of a node properties dialog (see [Changing the Properties of a Node on page 321](#))
- The **Element Search** tab of the Node Manager ([Searching for Elements on page 361](#))
- The **Report Viewer** of some reports (see [Running a Report Manually on page 601](#))

To edit a single start point for an element with the Adjust Rule feature:

1. In the Manager bar, click **NODES**.
2. In the tree pane, select the element's node.

Note If Detailed Node View is enabled, you must also select a rule in the tree pane. To enable or disable Detailed Node View, see [Changing User Preference Settings on page 262](#).

3. In the main pane, select the check box for the start point's element.
4. Click **Modify** >  **Adjust Rule**.
5. In the Adjust Associated Rule dialog, select **Edit the existing start point for the selected element** and click **OK**. (If a start point does not exist for the selected element, this option will not appear.)
6. In the start point properties dialog, edit the appropriate tabs.
7. Click **OK**.

Next (Directory rules only) If you changed the list of directory attributes monitored by a start point, you should run a version check of all entries monitored by the rule. For instructions, see:

- [Version Checking Monitored Systems on page 385](#)
- [Version Checking Specific Monitored Objects on page 386](#)

Once done, you should promote all new change versions created by the version check (see [Promoting All Current Versions for a Node or Node Group on page 395](#)).

Adding a Stop Point with the Adjust Rule Feature

With this procedure, you use the Adjust Rule button to add a stop point to a file system rule, Windows registry rule, directory rule, or database metadata rule. For an introduction to this feature, see [What is the Adjust Rule Feature? on page 84](#).


Tip This procedure explains how to add a stop point for an element displayed in the main pane of the Node Manager. However, you can also add stop points with the Adjust Rule button in:

- The **Elements** tab of a node properties dialog (see [Changing the Properties of a Node on page 321](#))
- The **Element Search** tab of the Node Manager (see [Searching for Elements on page 361](#))
- The **Elements** or **Versions** Views of the Report Viewer (see [Running a Report Manually on page 601](#))

To create a stop point for an element with the Adjust Rule feature:

1. In the Manager bar, click **NODES**.
2. In the tree pane, select the element's node.

Note If Detailed Node View is enabled, you must also select a rule in the tree pane. To enable or disable Detailed Node View, see [Changing User Preference Settings on page 262](#).

3. In the main pane, select the check box for the element.
4. Click **Modify** >  **Adjust Rule**.
5. In the Adjust Associated Rule dialog, select **Create a stop point for the selected element** and click **OK**. (If the rule already has a stop point for the element, this option will not appear.)
6. Optional step -
(For **file system rules**) If the stop point is a directory, select the **Stop recursion** check box to prevent checking of sub-directories within the directory.
(For **Windows registry rules**) If the stop point is a registry key, select the **Stop recursion** check box to prevent checking of registry entries within the key.
(For **directory rules**) Select the **Stop recursion** check box to prevent checking of sub-entries under the selected entry.
7. Click **OK**.

Deleting a Stop Point with the Adjust Rule Feature

With this procedure, you use the Adjust Rule button to delete a stop point for a file system rule, Windows registry rule, directory rule, or database metadata rule. For an introduction to this feature, see [What is the Adjust Rule Feature? on page 84](#).


Tip This procedure explains how to delete a stop point for an element displayed in the main pane of the Nodes tab of the Node Manager. However, you can also delete stop points with the Adjust Rule button in:

- The **Elements** tab of a node properties dialog (see [Changing the Properties of a Node on page 321](#))
- The **Element Search** tab of the Node Manager ([Searching for Elements on page 361](#))
- The **Elements** or **Versions** Views of the Report Viewer (see [Running a Report Manually on page 601](#))

To delete a single stop point for an element with the Adjust Rule feature:

1. In the Manager bar, click **NODES**.
2. In the tree pane, select the element's node.

Note If Detailed Node View is enabled, you must also select a rule in the tree pane. To enable or disable Detailed Node View, see [Changing User Preference Settings on page 262](#).

3. In the main pane, select the check box for the stop point's element.
4. Click **Modify** >  **Adjust Rule**.
5. In the Adjust Associated Rule dialog, select **Delete the stop point for the selected element**. (If a stop point does not exist for the selected element, this option will not appear.)
6. Click **OK** to confirm.

Using the Run Actions Feature

Running Actions for Specific Elements

For an introduction to the Run Actions feature, see [How Do I Run an Action?](#) on page 119.

Tip This procedure explains how to use the Run Actions button with changed elements displayed in the main pane of the Nodes tab of the Node Manager. However, you can also access this button in:

- The **Elements** tab of a node properties dialog (see [Changing the Properties of a Node](#) on page 321)
- The **Element Search** tab of the Node Manager ([Searching for Elements](#) on page 361)
- The **Nodes**, **Elements**, or **Versions** Views of the Report Viewer (see [Running a Report Manually](#) on page 601)


To run actions for one or more elements:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the node for the element(s).

Note If Detailed Node View is enabled, you must also select a rule in the tree pane. To enable or disable Detailed Node View, see [Changing User Preference Settings](#) on page 262.

3. Select the check box of each element for which actions will be run.

Note The Run Actions feature can only be used with elements marked with a severity indicator. For descriptions of severity indicators, see [What are Severity Ranges?](#) on page 114.

4. Click **Control** >  **Run Actions**.
5. In the Run Actions dialog, select an action or action group to be executed. (The dialog only lists the actions that apply to the selected elements.)
6. Click **OK**.

Running Actions for a Node or Node Group


For an introduction to the Run Actions feature, see [How Do I Run an Action? on page 119](#).

- Tip** This procedure explains how to use the Run Actions button with changed nodes or node groups displayed in the main pane of the Nodes tab of the Node Manager. However, you can also access this button in:
- The Report Viewer for some reports (see [Running a Report Manually on page 601](#))
 - The **Node Search** tab of the Node Manager (see [Searching for Nodes on page 355](#))
 - The **Parent Groups** tab of a node properties dialog (see [Changing the Properties of a Node on page 321](#))
 - The **Parent Groups** tab of a node group properties dialog (see [Changing the Properties of a Node Group on page 325](#))

To run actions for selected nodes or node groups:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the group containing the node(s) and/or node group(s).
3. In the main pane, select the check box of each node or node group for which actions will be run.

Note The Run Actions feature can only be used with nodes and node groups marked with a severity indicator. For descriptions of severity indicators, see [What are Severity Ranges? on page 114](#).

4. Click **Control** >  **Run Actions**.
5. In the Run Actions dialog, select an action or action group to be executed. (The dialog only lists the actions that apply to the selected node types.)
6. Click **OK**.

Restoring a Changed File with the Run Actions Feature

This procedure returns a changed file on a network device to the state of a previous element version, such as a baseline. To restore all changed files on one or more network devices to their current baselines, see [Restoring Multiple Files with the Run Actions Feature on the next page](#).

To restore a file on a network device, the following requirements must be met:

- The Update Elements permission must be assigned to your user account. For more information, see [What are User Permissions and User Roles? on page 204](#).
- Your Tripwire Enterprise implementation must include a **restore action** appropriate for the monitored system. To create a restore action, see [Creating a Restore Action on page 496](#).


Notes Files in a file system can only be restored with **execution actions** (see [How Does an Execution Action Work? on page 121](#)).

Files on directory servers, database servers, Nokia network devices, and HP ProCurve XL network devices cannot be restored. In addition, you cannot restore files in new network devices (or network device operating systems) that have been introduced since Tripwire Enterprise 5.5. In such cases, you should use an appropriate configuration tool to restore the network device.

To restore a changed file with the Run Actions feature:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the node of the element that represents the file.

Note If Detailed Node View is enabled, you must also select a rule in the tree pane. To enable or disable Detailed Node View, see [Changing User Preference Settings on page 262](#).

3. In the main pane, select the file's element in the **Element** column.
4. In the element properties dialog, select the **History** tab.
5. Select the check box of the element version with which you want to restore the file. (The current baseline is highlighted.)
6. Click  **Run Actions**.
7. Select a restore action for the network device and click **OK**.

Next If you restored the file with its current baseline, you can check the file to verify that it was successfully restored. For instructions, see [Version Checking Specific Monitored Objects on page 386](#).

Restoring Multiple Files with the Run Actions Feature

With this procedure, you can restore all changed files on one or more network devices to their current baselines. If the current version of a file is the file's current baseline, no action is taken.

To restore a file, the following requirements must first be met:

- The Update Elements permission must be assigned to your user account. For more information, see [What are User Permissions and User Roles?](#) on page 204.
- Your Tripwire Enterprise implementation must include a **restore action** appropriate for the monitored system. To create a restore action, see [Creating a Restore Action](#) on page 496.


To restore a specific file to its baseline, see [Restoring a Changed File with the Run Actions Feature](#) on the previous page.

Notes Files in a file system can only be restored with **execution actions** (see [How Does an Execution Action Work?](#) on page 121).

Files on directory servers, database servers, Nokia network devices, and HP ProCurve XL network devices cannot be restored. In addition, you cannot restore files in new network devices (or network device operating systems) that have been introduced since Tripwire Enterprise 5.5. In such cases, you should use an appropriate configuration tool to restore the network device.

Tip This procedure uses the Run Actions button to restore nodes or node groups displayed in the main pane of the Node Manager. However, you can also access this button in the **Parent Groups** tab of a node properties dialog (see [Changing the Properties of a Node](#) on page 321) or node group properties dialog (see [Changing the Properties of a Node Group](#) on page 325).

To restore all changed files on one or more network devices:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the group containing the node(s) and/or node group(s) to be restored.
3. In the main pane, select the check box of each node or node group to be restored. Only nodes and node groups marked with a severity indicator can be restored. (For descriptions of severity indicators, see [What are Severity Ranges?](#) on page 114.)
4. Click **Control** >  **Run Actions**.
5. Select an appropriate restore action(s) for the specified monitored systems and click **OK**.

Next If desired, you can check the monitored systems to verify that the files were successfully restored to their current baselines. For instructions, see [Version Checking Monitored Systems](#) on page 385.

Exporting and Importing Objects in the Node Manager


Exporting Nodes and Node Groups

This procedure exports and saves selected nodes and node groups in an XML file. As needed, the contents of the XML file may be re-imported at a later date (see [Importing Nodes and Node Groups on the next page](#)).

To export node-access passwords to an XML node file, the **export passwords** permission must be assigned to your user account (see [What are User Permissions and User Roles? on page 204](#)). By default, only Administrators have this permission. If you do not have this permission, the passwords are excluded from the export output.

- Tip** This procedure explains how to export nodes and node groups displayed in the main pane of the Node Manager. However, you can also export:
- Nodes in the Report Viewer for some reports (see [Running a Report Manually on page 601](#))
 - Nodes in the **Node Search** tab of the Node Manager (see [Searching for Nodes on page 355](#))
 - Node groups in the **Parent Groups** tab of a node properties dialog (see [Changing the Properties of a Node on page 321](#))
 - Node groups in the **Parent Groups** tab of a node group properties dialog (see [Changing the Properties of a Node Group on page 325](#))

To export nodes and node groups to an XML file:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the node group containing the nodes and node groups to be exported.
3. (Optional) To export **specific** nodes and node groups, select the appropriate check boxes in the main pane. Only objects on the same page of the Node Manager can be selected in a single export operation.
4. Click **Manage** >  **Export**.
5. In the Export Nodes dialog, select one of the following options and click **OK**:
 - **All nodes and node groups**. This option exports all nodes and node groups in your Tripwire Enterprise implementation.
 - **Selected nodes and node groups**. This option exports the selected nodes and node groups only.
6. To export the XML file to a local directory, complete the steps for your operating system.

Caution Node XML files may contain sensitive network information. Therefore, these files should be saved in a secure location.

Importing Nodes and Node Groups

This procedure imports nodes (and node groups) from an XML or CSV file to your Tripwire Enterprise implementation.


- To create an XML file for nodes, see [Exporting Nodes and Node Groups on the previous page](#).
- Import of CSV files is a legacy feature from Tripwire for Network Devices. In Tripwire Enterprise, nodes cannot be exported to a CSV file.

Notes Prior to this procedure, you should first review the guidelines employed by Tripwire Enterprise when importing the contents of a CSV or XML file (see [How Do I Import and Export Tripwire Enterprise Objects? on page 217](#)).

If you import a node with a custom property that does *not* exist in your TE implementation, TE creates the property in the Settings Manager. However, if the property already exists, TE does *not* overwrite the property's settings in the Settings Manager.

If you import a file with smart node groups (see [About Node Groups and Smart Node Groups on page 57](#)), the smart node groups will not be recreated in the node tree, and any smart node groups on the target system will not be changed. Any nodes in the import file that were descendant from the Smart Node Group will be placed in an **Imported from Smart Node Groups** group.

To import the nodes and node groups in an XML or CSV file:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the node group to which the XML or CSV file will be imported. The node group hierarchy specified in the file will be created in this location.
3. Click **Manage** >  **Import**.
4. In the Import Nodes dialog, click **Browse**.
5. To locate and select the XML or CSV file, complete the standard steps for your operating system.

Caution XML and CSV files may contain sensitive network information. Therefore, these files should be saved in a secure location or deleted following import.

6. In the Import Nodes dialog, click **OK**.

Exporting, Importing, and Cloning Element Versions

Exporting the Content of an Element Version


If an element version represents a monitored object for a database server, or a file on a network device or file server, and the version contains the content of the monitored object, you can export the content to a text file (known as a **version content file**).

Tip This procedure explains how to export a version of an element displayed in the main pane of the Node Manager. However, you can also export element versions through the **Elements** tab of a node properties dialog (see [Changing the Properties of a Node on page 321](#)).

To export and save the content of an element version:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the version's node.

Note If Detailed Node View is enabled, you must also select a rule in the tree pane. To enable or disable Detailed Node View, see [Changing User Preference Settings on page 262](#).

3. In the main pane, click the version's element in the **Elements** column.
4. In the element properties dialog, select the **History** tab.
5. In the **Version** column, click the element version to be exported.
6. In the version properties dialog, select the **Content** tab.
7. Click  **Export**.
8. To save the content file to a local directory, complete the standard steps for your operating system.

Importing Element Version Content


By importing content from a version content file, this procedure creates a new element version for a monitored object of a network device.


To create a version content file, see [Exporting the Content of an Element Version on the previous page](#).

To create a new version of an element by importing a version content file:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the node group containing the element's node.
3. In the main pane, click the node in the **Name** column.
4. In the node properties dialog, select the **Elements** tab.
5. In the **Element** column, click the desired element.

Note If Detailed Node View is enabled, you must first select a rule from the tree in the Elements tab. To enable or disable Detailed Node View, see [Changing User Preference Settings on page 262](#).

6. In the element properties dialog, select the **History** tab.
7. Select the check box for the element version to be imported.
8. Click  **New Version**.
9. In the New Version Editor, select **Import** and click **Browse**.
10. To import the file to Tripwire Enterprise, complete the standard steps for your system.

Tip To promote the imported element version to the baseline, select the check box for the version (in the element properties dialog) and click  **Promote**. For further details, see [Promoting a Specific Element Version on page 393](#).

Cloning an Element Version


Element versions **cannot** be directly modified by users. However, you can create a copy of an element version that represents a file on a network device and then modify the copy.

Note An element version that represents a file in a file system *cannot* be cloned.

To create and modify a cloned copy of a file element version:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the node group containing the version's node.
3. In the main pane, click the node in the **Name** column.
4. In the node properties dialog, select the **Elements** tab.
5. In the **Element** column, click the desired element.

Note If Detailed Node View is enabled, you must first select a rule from the tree in the Elements tab. To enable or disable Detailed Node View, see [Changing User Preference Settings](#) on page 262.

6. In the element properties dialog, select the **History** tab.
7. In the **Version** column, click the element version to be copied.
8. In the version properties dialog, select the **Content** tab.
9. Click  **New Version**.
10. If desired, enter a **Comment**.
11. Select **Clone and edit** and modify the element version content, as appropriate.
12. Click **OK**.

Managing Agent Nodes

Assigning a Delegated Agent to a Node

When you create a database node, directory server node, or VI management node, you also specify a **delegated Agent** for the node. A delegated Agent is an Agent system that processes some Tripwire Enterprise functions for the node.

Note Only nodes with Tripwire Enterprise Agent installed can be a delegated Agent for a database, directory server, or VI management node. Tripwire strongly recommends that you install TE Agent on these nodes, and use that Agent both to monitor that system's file system, and as the delegated Agent for the database, directory server, or VI management system itself.

Nodes with Axon Agent installed cannot be used as a delegated Agent.

To change the delegated Agent for a database node, directory server node, or VI management node:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the node group containing the node.
3. In the main pane, select the node in the **Name** column.
4. In the node properties dialog, select the **Delegated Agent** tab.
5. In the node tree, select the Agent node.

Note Only nodes with Tripwire Enterprise Agent installed can be a delegated Agent. Nodes with Axon Agent installed cannot be used as a delegated Agent.

6. To test the connection with the Agent node:
 - a. Click **Test Login**.
 - b. If the test was successful, click **OK** in the success message.

If the test was unsuccessful, verify the information in the General, Connection, Login, and Delegated Agent tabs of the Agent's properties dialog (see [Changing the Properties of a Node on page 321](#)).
7. Click **OK** to close the node properties dialog.

Restarting Tripwire Enterprise Agents

The **Tripwire Enterprise Agent service** is a process that runs on a file system on which Tripwire Enterprise Agent software is installed. The TE Agent service collects change data for the file server node, as well as any directory server or database nodes to which the TE Agent has been assigned. The TE Agent service then reports this data to the Tripwire Enterprise Server.

With this procedure, you can stop and restart the TE Agent service for one or more file server nodes. If needed, you can also refresh the Agent data upon restart. Data refresh synchronizes the local TE Agent database with the TE Console database.

Notes Restarting Agents only affects Tripwire Enterprise Agents. It does not have any effect on nodes with Axon Agent installed or on network device nodes.

If you restart a directory server or database node, the TE Agent on the file system node assigned to that node (known as the **delegated Agent**) is restarted. For more information on delegated Agents, see [Creating a Node Manually on page 56](#)

If you upgrade from an earlier version of TE Console, all Agents should be restarted and refreshed.

If you restart a TE Agent that is currently being baselined or version checked, an error will occur.

To restart TE Agents in the Asset View tab:

1. (Optional) Use the Asset Filter pane to refine the list of assets in the Asset List.
2. In the Asset List, click the checkbox for each asset that you want to restart.
As you select each asset, it is added to the list in the Selection Information pane.
3. Click **Health Check** at the top of the list in the right pane, then select **Restart Agents** from the dropdown menu.
4. In the confirmation dialog, leave **Refresh agent data** selected to regenerate the database of each restarted TE Agent.
5. Click **OK**.

Tip You can also restart TE Agents from the Nodes or Node Search tabs of the Node Manager. Select the nodes or node groups, then click **Modify > Restart Agents**.

Next If you refreshed data for a TE Agent system that is being monitored in real-time by Tripwire Enterprise, you should run a manual version check of the Agent node with all applicable RTM-enabled rules. For instructions, see [Version Checking Monitored Systems on page 385](#).

Upgrading Agents

To upgrade a Tripwire Enterprise Agent or Axon Agent, complete the following steps:

Step 1. Upload Agent Updaters (below)

Step 2. Upgrade Agent Software (on page 415)

During an upgrade, Tripwire Enterprise will install either the 32-bit or 64-bit Agent software, matched to the operating system of the Agent system. If you want to upgrade 32-bit Agent software on a 64-bit OS, you must manually uninstall and re-install the Agent software.

Note You cannot use this procedure to upgrade an Agent on a platform that is not supported by the current version of Tripwire Enterprise. For a complete list of supported platforms for the current TE release, see <https://www.tripwire.com/products/tripwire-enterprise/tripwire-enterprise-platform-and-device-support-register>.

When upgrading a TE Agent older than version 8.5.0, you must first upgrade to TE Agent version 8.5.0 before upgrading to any later version.


Step 1. Upload Agent Updaters

To upgrade an Agent, you must first upload Agent updaters to the system where Tripwire Enterprise Console is installed, using the TE Console Settings Manager.

Note You can also upload Agent updaters for Tripwire Enterprise Agents using the command line. For more information, see [Uploading TE Agent Updaters from the Command Line on the next page](#).

Axon Agent updaters **must** be uploaded from TE Console using the steps below.

To upload Agent updaters:

1. Download the Agent updaters you want to install from the Tripwire Customer Center (<https://tripwireinc.force.com/customers>) and copy them to a location that is accessible from the TE Console system.
2. In the Manager bar, click **SETTINGS**.
3. Under the System folder, click  **Agent Updaters**.
4. In the main pane, click **Add Updater**.
5. In the Select Agent Updater Files dialog, click **Choose Files** and browse to the updaters you downloaded. Select one or more updaters and click **Open**.
6. Click **OK** when you are done selecting updaters.

After you have uploaded the Agent updaters to the TE Console system, proceed to [Step 2. Upgrade Agent Software on page 415](#).

Uploading TE Agent Updaters from the Command Line

Follow the steps below to upload TE Agent updaters without using the TE Console UI.

To upload Axon Agent updaters, you **must** use the process described in [Step 1. Upload Agent Updaters on the previous page](#).

To upload TE Agent updaters from the command line on a Linux TE Console:

1. Download the updaters you want to install from the Tripwire Customer Center (<https://tripwireinc.force.com/customers>).
2. Log in to the TE Console system as a privileged user.
3. If it doesn't exist already, create the following directory on the TE Console system:

```
mkdir /usr/local/tripwire/te/server/lib/updaters
chown tripwire:tripwire /usr/local/tripwire/te/server/lib/updaters
```

4. Copy the Agent updaters to the TE Console updaters directory:

```
cp -r updaters/* /usr/local/tripwire/te/server/lib/updaters
```

Do not unzip the files. They will be unzipped automatically during the update process.

5. Change directories to the Agent updaters directory:

```
cd /usr/local/tripwire/te/server/lib/updaters
```

6. To configure the user permissions for all contents of the directory, enter:

```
chmod 0444 *
chown tripwire:tripwire *
```

To upload TE Agent updaters from the command line on a Windows TE Server:

1. Download the updaters you want to install from the Tripwire Customer Center (<https://tripwireinc.force.com/customers>).
2. If it doesn't exist already, create the following directory on the TE Console system:

```
C:\Program Files\Tripwire\TE\Server\lib\updaters
```

3. Copy the Agent updaters to the new updaters directory on the TE Console system.

Do not unzip the files. They will be unzipped automatically during the update process.

4. To configure the user permissions for the updaters directory:

- a. In Windows Explorer, right-click the directory and select **Properties**.

- b. In the Properties dialog, clear (disable) the **read-only** attribute and verify that the Administrators user group has the **Full Control** permission.

Step 2. Upgrade Agent Software

Notes By default, the Event Generator software on TE Agent systems is updated at the same time as the Agent software. For more information, see [Upgrading Event Generator Software on TE Agents on the next page](#).


When upgrading a TE Agent on a Solaris system, the procedures in this section do not allow you to change the user account with which the Agent is running. For more information, see *Installing Tripwire Enterprise Agent on Solaris* in the *Tripwire Enterprise Installation & Maintenance Guide*.

To upgrade a TE Agent on a Solaris system, the upgrade must run as the root user, and root must be added as an authorized user to the `at.allow` file. If you edit this file, you may need to create a policy waiver for some Tripwire-published policies.

To upgrade Agent software on one or more Agent systems:

1. In the TE Console Manager bar, click **NODES**.
2. In the tree pane, select the node group with the Agent nodes to be upgraded.
3. **To upgrade specific Agents**, select the check box of each Agent node (or node group) in the main pane.

To upgrade all Agents in the selected node group, do not select any check boxes.

4. Click **Modify** >  **Upgrade**.
5. In the Upgrade Agents dialog, click **Next**.
6. (Optional) To upload a properties file for Linux or Windows TE Agents:
 - a. Click **Select**.
 - b. Click **Browse**.
 - c. In the Choose File dialog, select the file and click **Open**.
 - d. Click **Upload**.
7. Click **Finish**.

Tip If an error occurs, Tripwire Enterprise will generate an Error message in the Log Manager and the node will be tagged with a Health:Push Upgrade Error tag in Asset View. To begin troubleshooting, review these messages.

8. **For TE Agent upgrades on AIX systems only**, perform the following steps to enable real-time and Event Generator functionality:
 - a. Log into the AIX box with root privileges.
 - b. Run `<te root>/sup/rtm/teauditconfig`.
 - c. Start GES (`startsrc -s teges`).

Upgrading Event Generator Software on TE Agents

When upgrading a TE Agent running a platform that supports Event Generators, by default the upgrade also:

1. Installs an Event Generator on the Agent system,
2. Enables audit-event collection and real-time monitoring (RTM) for the Agent, and
3. Specifies port 1169 (TCP) as the port on the Agent system to be used by Tripwire Enterprise for all communications with the Event Generator.

On Linux and Windows TE Agents, you can override this default behavior by uploading a properties file (in [Step 2. Upgrade Agent Software on the previous page](#)) containing one or both of the following lines:

```
install_rtm=false  
rtm_port=<port_number>
```

where:

`install_rtm=false` prevents the installation of Event Generators, and
`<port_number>` specifies a port other than 1169.

On Solaris 10 systems, the `install_rtm` option cannot be used to prevent the installation of an Event Generator. An Event Generator is always installed.

On AIX systems, Tripwire does **not** recommend setting the `install_rtm` flag to `false` in the properties file, even if you do not intend to use real-time monitoring or Event Generator functionality with the TE Agent. If you do not want to use real-time monitoring, shut down the Event Generator (`stopsrc -s teeg`) after upgrading the TE Agent.

Changing TE Agent Configuration Properties

With this procedure, you can modify most TE Agent configuration properties for one or more monitored file systems. For a complete list of TE Agent property descriptions, see *Tripwire Enterprise Agent Configuration Properties* in the *Tripwire Enterprise Reference Guide*.

Note If the `tw.disableConfigEditing` property in a TE Agent's properties file is set to true, any edits made to that Agent's properties file using the TE Console user interface will be ignored. You can still edit the file directly using a text editor.


Tip This procedure explains how to configure the properties of TE Agents displayed in the main pane of the Nodes tab of the Node Manager. However, you can also configure the properties of TE Agents in:

- The **Parent Groups** tab of a node properties dialog (see [Changing the Properties of a Node on page 321](#))
- The **Node Search** tab of the Node Manager (see [Searching for Nodes on page 355](#))

To configure Tripwire Enterprise Agent for one or more file server nodes:

1. In the Manager bar, click **NODES**.
2. To configure specific TE Agents, select the check box of each file server node in the main pane.

To configure all TE Agents, do not select any check boxes.

3. Click **Modify** >  **Configure**.
4. In the Configure Agents dialog, edit the property values.
 - To assign the default value to a property, click the associated **Default** button.
 - To view the names of all properties, select **Show full names of properties**.
 - To view the descriptions of all properties, select **Show detailed descriptions**.
5. Click **OK**.

Caution If you edit property values and click **OK**, Tripwire Enterprise restarts the service for each affected TE Agent. If one of the Agents is currently being baselined or version checked, an error will occur. For more information, see [Restarting Tripwire Enterprise Agents on page 412](#).

Managing Licenses for Nodes

With this procedure, you can enable or disable licenses on specified nodes. For more information, see [About Tripwire Enterprise Licenses on page 202](#).


Tips If you remove all licenses from a node, Tripwire Enterprise disables version checks and baseline operations on the node until a license is applied to the node again. For more information, see [Temporarily Disabling Checks and Baselines on a Node on page 387](#).


You can also manage licenses in the Node Search tab (see [Searching for Nodes on page 355](#)).

To apply or remove licenses to/from specified nodes:

1. In the Manager bar, click **NODES**.
2. In the tree pane, select the node group containing the nodes.
3. To apply or remove licenses to/from specific nodes, select the check box of each node and/or group in the main pane.

To apply or remove licenses to/from all nodes in the selected node group, do not select any check boxes.

4. Click **Modify** >  **Licenses**.
5. Complete the Update Node Licenses dialog and click **OK**.

Tip For more information, click  **Help**.

Configuring SSL for Database, Directory Server, and Virtual Nodes

Tripwire Enterprise can use SSL to secure communication with many monitored node types:

- Microsoft SQL Server databases
- Oracle databases
- PostgreSQL databases
- Active Directory servers
- LDAP directory servers
- VMware virtual systems

Some SSL modes, and all SSL connections with a TE Agent in FIPS mode, require a trust relationship between the monitored system and the TE Agent that monitors it. If the monitored system is using a certificate that is self-signed, or signed by an internal CA, its root certificate (and any intermediates) will need to be added to the customer trust store used by the Tripwire Enterprise Agent. You can add the certificate before or after you create the node in TE Console, but you must do so before you can use SSL.

Notes **To configure SSL between TE Console and an LDAP or Active Directory server used to authenticate TE Console user logins**, see [Configuring the Tripwire Enterprise Login Method](#) on page 294.

To configure SSL between TE Console and a backend database, see:

- *Step 3: Install Tripwire Enterprise Console* in the *Tripwire Enterprise Installation & Maintenance Guide* (for MS SQL Server backend databases)
- *Configuring SSL for a MySQL Backend Database* in the *Tripwire Enterprise Hardening Guide*, available from the [Tripwire Customer Center](#).

To add an SSL certificate to a Tripwire Enterprise Agent:

1. Acquire an SSL certificate from the system to be monitored. Make sure that the certificate is exported in either **DER Encoded Binary** or **PEM X.509** format.

Note For VMware nodes, acquire the SSL certificate for the vCenter system used to manage that node.

2. Copy the SSL certificate file to the following directory on the TE Agent system used to monitor the database, directory server, or virtual node (specified on the node's **Delegated Agent** tab):

```
<te_root>/agent/data/security
```

where <te_root> is the root Tripwire Enterprise Agent installation directory.

3. Open a command prompt or terminal session on the TE Agent system where you copied the certificate file, then run one of the following commands:

Windows:

```
<te_root>\Agent\jre\bin\keytool -import -alias <name> -file <cert>  
-keystore customer_trust_store.ks
```

Linux:

```
<te_root>/agent/jre/bin/keytool -import -alias <name> -file <cert>  
-keystore customer_trust_store.ks
```

where:

<name> can be any value. It is only used to refer to a certificate in the keystore, and <cert> is the full path to the certificate you copied into the data\security directory

4. When prompted for a password enter the password change it.
5. Answer y to trust the certificate and add it to the keystore.
6. Restart the TE Agent service:

UNIX or Linux systems: <te_root>/agent/bin/twdaemon restart

Windows: "<te_root>\Agent\bin\twdaemon" restart

After completing these steps, you will be able to use SSL to secure communication with the monitored system, as long as SSL is specified in the node's Connection tab.

Changes to Keystores in Tripwire Enterprise 8.4.1

Tripwire Enterprise Console

A new key store has been added to TE Console at `<te_root>/server/data/security/customer_trust_store.ks`. This keystore stores certificates added by users to authenticate communication with an Active Directory login server or backend database. Any existing user-supplied certificates in the previous `<te_root>/server/data/security/cacerts.ks` keystore are migrated to the new keystore during a TE Console upgrade.

If your TE installation uses certificates to authenticate communication, you should review the certificates in the new keystore after upgrading from TE Console 8.4.0 to verify that all certificates were migrated correctly, and to delete any extraneous certificates. This verification only needs to happen once, the first time that TE Console 8.4.0 is upgraded.

To view certificates in the trust store:

```
keytool -list -v -keystore customer_trust_store.ks -storepass changeit
```

To remove certificates from the trust store:


```
keytool -delete -keystore customer_trust_store.ks -storepass changeit -alias <cert_alias>
```

Tripwire Enterprise Agents

TE 8.4.1 Agents use a new key store at `<te_root>/agent/data/security/customer_trust_store.ks` to store user-supplied certificates. During an upgrade, the existing `<te_root>/agent/jre/lib/security/cacerts` keystore on the Agent system will be deleted. Any existing user-supplied certificates in the `cacerts` keystore must be manually imported into the new keystore.

Starting with Tripwire Enterprise 8.4.1, certificates in the new keystore will be retained when the TE Agent is upgraded. This means that certificates only need to be imported one time, the first time that the Agent is upgraded from version 8.4.0.

Configuring Audit Event Collection and Real-Time Monitoring for Multiple Systems

With the  **Events** button in the Node Manager, you can configure the following features for multiple nodes:

- Audit event collection (see [What is Audit Event Collection? on page 63](#))
- Real-time monitoring (see [How Does Real-Time Monitoring Work? on page 70](#))

If you attempt to configure a feature that is unavailable for a selected node, the Events button will have no effect on that particular feature for the node. For example, consider a file server node for which audit event collection is disabled, and an Event Generator has yet to be installed on the file server represented by the node. If you use the Events button to enable audit event collection for the node, and select the Event Generator as the audit event source, TE makes the following changes in the properties of the node:


- TE enables audit event collection.
- Since the file server lacks an Event Generator, TE assigns the default audit event source (see [Table 13 on page 63](#)).

Tip This procedure explains how to configure audit event collection and real-time monitoring for nodes displayed in the main pane of the Nodes tab of the Node Manager. However, you can also configure these features for nodes in the Node Search tab (see [Searching for Nodes on page 355](#)).

To configure audit event collection and real-time monitoring for one or more nodes:

1. In the Manager bar, click **NODES**.
2. In the tree pane, select the node group that contains the nodes to be configured.
3. To configure specific nodes and/or node groups, select the check box of each object in the main pane.

To configure all nodes and/or node groups currently displayed in the main pane, do not select any check boxes.

4. Click **Modify** >  **Events**.
5. Complete the Events dialog and click **Finish**.

Notes Additional steps may be necessary to configure audit event collection or real-time monitoring after using the Events dialog. For more information, see [What is Audit Event Collection? on page 63](#) and [How Does Real-Time Monitoring Work? on page 70](#).

In the Log Manager, TE generates a Node Change log message for each node on which the procedure ran. To assess the results of the operation, go to the Log Manager and review the associated log messages.

Downloading Agent Log Files

With this procedure, you can download and save the log files of an Agent installed on a monitored file system.

To download Agent log files for a file server node:

1. In the Manager bar, click **NODES**.
2. In the tree pane, click the node group containing the node.
3. In the main pane, select the node in the **Name** column.
4. In the node properties dialog, select the **Agent Logs** tab.
5. The **Agent log files** list includes all files in the Agent's log directory (<install_directory>/data/log). For instance:
 - **install.log**. When Agent software is installed, this file records information about the process.
 - **teagent.log**. When the Agent's service is started or stopped, the event is recorded in this log file. In addition, this file records all errors that occur on the Agent.
 - **teserver.log**. When the Tripwire Enterprise Console services are started or stopped, the event is recorded in this log file. In addition, this file records all errors that occur on the TE Server.
 - **tesvc.log**. When an Event Generator is installed on an Agent, this file records audit events for real-time monitoring. For more information, see [How Does Real-Time Monitoring Work? on page 70](#).
 - **tomcat.log**. When the Tripwire Enterprise Web Service is started or stopped, the event is recorded in this log file. In addition, this file records all errors that occur with the Web Service.

Note When one of these log files reaches its maximum size, the file is 'rolled' (in other words, the file is archived and a new file is created). Therefore, archived files may also appear in the Log files list. Archived files have a numeric extension (for example, `teagent.log.2`, `teagent.log.3`, and so on), and higher extension numbers indicate older log files.

`teserver.log` and `tomcat.log` only appear in the **Log files** list if the Agent system is also your Tripwire Enterprise Server.

6. Click **Download**.
7. To download and/or save the log file to a local directory, complete the standard steps for your operating system.

Restricting Commands on Agent Nodes with Whitelists

A number of components of Tripwire Enterprise can be configured to run arbitrary commands on Tripwire Enterprise Agents or Axon Agents:

- command output capture rules (COCRs)
- log transfer rules
- command execution actions
- automated remediation scripts
- post-remediation service commands
- Windows RSoP rules

Because these objects can be modified by any TE user with the appropriate permissions, there is a risk that they could be used to run malicious commands on Agent systems.

To address this threat, whitelists can be used to manage the commands that TE can execute on Agent systems. A **whitelist**, installed on each TE Agent or Axon Agent system, contains an explicit list of commands that Tripwire Enterprise can run on that Agent. Each command that Tripwire Enterprise attempts to execute must **exactly** match a command in the whitelist file. Any other command initiated by Tripwire Enterprise on the Agent system will be denied and logged in the Agent's log file (`teagent.log` for TE Agents, `twexec.log` for Axon Agents), and in the Log Manager in the Tripwire Enterprise Console.

Whether or not a command is executed on an Agent depends on 1) if a whitelist is installed on an Agent, and 2) if the Agent requires that a whitelist is used. [Table 97](#) summarizes the possible outcomes.

Table 97. Command execution matrix for whitelists

Is a whitelist installed on the Agent?	Is a whitelist required on the Agent?	Is the command on the whitelist?	Is the command executed?
N	N	N/A	Y (default)
N	Y	N/A	N
Y	N/A	Y	Y
Y	N/A	N	N

To create and install a whitelist, see:

- [Implementing a Whitelist for a TE Agent on the next page](#)
- [Implementing a Whitelist for an Axon Agent on page 427](#)

Implementing a Whitelist for a TE Agent

To use a whitelist for a TE Agent, a whitelist file is created using a TE Console and then installed on the TE Agent system that will use it.

Note After a whitelist is installed on a TE Agent system, it can only be edited, enabled, or disabled by users on that system who have the proper permissions. A whitelist **cannot** be edited, enabled, or disabled from the TE Console.

If you use post-remediation service commands, and you want TE to expand variables in these commands when generating and validating whitelists, follow the steps in [Expanding Post-Remediation Service Commands in Whitelists on the next page](#) before using the procedure below.

To create and install a whitelist file on a TE Agent system:

1. On the TE Console system, run the following command from the command line:

```
<te_root>/server/bin/tetool  
run com.tripwire.tools.whitelist.WhitelistGenerator <output_file>
```

where <output_file> is any name you specify. The Console will generate a UTF-8 encoded XML file listing every command that Console can run on an Agent system. If <output_file> is not specified, the command will print results to standard output.

2. Edit the output file to limit the commands that can be run on a specific Agent system. Standard XML comments can be added (<https://www.w3.org/TR/REC-xml/#sec-comments>).
3. Save the whitelist file, then copy it to the following location on a TE Agent system:

```
<te_root>/agent/data/agent/execWhitelist.xml
```

4. (Optional) To require this TE Agent to always use a whitelist to validate TE commands (see [Table 97 on the previous page](#)), follow these steps:
 - a. Open the Agent properties file with a text editor. By default, the Agent properties file is located at <te_root>/agent/data/config/agent.properties.
 - b. Add the following line to the Agent properties file:

```
tw.agent.exec.requireWhitelist=true
```

Notes This setting cannot be accessed from the Tripwire Enterprise Console; it must be set by editing the Agent configuration file directly.

If a whitelist is required on a TE Agent node and that node is **also** used as the delegated Agent used to monitor a database, a query whitelist will also be required to run database query rules on the database. For more information on query whitelists, see [Restricting Queries on Database Nodes with Whitelists on page 429](#).

- c. Save and close the file.

5. (Windows Agents only) If you want this Agent to validate the commands used for RSOP rules (secedit, auditpol, gpresult) against a whitelist each time they are run, follow these steps:
 - a. Open the Agent properties file with a text editor. By default, the Agent properties file is located at <te_root>/agent/data/config/agent.properties.
 - b. Add the following line to the Agent properties file:

```
tw.whitelist.validateRSOPCommandLine=true
```
 - c. Save and close the file.
6. If you edited the Agent properties file, restart the Agent service to apply those changes. Individual Agents can be restarted from the command line, or multiple Agents can be restarted from the Node Manager in the TE Console. For more information, see:
 - *Managing the Tripwire Enterprise Agent Service* in the *Tripwire Enterprise Installation & Maintenance Guide*
 - [Restarting Tripwire Enterprise Agents on page 412](#)

Expanding Post-Remediation Service Commands in Whitelists

Post-remediation service commands are activities initiated by Tripwire Enterprise on a TE Agent node following automated remediation. Post-remediation service commands start, stop, restart, or reload a service on a TE Agent node in order to implement the changes made by automated remediation.

Most post-remediation service commands use `Action` and `Service` variables defined in a script associated with the command. By default, post-remediation service commands are added to a whitelist and validated without expanding these variables.

Follow the steps below to expand `Action` and `Service` variables in post-remediation service commands when whitelists are generated and validated.

To expand variables in post-remediation service commands during whitelist creation and validation:

1. In a text editor, edit a TE Console's `server.properties` file to add `tw.remediation.validateExpandedServiceRestartCommandLine=true`.
2. Save the file, then restart the Console service to implement the change:

```
<te_root>\Server\bin\twservices restart
```
3. Generate and distribute a whitelist file, as described in [Restricting Commands on Agent Nodes with Whitelists \(on page 424\)](#).

Implementing a Whitelist for an Axon Agent

To use a whitelist for an Axon Agent, a whitelist file is created using a TE Console and then installed on the Axon Agent system that will use it.

Notes Because Axon Agents do not support log transfer rules, automated remediation scripts, or post-remediation service commands, whitelists for Axon Agents do not need to include them. RSoP rules run using the Axon Agent do not require whitelisting, because the RSoP implementation on Axon Agents does not allow the Agent to run arbitrary commands.

For command output capture rules (COCRs), Axon Agents only support whitelisting of the **Command Line** field. Text in the **Script** field will be included in the generated whitelist XML file but during validation the Axon Agent will compare only the COCR's command line (not the script) to the whitelist. To prevent a COCR script from running on an Axon Agent, remove the command line from the whitelist.

After a whitelist is installed on an Axon Agent system, it can only be edited, enabled, or disabled by users on that system who have the proper permissions. A whitelist **cannot** be edited, enabled, or disabled from the TE Console.

To create and install a whitelist file on an Axon Agent system:

1. On the TE Console system, run the following command from the command line:

```
<te_root>/server/bin/tetool  
run com.tripwire.tools.whitelist.WhitelistGenerator <output_file>
```

where <output_file> is any name you specify. The Console will generate a UTF-8 encoded XML file listing every command that Console can run on an Agent system. If <output_file> is not specified, the command will print results to standard output.

2. Edit the output file to limit the commands that can be run on a specific Agent system. Standard XML comments can be added (<https://www.w3.org/TR/REC-xml/#sec-comments>).
3. Save the whitelist file, then copy it to the following location on an Axon Agent system:

Linux: /etc/tripwire/execWhitelist.xml

Windows: %PROGRAMDATA%\Tripwire\agent\config\execWhitelist.xml

4. (Optional) You can configure whitelist behavior on an Axon Agent by editing that Agent's twexec.conf file. To edit this file, follow these steps:

- a. Create a plain text file named twexec.conf at:

Linux: /etc/tripwire/twexec.conf

Windows: %PROGRAMDATA%\Tripwire\agent\config\twexec.conf

- b. To prevent this Axon Agent from running any TE commands, add this line to the file:

```
prevent.commandline.execution=true
```

- c. To require this Axon Agent to always use a whitelist to validate TE commands (see [Table 97 on page 424](#)), add this line to the file:

```
require.whitelist=true
```

Note This setting cannot be accessed from the Tripwire Enterprise Console; it must be set by editing the <code>twexec.conf</code> file directly.

- d. Save and close the file.
- e. Enter one of the following sets of commands to restart the Agent Service:

Linux (RHEL and CentOS):

```
/sbin/service tripwire-axon-agent stop  
/sbin/service tripwire-axon-agent start
```

Linux (Debian and Ubuntu):

```
/usr/sbin/service tripwire-axon-agent stop  
/usr/sbin/service tripwire-axon-agent start
```

Windows:

```
net stop TripwireAxonAgent  
net start TripwireAxonAgent
```

Restricting Queries on Database Nodes with Whitelists

Tripwire Enterprise uses whitelist files to manage the commands that the software can run on Agents. For more information on whitelists, see [Restricting Commands on Agent Nodes with Whitelists](#) on page 424.

A **query whitelist** provides similar functionality for SQL queries. A query whitelist file contains an explicit list of SQL queries that Tripwire Enterprise can run. This file is installed on a delegated TE Agent used to monitor database nodes. Each query that Tripwire Enterprise initiates from a database query rule is compared to this whitelist, and must **exactly** match a query in the file. Any other queries initiated by Tripwire Enterprise on the TE Agent system will be denied and logged in the Agent's `teagent.log` file and on the Tripwire Enterprise Console.

Whether or not a query is executed on a database depends on 1) if a query whitelist is installed on that database's delegated TE Agent, and 2) if the TE Agent requires that a whitelist is used. [Table 98](#) summarizes the possible outcomes.

Table 98. Database query execution matrix for whitelists

Is a query whitelist installed on the Agent?	Is a whitelist required on the Agent?	Is the query on the whitelist?	Is the query executed?
N	N	N/A	Y (default)
N	Y	N/A	N
Y	N/A	Y	Y
Y	N/A	N	N

Implementing a Query Whitelist File

To use a query whitelist, a whitelist file is created using a TE Console and then copied to each delegated TE Agent system that is used to monitor database nodes.

Note After a query whitelist is installed on a TE Agent system, it can only be edited, enabled, or disabled by users on that system who have the proper permissions. A whitelist **cannot** be edited, enabled, or disabled from the TE Console.

To create and install a query whitelist file on a delegated TE Agent system:

1. On the TE Console system, run the following command from the command line:

```
<te_root>/server/bin/tetool run  
com.tripwire.tools.whitelist.SqlWhitelistGenerator sql-whitelist.xml
```

The Console will generate a UTF-8 encoded XML file listing every database query that Console can run on a monitored database.

2. Edit the whitelist file to limit the commands that can be run on a specific Agent system. Standard XML comments can be added (<https://www.w3.org/TR/REC-xml/#sec-comments>). Note that the whitelist file interprets queries literally and wildcard characters are not supported.
3. Save the file to this location on each delegated TE Agent system that is used to monitor database nodes:

```
<te_root>/agent/data/agent/sql-whitelist.xml
```

Note The whitelist file must have the filename (case-sensitive) and location specified above.
--

4. (Optional) To require this TE Agent to always use a query whitelist to validate database queries (see [Table 98 on the previous page](#)), follow these steps:
 - a. Open the Agent properties file with a text editor. By default, the Agent properties file is located at `<te_root>/agent/data/config/agent.properties`.
 - b. Add the following line to the Agent properties file:

```
tw.agent.exec.requireWhitelist=true
```

Notes This setting cannot be accessed from the Tripwire Enterprise Console; it must be set by editing the Agent configuration file directly. If you edit a node to require a query whitelist and that node is also used to run command rules, a standard whitelist (see Restricting Commands on Agent Nodes with Whitelists on page 424) will also be required to run commands on that node.

- c. Save and close the file.
5. If you edited the Agent properties file, restart the TE Agent service to apply those changes. Individual Agents can be restarted from the command line, or multiple Agents can be restarted from the Node Manager in the TE Console. For more information, see:
 - *Managing the Tripwire Enterprise Agent Service* in the *Tripwire Enterprise Installation & Maintenance Guide*
 - [Restarting Tripwire Enterprise Agents on page 412](#)

Chapter 7. Rule Procedures

Viewing and Changing Objects in the Rule Manager

Viewing Rules and Rule Groups

To view rules and rule groups in the Rule Manager:

1. In the Manager bar, click **RULES**.
2. In the tree pane, select a rule group.
3. In the main pane, review the rule group's contents in the Rule Manager table (see [Figure 28](#)). [Table 99 on the next page](#) defines each of the columns in the Rule Manager table.
 - To **sort** the contents of the Rule Manager table by the values in a column, click the column header. To reverse the order, click the column header a second time.
 - If the Rule Manager contains multiple pages, use the navigation controls at the bottom of the Rule Manager to **scroll** through the pages.
 - To change the **table page size** setting, see [Changing User Preference Settings on page 262](#).

Figure 28. The Rule Manager

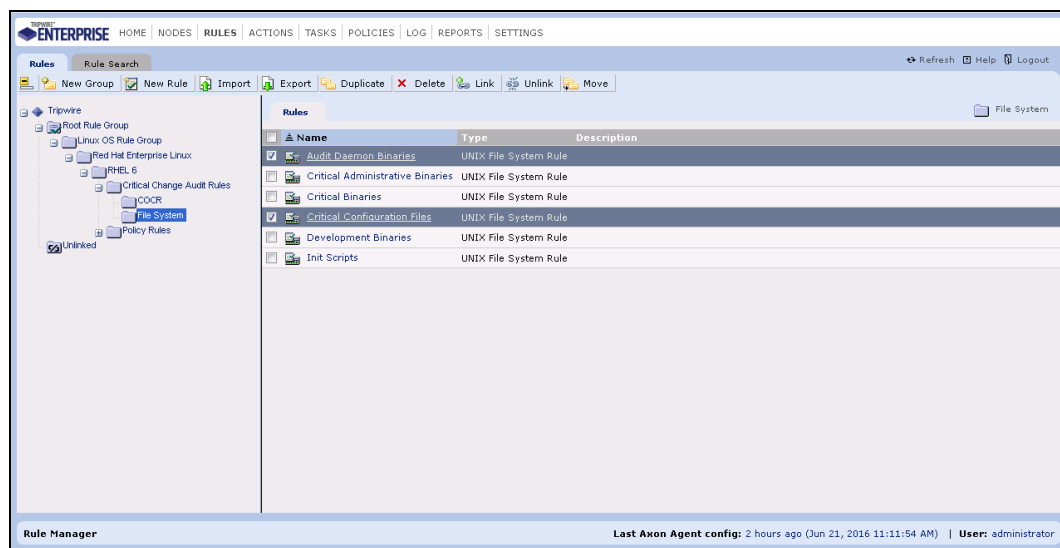


Table 99. Columns in the Rule Manager table


Column	Description
Name	<p>This column lists the names of rules and rule groups.</p> <p>To view the properties of a rule or rule group, click a Name link. For more information, see:</p> <ul style="list-style-type: none">• Changing the Properties of a Rule (on page 437)• Changing the Properties of a Rule Group (on page 440)
Type	<p>This column identifies the type of each Rule Manager entry.</p> <ul style="list-style-type: none">• Rule. For rules, the Type column identifies the type of rule (see What are Rule Types? on page 79).• Rule Group
Description	<p>This column provides a description of each rule or rule group. Descriptions are optional.</p> <p>To add or edit descriptions, see:</p> <ul style="list-style-type: none">• Changing the Properties of a Rule (on page 437)• Changing the Properties of a Rule Group (on page 440)

Searching for Rules

Notes For an introduction to common search features such as wildcards, text-field qualifiers, and saved searches, see [How Do I Run a Search? on page 232](#).


In the Rule Search tab, the button bar contains many of the same buttons available in the Rules tab. To use these buttons, refer to the procedures in [Chapter 7: Rule Procedures \(on page 431\)](#).

To search for rules:

1. In the Manager bar, click **RULES**.
2. Select the **Rule Search** tab.
3. From the **Type** list, select (**any rule**) or a specific rule type. The available search fields vary by rule type. For rule type definitions, see [What are Rule Types? on page 79](#).
4. Enter additional search criteria. For guidance, see [Table 100 on the next page](#).
 - Some of the search criteria are based on values that can be edited in rule property dialogs (see [Changing the Properties of a Rule on page 437](#)).
 - All text-field entries are case-insensitive. For example, ‘Rule’ and ‘rule’ will return the same results.
 - Any string may be entered in a text field. For example, if you enter a string in the **Name** field, and select **Contains** as the text-field qualifier, search results will include any rule with a name that includes the string.
5. Click  **Search**

Next If desired, you can save the entered search criteria for future use. For instructions, see [Creating a Saved Search on page 234](#).

Table 100. Rule search criteria

Search Criteria	To limit search results to ...
Access lists	<p>... rules that apply to all CiscoIOS access lists, select All.</p> <p>... rules that apply to specific CiscoIOS access lists, select Name.</p>
Access list name	<p>... rules that identify CiscoIOS access lists that have specific names:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial name in the text field.
Cat file content?	<p>... VMware ESX file rules that use the `cat` command as a file-transfer technique.</p> <p>Note: VMware ESX file rules are network device rules that identify files on VMware ESX host machines. For more information, see Table 10 on page 52.</p>
Check Point installation base directory	<p>... rules that identify specific installation base directories for Check Point files:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial directory path in the text field.
Check Point installation shared directory	<p>... rules that identify specific installation shared directories for Check Point files:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial directory path in the text field.
Commands to capture	<p>... COVRs with specified, user-entered text in the Commands to capture field:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a search string in the text field.
Descends from rule group	<p>... rules that descend from a specific rule group:</p> <ol style="list-style-type: none"> 1. Click  Chooser. 2. Select the rule group and click OK.
Description	<p>... rules with specific descriptions:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial description in the text field.
Element name	<p>... COVRs that use a specified value to name the elements created by the rule:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial element name in the text field.
Filenames	<p>... rules that check files with specified names:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial file name in the text field.

Search Criteria	To limit search results to ...
Initial baseline	<p>... COVRs with specified, baseline-output text entered in the Initial baseline field:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a search string in the text field.
ISS installation base directory	<p>... rules that identify specified installation base directories for ISS files:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial directory name in the text field.
Line inclusion pattern	<p>... COVRs with a selection method of Include lines containing:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a search string in the text field.
Name	<p>... rules with specific names:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial rule name in the text field.
Paths to files	<p>... rules that identify specific paths to system files:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial path in the text field.
Post-commands	<p>... COVRs with specified, user-entered text in the Post-commands field:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a search string in the text field.
Pre-commands	<p>... COVRs with specified, user-entered text in the Pre-commands field:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a search string in the text field.
RealSecure installation base directory	<p>... rules that identify specific installation base directories for RealSecure files:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial directory path in the text field.
Replacement string	<p>... COVRs with a specific string or variable entered in the Replacement string field:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a search string in the text field.
Search pattern	<p>... COVRs with a specific regular expression entered in the Search pattern field:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a search string in the text field.


Search Criteria	To limit search results to ...
Selection method	... COVRs with a specific selection method, select one of the following options: <ul style="list-style-type: none"> • Include lines containing • Include text matched by
Test login?	... status check rules that direct Tripwire Enterprise to log in to monitored systems when the rule is run, select Yes .
Text inclusion pattern	... COVRs with a specific pattern entered for the Include text matched by selection method: <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a search string in the text field.
Type	... rules of a specific type, select a type from the drop-down list. Otherwise, accept the default value (any rule).

Changing the Properties of a Rule

For an introduction to rules, see [What are Rule Types?](#) on page 79.

To change the properties of a rule:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group containing the rule.
3. In the main pane, select the rule in the **Name** column.
4. As needed, modify the tabs in the rule properties dialog (see [Table 101](#)).

Tips For more information, click  **Help** in any tab.

5. Click **OK**.

Note If you make a change in the Specifiers tab or Real-Time tab of a rule used to monitor an Agent node that uses the Event Generator as the audit-event source, the TE Server notifies the Agent system of the change.

Table 101. Tabs in rule properties

Tab	Available with ...	Description
Actions	... all rules	Specifies the actions to be run if the rule identifies a changed monitored object for which TE creates a change version.
Advanced	... COVRs	Limits the rule to a specific type of network device node. Note: If this tab specifies a node type, the rule cannot be used to baseline or version check other types of nodes.
Baseline	... COVRs	Defines content that TE will save in any baseline versions created by the rule. TE saves this content, rather than the command output generated by the rule. If this tab is blank, TE will save the generated output in each baseline version. Tip: To ensure the integrity of baseline text, you can copy-and-paste generated output that is in a known-good state.
Command	... COVRs, COCRs, COHRs, and log transfer rules	For a COVR, COCR, or COHR, defines the commands to be run when TE uses the rule to baseline or version check a monitored system. For a log transfer rule, defines the commands to query the contents of one or more files on TE Agents.
Dependent Tests	... all rules	Lists the policy tests to which the rule is assigned. Note: This tab includes some of the same buttons that appear in the Policy Manager. For guidance in using these buttons, refer to the following procedures in Chapter 10: Policy Procedures (on page 529) : <ul style="list-style-type: none">• Exporting Policy Manager Objects (on page 573)• Creating a TE Policy (on page 543)• Changing the Properties of a Policy Test Group (on page 538)• Changing the List of Excluded Nodes for Multiple Policy Tests (on page 540)• Linking Policy Manager Objects (on page 571)
Filter	... COVRs, COCRs, and log transfer rules	For a COVR or COCR, specifies content in command output to be removed or replaced when TE saves the content in a new element version (see Changing Filter or Search-and-Replace Criteria for a COVR or COCR on page 442). For a log transfer rule, specifies content in command output to be removed or replaced before forwarding output to TLC.
General	... all rules	Specifies the rule's name and description (optional), and applies or removes a Tracking Identifier to/from the rule (see What are Tracking Identifiers? on page 223). In some cases, this tab also includes additional properties, such as severity levels for network device rules, COCRs, and VI rules.


Tab	Available with ...	Description
Options	<ul style="list-style-type: none"> • Status check rules • Some configuration file rules 	<p>In a status check rule, this tab contains a setting that directs TE to log in to a monitored system when the rule is used to baseline or version check the system. If this setting is disabled, TE simply verifies that the device is listening on the connection-method port specified in the properties of the device's node.</p> <p>In a configuration file rule, defines the list of files and directories identified by the rule (see Changing the List of Monitored Objects in a File Rule or Configuration File Rule on page 441).</p>
Parent Groups	... all rules	<p>Displays the full path of each rule group to which the rule is linked.</p> <ul style="list-style-type: none"> • This tab includes some of the same buttons that appear in the Rule Manager. For guidance in using these buttons, refer to the corresponding procedure in this chapter. • To view or edit the properties of a rule group, select the group's link. (For more information, see Changing the Properties of a Rule Group on the next page.)
Real-Time	... Windows file system rules and registry rules.	Enables real-time monitoring for the rule. For more information, see How Does Real-Time Monitoring Work? on page 70 .
Queries	... database query rules	Contains any queries that have been defined for the rule (see Adding a Query to a Database Query Rule on page 470).
Security	... all rules	Contains any access controls that have been created for the rule. For more information, see Working with Rule Access Controls on page 443 .
Selection	... COVRs	Specifies command-output content to be baselined or version checked by the rule. For definitions of regular expressions that can be entered in this tab, see Table 34 on page 108 .
Server	... log transfer rules	Specifies the hostname (or IP address) and communication port for SFTP, along with the authentication credentials to be used by the log transfer rule when communicating with TLC.
Specifiers	<ul style="list-style-type: none"> • Database metadata rules • Directory rules • File system rules • RSoP rules • Windows registry rules 	<p>Contains the start points, stop points, and/or RSoP specifiers that have been defined for the rule. See:</p> <ul style="list-style-type: none"> • About Start Points and Stop Points (on page 461) • Adding a Specifier to a Windows RSoP Rule (on page 472)

Changing the Properties of a Rule Group

Tip This procedure explains how to change the properties of a rule group displayed in the main pane of the Rule Manager. However, you can also change the properties of a rule group in the **Parent Groups** tab of a rule properties dialog (see [Changing the Properties of a Rule on page 437](#)) or rule group properties dialog (accessed below).

To view the properties of a rule group:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the group containing the rule group.
3. In the main pane, select the rule group in the **Name** column.
4. As needed, modify the tabs in the rule group properties dialog. For tab descriptions, see [Table 102](#).

Tip For more information, click  **Help** in any tab.

5. Click **OK**.

Table 102. Tabs in rule group properties

Tab	Description
General	Specifies the group's name and description (optional), and applies or removes a Tracking Identifier to/from the group (see What are Tracking Identifiers? on page 223).
Security	Contains any access controls that have been created for the rule group. For more information, see Working with Rule Access Controls on page 443 .
Parent Groups	Displays the full path of each rule group to which this rule group is linked. <ul style="list-style-type: none">• This tab includes some of the same buttons that appear in the Rule Manager. For guidance in using these buttons, refer to the corresponding procedure in this chapter.• To view or edit the properties of a rule group, select the group's link.


Changing the List of Monitored Objects in a File Rule or Configuration File Rule

With this procedure, you can modify the list of files and directories identified by the following types of rules:

- F5 BigIP configuration rules
- All Nokia configuration rules
- File rules

To change the list of files and directories:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group containing the rule.
3. In the main pane, select the rule in the **Name** column.
4. In the rule properties dialog, select the **Options** tab.
5. (Applicable to some Nokia rules only) If appropriate, edit the path of the installation base directory.
6. Modify the list and click **OK**.
 - **To add a file**, insert the path and file name on a separate line.
 - **To add a directory**, insert the path and directory name on a separate line.
 - **To remove a file or directory**, delete the entire line.

Tips For field definitions, click  **Help**.

If the rule has an installation base directory, begin each file and directory entry with the variable defined for the base directory.

Next If you removed files or directories from the rule, you can now delete the corresponding elements in Tripwire Enterprise. For instructions, see [Deleting Elements on page 378](#).

If you added files or directories to the rule, or modified the installation base directory location, you should initialize baselines for all related monitored objects. For instructions, see [Initial Baselineing of Monitored Objects on page 382](#).

Changing Filter or Search-and-Replace Criteria for a COVR or COCR

With this procedure, you can enter criteria in a COVR or COCR that will either:

- Filter (remove) specified content from command output generated by the rule.
- Replace specified command-output content with a variable or text.

For more information, see:

- [How Does a Command Output Capture Rule \(COCR\) Work? \(on page 99\)](#)
- [How Does a Command Output Validation Rule \(COVR\) Work? \(on page 103\)](#)

To modify the filter or search-and-replace criteria for a rule:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group containing the rule.
3. Select the rule in the **Name** column.
4. In the rule properties dialog, select the **Filter** tab.
5. To filter command output:
 - a. In the **Search pattern** field, enter a regular expression(s) to specify the content to be removed. (For definitions of regular-expression characters, see [Table 34 on page 108.](#))
 - b. Leave the **Replacement string** field blank and click **OK**.

To replace command output:

- a. In the **Search pattern** field, enter a regular expression to specify the string(s) to be replaced.
- b. In the **Replacement string** field, enter the text or variable to be inserted in place of the **Search pattern**.

Note	To enter a variable in the Replacement string field for a COVR, use the \$n format. For more information, see Advanced Search-and-Replace with Variables on page 109.
-------------	--

- c. Click **OK**.


Working with Rule Access Controls

Creating an Access Control for a Rule or Rule Group

For an introduction to access controls, see [What are Access Controls? on page 208](#).

Note If one or more access controls have already been created for the rule or rule group, an additional access control can only be created by the default administrator account or a user account assigned to one of the existing access controls.

To set an access control for a rule or rule group:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the group containing the rule or rule group.
3. In the main pane, click the rule or rule group in the **Name** column.
4. In the properties dialog, click the **Security** tab.
5. Click  **Add Control**.
6. Select the check box of each **Principal** (user or user group) to be assigned to the access control and click **Next**.
7. Select the user role for the access control and click **Finish**.

Changing an Access Control for a Rule or Rule Group

For an introduction to access controls, see [What are Access Controls? on page 208](#).

Note An access control can only be changed by the default administrator account or a user account assigned to the control.

To change the user role assigned to an access control:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the group containing the rule or rule group associated with the access control.
3. In the main pane, click the rule or rule group in the **Name** column.
4. In the properties dialog, click the **Security** tab.
5. In the **Access Control** column, select the access control.
6. In the Access Control dialog, select the new user role and click **OK**.

Deleting Access Controls for a Rule or Rule Group

Note An access control can only be deleted by the default administrator account or a user account assigned to the control.

Caution With an access control, non-Administrators may be granted Administrator-level access to a particular node or node group. If the access control is deleted, the user will no longer be able to modify the properties of the rule or rule group.

To delete an access control from a rule or rule group:


1. In the Manager bar, click **RULES**.
2. In the tree pane, click the group containing the rule or rule group associated with the access control.
3. In the main pane, click the rule or rule group in the **Name** column.
4. In the properties dialog, select the **Security** tab.
5. Select the check box of each access control to be deleted.
6. Click **✖ Delete**.
7. Click **OK** to confirm.

Creating and Deleting Objects in the Rule Manager

Creating a Rule Group

For an introduction to rule groups, see [About Groups](#) on page 29.

To create a rule group:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group in which to create the new rule group.
3. Click  **New Group**.
4. In the New Rule Group Wizard, enter a **Name** and **Description** (optional) for the new rule group.
5. Click **Finish**.


Next To add existing rules and rule groups to the new group, see:


- [Moving Rules and Rule Groups](#) (on page 473)
- [Linking Rules and Rule Groups](#) (on page 473)

Creating a Command Output Capture Rule

For an introduction to command output capture rules, see [How Does a Command Output Capture Rule \(COCR\) Work?](#) on page 99.

To create a command output capture rule:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group in which the new rule will be created.
3. Click  **New Rule**.
4. In the Create Rule dialog, select **File Server > Command Output Capture Rule** and click **OK**.
5. Complete the New Rule Wizard.

Tips For field descriptions, click  **Help** in any wizard page.

When entering the **Command Line**, you should verify that the command is compatible with the shell that will be invoked on monitored systems. On a UNIX system, `/bin/sh` is invoked; on a Windows system, `cmd.exe` is invoked.

Next To add the rule to an existing rule task, see [Changing the Properties of a Task on page 512](#).


To create a new rule task, see:


- [Creating a Baseline Rule Task \(on page 517\)](#)
- [Creating a Check Rule Task \(on page 518\)](#)

Creating a Command Output Hypervisor Rule

For an introduction to command output hypervisor rules (COHR), see [Table 24 on page 82](#).

To create a COHR:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group in which the new rule will be created.
3. Click  **New Rule**.
4. In the Create Rule dialog, select a type of COHR (for example, a VMware ESXi Service Console Rule) from the **Virtual Infrastructure** folder and click **OK**.
5. Complete the New Rule Wizard.

Tips For field descriptions, click  **Help** in any wizard page.

In the **Commands** field, you should only enter commands that are compatible with the shell (`/bin/sh`) invoked by COHRs on hypervisor host machines.

Next To add the rule to an existing rule task, see [Changing the Properties of a Task on page 512](#).

To create a new rule task, see:


- [Creating a Baseline Rule Task \(on page 517\)](#)
- [Creating a Check Rule Task \(on page 518\)](#)

Creating a Command Output Validation Rule

For an introduction to COVRs, see [How Does a Command Output Validation Rule \(COVR\) Work? on page 103](#).

To create a COVR:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group in which the new rule will be created.

3. Click  **New Rule**.
4. Select **Network Device > Common > Command Output Validation Rule** and click **OK**.
5. Complete the New Rule Wizard.

Tip For more information, click  **Help**.

For definitions of regular-expression characters that may be entered in the **Selection method** wizard page, see [Table 34 on page 108](#).

Next To add the rule to an existing rule task, see [Changing the Properties of a Task on page 512](#).


To create a new rule task, see:

- [Creating a Baseline Rule Task \(on page 517\)](#)
- [Creating a Check Rule Task \(on page 518\)](#)

Creating a Configuration File Rule

A configuration file rule identifies configuration files on a specific type of network device. Each configuration file rule applies only to a specific type of device produced by a single vendor. For example, a Cisco IOS configuration file rule can only check Cisco IOS routers and switches for changes.

To create a configuration file rule:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group in which the new rule will be created.
3. Click  **New Rule**.
4. In the Create Rule dialog, select **Network Device > Configuration File Rules**. Then, select a rule type and click **OK**.
5. Complete the New Rule Wizard.

Tip For more information, click  **Help**.

Next To add the rule to an existing rule task, see [Changing the Properties of a Task on page 512](#).


To create a new rule task, see:


- [Creating a Baseline Rule Task \(on page 517\)](#)
- [Creating a Check Rule Task \(on page 518\)](#)


Creating a Database Metadata Rule

For an introduction to database metadata rules, see [How Does a Database Metadata Rule Work?](#) on page 89.

To create a database metadata rule:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group in which to create the new rule.
3. Click  **New Rule**.
4. In the Create Rule dialog, select a type of database metadata rule from the **Database Server** folder and click **OK**.
5. In the New Rule Wizard, enter a **Name** and **Description** (optional). Then, click **Next**.
6. Add all desired **start points**. For instructions, see [Adding a Start Point to a Rule](#) on page 462.
7. (Optional) Add all desired **stop points**. For instructions, see [Adding a Stop Point to a Rule](#) on page 467.

Tips For field and column definitions, click  **Help**.

To remove a start point or stop point, select the check box for the point and click  **Delete**.

8. If the Database Server Browser is open, close it.
9. In the New Rule Wizard, click **Next**.
10. Select the actions to be associated with the rule and click **Finish**.

Next To add the rule to an existing rule task, see [Changing the Properties of a Task](#) on page 512.



To create a new rule task, see:

- [Creating a Baseline Rule Task](#) (on page 517)
- [Creating a Check Rule Task](#) (on page 518)

Creating a Database Query Rule

For an introduction to database query rules, see [How Does a Database Query Rule Work?](#) on page 92.

To create a database query rule:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group in which to create the new rule.
3. Click  **New Rule**.
4. In the Create Rule dialog, select **Database Server > Query Rule** and click **OK**.
5. In the New Rule Wizard, enter a **Name** and **Description** (optional). Then, click **Next**.
6. To add a query to the rule:
 - a. Click  **New Query**.
 - b. In the New Query Wizard, enter the query properties and click **Next**.
 - c. In the **Query** field, enter the query string and click **Next**.

Tips For more information, click  **Help**.

To ensure that query results are always saved in the same order, add an **ORDER BY** clause to the end of the query. Without an **ORDER BY** clause, the sequence of query rows may vary between version checks run with the rule. If a version check detects a change in the row sequence, Tripwire Enterprise creates a new change version, even if the content of the database is identical to the baseline.

- d. Select or create a criteria set, and click **Next**.

To create a new criteria set, click  **New Criteria Set** or  **New From Selected**. For further instructions, see [Creating a Criteria Set for a Database Rule](#) (on page 307).

7. To add additional queries to the rule, repeat [step 6](#) above. Once all queries have been added, click **Next**.
8. Select the actions to be associated with the rule.
9. Click **Finish**.

Next To add the rule to an existing rule task, see [Changing the Properties of a Task](#) on page 512.

To create a new rule task, see:

- [Creating a Baseline Rule Task](#) (on page 517)
- [Creating a Check Rule Task](#) (on page 518)

Creating a Directory Rule


With this procedure, you can create the following types of directory rules:



- LDAP rules
- Active Directory rules

For an introduction to directory rules, see [How Does a Directory Rule Work?](#) on page 93.

Notes For your convenience, Tripwire provides a collection of default directory rules on the Tripwire Web site. For more information, see [What are Pre-Configured Rules and Policies?](#) on page 219.

To create a directory rule:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group in which the new rule will be created.
3. Click  **New Rule**.
4. In the Create Rule dialog, select a directory rule type from the **Directory Server** folder and click **OK**.
5. In the New Rule Wizard, enter a **Name** and **Description** (optional). Then, click **Next**.
6. Add all desired **start points**. For instructions, see [Adding a Start Point to a Rule](#) on page 462.
7. (Optional) Add all desired **stop points**. For instructions, see [Adding a Stop Point to a Rule](#) on page 467.

Tips For field and column definitions, click  **Help**.
To remove a start point or stop point, select the check box for the point and click  **Delete**.

8. If the Directory Server Browser is open, close it.
9. In the New Rule Wizard, click **Next**.
10. Select the actions to be associated with the rule and click **Finish**.


Next To add the rule to an existing rule task, see [Changing the Properties of a Task](#) on page 512. To create a new rule task, see:

- [Creating a Baseline Rule Task](#) (on page 517)
- [Creating a Check Rule Task](#) (on page 518)

Creating a File Rule

File rules include UNIX file rules and custom file rules. For more information, see [Table 21 on page 80](#).

To create a file rule:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group in which the new rule will be created.
3. Click  **New Rule**.
4. In the Create Rule dialog, select a file rule type in **Network Device > File Rules** and click **OK**.
5. Complete the New Rule Wizard.

Tip For more information, click  **Help**.

Next To add the rule to an existing rule task, see [Changing the Properties of a Task on page 512](#).

To create a new rule task, see:


- [Creating a Baseline Rule Task \(on page 517\)](#)
- [Creating a Check Rule Task \(on page 518\)](#)


Creating a Log Transfer Rule

For an introduction to log transfer rules, see [How Does a Log Transfer Rule Work? on page 98](#).

Note Log transfer rules cannot be used with Axon Agents.

To create a log transfer rule:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group in which the new rule will be created.
3. Click  **New Rule**.
4. In the Create Rule dialog, select **File Server > Log Transfer Rule** and click **OK**.
5. Complete the New Rule Wizard.

Tips For field descriptions, click  **Help** in any wizard page.

When entering the **Command Line**, you should verify that the command is compatible with the shell that will be invoked on monitored systems. On a UNIX system, /bin/sh is invoked; on a Windows system, cmd.exe is invoked.

Next To add the rule to an existing rule task, see [Changing the Properties of a Task on page 512](#).


To create a new rule task, see:

- [Creating a Baseline Rule Task \(on page 517\)](#)
- [Creating a Check Rule Task \(on page 518\)](#)

Creating a Status Check Rule

A status check rule determines the availability of a network device (in other words, whether or not the Tripwire Enterprise Server can access and communicate with the system).

To create a status check rule:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group in which the new rule will be created.
3. Click  **New Rule**.
4. In the Create Rule dialog, select **Network Device > Common > Status Check Rule** and click **OK**.
5. Complete the New Rule Wizard.

Tip For more information, click  **Help**.

Next To add the rule to an existing rule task, see [Changing the Properties of a Task on page 512](#).


To create a new rule task, see:

- [Creating a Baseline Rule Task \(on page 517\)](#)
- [Creating a Check Rule Task \(on page 518\)](#)

Creating a VI Hypervisor Rule

For an introduction to VI hypervisor rules, see [Table 24 on page 82](#).

To create a VI hypervisor rule:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group in which the new rule will be created.
3. Click  **New Rule**.
4. In the Create Rule dialog, select a type of VI hypervisor rule (for example, a VMware ESXi Rule) from the **Virtual Infrastructure** folder and click **OK**.
5. Complete the New Rule Wizard.

Tip For more information, click  **Help**.

Next To add the rule to an existing rule task, see [Changing the Properties of a Task on page 512](#).


To create a new rule task, see:

- [Creating a Baseline Rule Task \(on page 517\)](#)
- [Creating a Check Rule Task \(on page 518\)](#)

Creating a Virtual Machine Configuration Rule

For an introduction to virtual machine configuration rules, see [Table 24 on page 82](#).

To create a virtual machine configuration rule:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group in which the new rule will be created.
3. Click  **New Rule**.
4. In the Create Rule dialog, select a type of virtual machine configuration rule (for example, VMware VM Rule) from the **Virtual Infrastructure** folder and click **OK**.
5. Complete the New Rule Wizard.

Tip For more information, click  **Help**.

Next To add the rule to an existing rule task, see [Changing the Properties of a Task on page 512](#).


To create a new rule task, see:

- [Creating a Baseline Rule Task \(on page 517\)](#)
- [Creating a Check Rule Task \(on page 518\)](#)

Creating a Virtual Switch Configuration Rule

For an introduction to virtual switch configuration rules, see [Table 24 on page 82](#).

To create a virtual switch configuration rule:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group in which the new rule will be created.
3. Click  **New Rule**.
4. In the Create Rule dialog, select a type of virtual switch configuration rule (for example, VMware vSwitch Rule) from the **Virtual Infrastructure** folder and click **OK**.
5. Complete the New Rule Wizard.

Tip For more information, click  **Help**.

Next To add the rule to an existing rule task, see [Changing the Properties of a Task on page 512](#).


To create a new rule task, see:

- [Creating a Baseline Rule Task \(on page 517\)](#)
- [Creating a Check Rule Task \(on page 518\)](#)

Creating a Distributed Virtual Switch Configuration Rule

For an introduction to distributed virtual switch configuration rules, see [Table 24 on page 82](#).

To create a virtual switch configuration rule:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group in which the new rule will be created.
3. Click  **New Rule**.
4. In the Create Rule dialog, select a type of distributed virtual switch configuration rule (for example, VMware vNetwork Distributed Switch Rule) from the **Virtual Infrastructure** folder and click **OK**.
5. Complete the New Rule Wizard.

Tip For more information, click  **Help**.

Next To add the rule to an existing rule task, see [Changing the Properties of a Task on page 512](#).

To create a new rule task, see:

- [Creating a Baseline Rule Task \(on page 517\)](#)
- [Creating a Check Rule Task \(on page 518\)](#)

Creating a File System Rule


Follow the steps below to create an Windows or UNIX file system rule. For an introduction to file system rules, see [How Does a File System Rule Work? on page 83](#).


Tips For your convenience, Tripwire provides a collection of pre-configured file system rules on the Tripwire Web site. For more information, see [What are Pre-Configured Rules and Policies? on page 219](#).


To optimize system performance, you should avoid using a single file system rule to monitor an entire file system. Instead, Tripwire recommends the use of multiple file system rules that identify different monitored objects. By doing so, you can significantly reduce the amount of bandwidth and memory required to baseline or version check file systems.

To create a file system rule:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group in which the new rule will be created.

3. Click  **New Rule**.
4. In the **File Server** folder of the Create Rule dialog, select the type of file system rule and click **OK**.
5. In the New Rule Wizard:
 - a. Enter a **Name** and **Description** (optional).
 - b. (UNIX file system rules only) To direct Tripwire Enterprise to cross file system mount points during version checks run with the rule, select **Traverse mount points** (optional).
 - c. Click **Next**.
6. Add all desired **start points**. For instructions, see [Adding a Start Point to a Rule on page 462](#).
7. (Optional) Add all desired **stop points**. For instructions, see [Adding a Stop Point to a Rule on page 467](#).

Tips For field and column definitions, click  **Help**.

To remove a start point or stop point, select the check box for the point and click  **Delete**.

8. If the File System Browser is open, close it.
9. Complete the remaining wizard pages and click **Finish**.

Next To add the rule to an existing rule task, see [Changing the Properties of a Task on page 512](#).

To create a new rule task, see:

- [Creating a Baseline Rule Task \(on page 517\)](#)
- [Creating a Check Rule Task \(on page 518\)](#)


Creating a Windows Registry Rule


For an introduction to Windows registry rules, see [How Does a Windows Registry Rule Work?](#) on page 85.


Tips For your convenience, Tripwire provides a collection of Windows registry rules on the Tripwire Web site. For more information, see [What are Pre-Configured Rules and Policies?](#) on page 219.

To optimize system performance, you should avoid using a single Windows registry rule to monitor an entire registry. Instead, Tripwire recommends the use of multiple Windows registry rules that identify different keys and entries. By using multiple rules (as opposed to a single rule), you can significantly reduce the amount of bandwidth and memory required to baseline or version check a registry.

To create a Windows registry rule:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group in which the new rule will be created.
3. Click  **New Rule**.
4. In the Create Rule dialog, select **File Server > Windows Registry Rule** and click **OK**.
5. In the New Rule Wizard, enter a **Name** and **Description** (optional). Then, click **Next**.
6. Add all desired **start points**. For instructions, see [Adding a Start Point to a Rule](#) on page 462.
7. (Optional) Add all desired **stop points**. For instructions, see [Adding a Stop Point to a Rule](#) on page 467.

Tips For field and column definitions, click  **Help**.

To remove a start point or stop point, select the check box for the point and click  **Delete**.

8. If the Windows Registry Browser is open, close it.
9. Complete the remaining wizard pages and click **Finish**.

Next To add the rule to an existing rule task, see [Changing the Properties of a Task](#) on page 512.



To create a new rule task, see:

- [Creating a Baseline Rule Task](#) (on page 517)
- [Creating a Check Rule Task](#) (on page 518)

Creating a Windows RSoP Rule

For an introduction to Windows RSoP rules, see [How Does a Windows RSoP Rule Work? on page 88](#).

To create a Windows RSoP rule:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group in which to create the new rule.
3. Click  **New Rule**.
4. In the Create Rule dialog, select **File Server > Windows RSoP Rule** and click **OK**.
5. In the New Rule Wizard, enter a **Name** and **Description** (optional). Then, click **Next**.
6. To add a specifier to the rule:
 - a. Click  **New Specifier**.
 - b. In the New RSoP Specifier Wizard, enter the specifier properties and click **Next**.
 - c. Select or create a criteria set, and click **Finish**.

To create a new criteria set, click  **New Criteria Set** or  **New From Selected**. For further instructions, see [Creating a Criteria Set for a Windows RSoP Rule \(on page 306\)](#).

7. To add additional specifiers to the rule, repeat [step 6](#) above.
Once all specifiers have been added, click **Next**.
8. Select the actions to be associated with the rule.
9. Click **Finish**.

Next To add the rule to an existing rule task, see [Changing the Properties of a Task on page 512](#).


To create a new rule task, see:

- [Creating a Baseline Rule Task \(on page 517\)](#)
- [Creating a Check Rule Task \(on page 518\)](#)

Duplicating Rules

With this procedure, you can either duplicate specified rules in a selected rule group, or all rules in a selected rule group.

To create a copy of existing rule(s):

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group containing the rule(s) to be duplicated.
3. (Optional) To duplicate specific rules, select the check box of each rule.
4. Click  **Duplicate**.
5. Click **OK** in the confirmation dialog.

Tripwire Enterprise uses the following convention to name a duplicate rule:

```
<original rule>(<#>)
```

where:

<original rule> is the name of the rule that was duplicated.

<#> is a number that increments each time the original rule is duplicated (beginning with 1) - for example, rule(1), rule(2), etc.

Deleting Rules and Rule Groups

This procedure permanently deletes all instances of selected rules and/or rule groups. To remove a rule or rule group from a group *without* deletion, see [Unlinking Rules and Rule Groups on page 474](#).

Caution When a rule is deleted, Tripwire Enterprise deletes the elements and element versions previously created by the rule. In addition, when a rule or rule group is deleted, TE deletes any baseline rule tasks or check rule tasks to which the object is directly assigned. However, if a deleted rule or rule group is in another rule group that is assigned to a rule task, TE does not delete the task.

Note To delete an object, your user account must have Delete permissions for that object, and (for groups) all objects descended from that object. For more information, see [What are User Permissions and User Roles? on page 204](#).

To delete rules and/or rule groups:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group containing the objects to be deleted.
3. Select the check box for each object to be deleted.

4. Click **✖ Delete**.
5. Specify whether or not to run the Clear Unlinked Groups task on all Unlinked groups in TE. For more information on this task, see [What are Task Types? on page 127](#).
6. Click **OK**.

Note If you get an error message when trying to delete objects, an access control (see [What are Access Controls? on page 208](#)) is preventing you from deleting a descendant object. To determine which objects have access controls, check the Objects tab for the Error log message associated with this operation.

Working with Start Points, Stop Points, Queries, and RSoP Specifiers

About Start Points and Stop Points

A **start point** is a component of a rule that identifies a monitored object to be baselined or version checked by the rule. A **stop point** is a rule component that identifies a monitored object to be excluded from baseline operations and version checks run with the rule.

Table 103 lists the types of rules to which start points and stop points may be added. For each rule type, Table 103 also identifies the type of monitored object represented by a start point or stop point.

Table 103. Monitored objects identified by start points and stop points

Rule Type	A start point or stop point identifies a(n) ...
Database metadata rules	... a database object For an introduction to database metadata rules, see How Does a Database Metadata Rule Work? (on page 89) .
Directory rules	... entry. For an introduction to directory rules, see How Does a Directory Rule Work? on page 93 .
File system rules	... directory or file in a Windows or UNIX file system. For an introduction to file system rules, see How Does a File System Rule Work? on page 83 .
Windows registry rules	... registry key or registry entry. For an introduction to Windows registry rules, see How Does a Windows Registry Rule Work? on page 85 .

To modify the start points and stop points associated with a rule, see:

- [Adding a Start Point to a Rule \(on the next page\)](#)
- [Changing or Deleting Start Points \(on page 466\)](#)
- [Adding a Stop Point to a Rule \(on page 467\)](#)
- [Changing or Deleting Stop Points \(on page 469\)](#)

Adding a Start Point to a Rule

Note The type of monitored object for which a start point may be created depends upon the type of rule (see [Table 103 on the previous page](#)).

To add a start point to a new or existing rule, complete the applicable steps below.

- *Step 1: Opening the Specifiers Tab below* (Existing rules only)
- *Step 2: Browsing to the Monitored Object below* (Optional)
- *Step 3: Completing the Start Point Wizard on page 464*

Step 1: Opening the Specifiers Tab

To add a start point to an existing rule, you must first open the Specifiers tab in the rule properties dialog:



1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group containing the rule.
3. In the **Name** column, click the rule.
4. In the rule properties dialog, select the **Specifiers** tab.

Step 2: Browsing to the Monitored Object

In this optional step, you can browse to select the start point's monitored object. For a directory rule, you can also filter the selected object (in this case, a directory entry) for specific sub-entries to be identified by the start point.

Note You cannot browse a node with Axon Agent installed. As a workaround, use a TE Agent installed on a similar node to create or edit rules by browsing, then run the rules on the Axon Agent.

To browse to the monitored object:

1. Click  **Browse** in the current dialog (either the Specifiers tab or New Rule Wizard).
2. In the Browser dialog, click  **Select Node**.

Tip Move the Browser dialog so that you can still see the Specifiers tab or New Rule Wizard. Start points will appear in these dialogs as you add them with the Browser.

3. In the Select Node dialog, select the monitored object's node and click **OK**.

4. Complete the appropriate steps below for the rule type.

For a **file system rule**:

- a. In the left pane, select the parent directory or library containing the start point's monitored object.
- b. Select the object in the right pane.

For a **Windows registry rule**:

- To assign a registry key to the start point, select the key in the left pane.
- To assign a registry entry to the start point, select the key in the left pane, and then select the entry in the right pane.

For a **database rule**:



- a. In the left pane, select the type of database object for the start point.
- b. Select the object in the right pane.

For a **directory rule**:

- a. In the left pane, select an entry for the start point.
- b. (Optional) To specify the attributes to be monitored by the start point, select the appropriate check boxes in the right pane.

Tips “(Binary attribute)” indicates a directory attribute that is defined as a binary attribute in the Settings Manager, while “(Security attribute)” indicates an attribute defined as a security attribute. For more information, see [What are Binary Attributes and Security Attributes?](#) on page 97.


A child entry in a directory may have a set of attributes that differs from its parent. However, you can monitor all children of a parent entry with the attributes of a specific child entry. To do so, select the child entry and the desired attributes in the Browser dialog. Then, remove the child entry from the **Distinguished Name** field in [Step 3: Completing the Start Point Wizard](#) on the next page.


5. (Optional; **directory rules** only) To limit the start point to specific children of the selected entry:
 - a. Click  **Search**.
 - b. In the Directory Server Search dialog, enter filtering criteria in the left pane.
 - c. Click  **Search**.
 - d. Repeat the preceding steps until the desired results are displayed in the main pane.

Next Proceed to [Step 3: Completing the Start Point Wizard](#) on the next page.

Step 3: Completing the Start Point Wizard

To open and complete the Start Point Wizard:

1. Click  **New Start Point** in the current dialog (either the Specifiers tab, New Rule Wizard, Browser dialog, or Directory Server Search dialog).
2. In the New Start Point Wizard, enter (or verify) the start point properties and click **Next**.
 - If you selected the start point's monitored object by browsing (see [Step 2: Browsing to the Monitored Object on page 462](#)), previously entered values will appear in the New Start Point Wizard.
 - (Windows registry rules only) For naming conventions used with start points in Windows registry rules, see [About Windows Registry Rules on page 86](#).
 - (File system rules only) If you select the **Archive element content** check box, Tripwire Enterprise will archive the content of a monitored text file if the file's content is smaller than the **Maximum size of archived content** setting in the Settings Manager (see [Setting File System Preferences on page 310](#)).



Tips For field definitions, click  **Help** in any wizard page.

For a file system rule, wildcard characters may be entered in the Path field. The ? wildcard indicates a single character, while the * wildcard represents any number of characters (including zero). However, neither wildcard can be used to indicate a directory separator (such as "/").

3. To complete the New Start Point Wizard, refer to the appropriate steps below for the rule type.

For a file system rule, Windows registry rule, or database rule:

- a. Select or create a criteria set, and click **Next**.

To create a new criteria set, click  **New Criteria Set** or  **New From Selected**. For further instructions, see:

- [Creating a Criteria Set for a File System Rule \(on page 300\)](#)
 - [Creating a Criteria Set for a Windows Registry Rule \(on page 304\)](#)
 - [Creating a Criteria Set for a Database Rule \(on page 307\)](#)
- b. In the **Include** and **Exclude** fields, enter any filters for the start point. (For a file system rule or database rule, these fields support use of the ? and * wildcard characters.)
 - c. Click **Finish**.

For a directory rule:

- a. (Optional) In the **Filter** field, enter filtering criteria to specify the entries to be identified by the start point and click **Next**.
- b. (Optional) In the **Include attributes** and **Exclude attributes** fields, enter the names of directory server attributes to be included or excluded from the start point.

Note To monitor the Group Policy Object referenced by a Group Policy container entry in an Active Directory, the `objectClass` attribute must be included in the **Include attributes** field. In addition, Microsoft's Group Policy Management Console (GPMC) must be installed on the Agent system that hosts the Active Directory. GPMC is available for all supported Windows platforms.

- c. Click **Finish**.

Changing or Deleting Start Points

For an introduction to start points, see [About Start Points and Stop Points on page 461](#).

To change or delete start points in an existing rule:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group containing the rule.
3. In the **Name** column, click the rule.
4. In the rule properties dialog, select the **Specifiers** tab.
5. To delete start points:
 - a. Select the check box of each start point to be deleted.
 - b. Click **✗ Delete**.

To change the properties of a start point:

- a. From the **Path** or **Distinguished Name** column, select the start point to be edited.
- b. In the start point properties dialog, edit the appropriate tabs and click **OK**.

Tip For more information, click  **Help** in any tab.

Next If you changed the list of attributes for a start point, you should run a version check of all monitored objects identified by the rule. For instructions, see:

- [Version Checking Monitored Systems on page 385](#)
- [Version Checking Specific Monitored Objects on page 386](#)

Once done, you should then promote all new change versions created by the version check (see [Promoting All Current Versions for a Node or Node Group on page 395](#)).

Adding a Stop Point to a Rule

Note The type of monitored object for which a stop point may be created depends upon the type of rule (see [Table 103 on page 461](#)).

To add a stop point to a new or existing rule, complete the applicable steps below.

- *Step 1: Opening the Specifiers Tab below* (Existing rules only)
- *Step 2: Browsing to the Monitored Object below* (Optional)
- *Step 3: Completing the Stop Point Wizard on page 469*

Step 1: Opening the Specifiers Tab

To add a stop point to an existing rule, you must first open the **Specifiers** tab in the rule properties dialog:



1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group containing the rule.
3. In the **Name** column, click the rule.
4. In the rule properties dialog, select the **Specifiers** tab.

Step 2: Browsing to the Monitored Object

In this optional step, you can browse to select the stop point's monitored object. For a directory rule, you can also filter the selected object for specific sub-entries to be identified by the stop point.

Note You cannot browse a node with Axon Agent installed. As a workaround, use a TE Agent installed on a similar node to create or edit rules by browsing, then run the rules on the Axon Agent.

To browse to the monitored object:

1. Click  **Browse** in the current dialog (either the Specifiers tab or New Rule Wizard).
2. In the Browser dialog, click  **Select Node**.

Tip Move the Browser dialog so that you can still see the Specifiers tab or New Rule Wizard. Start points will appear in these dialogs as you add them with the Browser.

3. In the Select Node dialog, select the monitored object's node and click **OK**.

4. Complete the appropriate steps below for the rule type.

For a **file system rule**:

- a. In the left pane, select the parent directory or library for the stop point's monitored object.
- b. Select the object in the right pane.

For a **Windows registry rule**:

- To assign a registry key to the stop point, select the key in the left pane.
- To assign a registry entry to the stop point, select the key in the left pane, and then select the entry in the right pane.

For a **database rule**:


- a. In the left pane, select the type of database object for the stop point.
- b. Select the object in the right pane.

For a **directory rule**:


- a. In the left pane, select an entry for the stop point.
- b. (Optional) To specify attributes to be omitted by the stop point, select the appropriate check boxes in the right pane.

Note “(Binary attribute)” indicates a directory attribute that is defined as a binary attribute in the Settings Manager, while “(Security attribute)” indicates an attribute defined as a security attribute. For more information, see [What are Binary Attributes and Security Attributes? on page 97](#).

5. (Optional; **directory rules** only) To limit the stop point to specific children of the selected entry:

- a. Click  **Search**.
- b. In the Directory Server Search dialog, enter filtering criteria in the left pane.


Tip For more information, click  **Help**.

- c. Click  **Search**.
- d. Repeat the two preceding steps until the desired results are displayed in the main pane.


Next Proceed to [Step 3: Completing the Stop Point Wizard on the next page](#).

Step 3: Completing the Stop Point Wizard

To open and complete the Stop Point Wizard:

1. Click  **New Stop Point** in the current dialog (either the New Rule Wizard, Browser dialog, or Directory Server Search dialog).
2. In the New Stop Point Wizard, enter (or verify) the stop point properties.

If you selected the stop point's monitored object by browsing (see [Step 2: Browsing to the Monitored Object on page 467](#)), Tripwire Enterprise automatically populates the **Path**, **Key**, or **Distinguished Name** field in the Stop Point Wizard.


<p>Tip For field definitions, click  Help in any wizard page.</p> <p>For a file system rule or database rule, wildcard characters may be entered in the Path field. The ? wildcard indicates a single character, while the * wildcard represents any number of characters (including zero). However, neither wildcard can be used to indicate a directory separator (such as "/").</p> <p>For naming conventions used with stop points in Windows registry rules, see About Windows Registry Rules on page 86.</p>

3. Click **Finish**.

Changing or Deleting Stop Points

For an introduction to stop points, see [About Start Points and Stop Points on page 461](#).

To change or delete stop points in an existing rule:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group containing the rule.
3. In the **Name** column, click the rule.
4. In the rule properties dialog, select the **Specifiers** tab.
5. To delete stop points:
 - a. Select the check box of each stop point to be deleted.
 - b. Click  **Delete**.

To change the properties of a stop point:


- a. From the **Path** or **Distinguished Name** column, select the stop point to be edited.
- b. In the stop point properties dialog, edit the appropriate tabs and click **OK**.

<p>Tip For more information, click  Help in any tab.</p>

Adding a Query to a Database Query Rule

For an introduction to database query rules, see [How Does a Database Query Rule Work?](#) on page 92.

To add a query to a query rule:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group containing the rule.
3. In the **Name** column, click the rule.
4. In the rule properties dialog, select the **Queries** tab.
5. Click  **New Query**.
6. In the New Query Wizard:
 - a. Enter the query properties and click **Next**.
 - b. In the **Query** field, enter the query string and click **Next**.

Tips For more information, click  **Help**.

To ensure that query results are always saved in the same order, add an **ORDER BY** clause to the end of the query. Without an **ORDER BY** clause, the sequence of query rows may vary between version checks run with the rule. If a version check detects a change in the row sequence, Tripwire Enterprise creates a new change version, even if the content of the database is identical to the baseline.

- c. Select or create a criteria set.

To create a new criteria set, click  **New Criteria Set**. For further instructions, see [Creating a Criteria Set for a Database Rule](#) (on page 307).

- d. Click **Finish**.

Changing or Deleting Queries in a Database Query Rule


For an introduction to database query rules, see [How Does a Database Query Rule Work?](#) on page 92.

To change or delete queries in a database query rule:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group containing the rule.
3. In the **Name** column, click the rule.
4. In the rule properties dialog, select the **Queries** tab.
5. To delete queries:
 - a. Select the check box of each query to be deleted.
 - b. Click **✗ Delete**.

To change the properties of a query:




- a. From the Query column, select the query.
- b. In the query properties dialog, edit the appropriate tabs and click **OK**.

Tip For more information, click  **Help** in any tab.

Adding a Specifier to a Windows RSoP Rule

For an introduction to Windows RSoP rules, see [How Does a Windows RSoP Rule Work? on page 88](#).


To add a specifier to a Windows RSoP rule:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group containing the rule.
3. In the **Name** column, click the rule.
4. In the rule properties dialog, select the **Specifiers** tab.
5. Click  **New Specifier**.
6. In the New Specifier Wizard:
 - a. Enter the specifier properties and click **Next**.
 - b. Select or create a criteria set. To create a new criteria set, click  **New Criteria Set** or  **New From Selected**. For further instructions, see [Creating a Criteria Set for a Windows RSoP Rule \(on page 306\)](#).
 - c. Click **Finish**.

Changing or Deleting Specifiers in a Windows RSoP Rule

For an introduction to Windows RSoP rules, see [How Does a Windows RSoP Rule Work? on page 88](#).

To change or delete specifiers in a Windows RSoP rule:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group containing the rule.
3. In the **Name** column, click the rule.
4. In the rule properties dialog, select the **Specifiers** tab.
5. To delete specifiers:
 - a. Select the check box of each specifier to be deleted.
 - b. Click  **Delete**.

To change the properties of a specifier:

- a. From the User Name column, select the specifier.
- b. In the specifier properties dialog, edit the appropriate tabs and click **OK**.


Moving, Linking, and Unlinking Objects in the Rule Manager

Moving Rules and Rule Groups

With this procedure, you can move a rule (or rule group) from one rule group to another. For example, you can move a rule from the **Unlinked** group to another rule group.

Caution If you move a rule or rule group to a rule group that is currently associated with a check rule task, you may need to initialize new baselines for the task. For instructions, see [Creating Current Baselines for a Check Rule Task on page 522](#).

To move rules and rule groups:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the group containing the objects to be moved.
3. In the main pane, select the check box of each rule (or rule group) to be moved.
4. Click  **Move**.
5. In the Move Rules dialog, select the destination rule group and click **OK**.


Linking Rules and Rule Groups


When you create a rule or rule group, the object is linked to the rule group in which it was created. As needed, the object may also be linked to other rule groups. For more information, see [What are Links and Linked Objects? on page 213](#).

Tips If you link a rule in the **Unlinked** rule group, Tripwire Enterprise *moves* the rule to the destination rule group.

This procedure explains how to link rules and rule groups in the main pane of the Rule Manager. However, you can also link rule groups in the **Parent Groups** tab of a rule properties dialog (see [Changing the Properties of a Rule on page 437](#)) or rule group properties dialog (see [Changing the Properties of a Rule Group on page 440](#)).

To link rules and rule groups to another rule group:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the group containing the objects to be linked.
3. Select the check box of each rule (or rule group) to be linked.
4. Click  **Link**.
5. Select the destination rule group and click **OK**.

Note In the Rule Manager, a link  emblem overlays the icon of each rule or rule group that is linked to multiple rule groups.

Unlinking Rules and Rule Groups


This procedure unlinks a rule (or rule group) from a rule group. For more information, see [What are Links and Linked Objects?](#) on page 213.

If you unlink a rule (or rule group) from the only rule group with which it is linked, Tripwire Enterprise moves the rule to the **Unlinked** node group. To retrieve an object from the **Unlinked** group, see [Moving Rules and Rule Groups](#) on the previous page.

Tip To unlink an object, your user account must have Delete and Link permissions for that object, and (for groups) all objects descended from that object. For more information, see [What are User Permissions and User Roles?](#) on page 204.

This procedure explains how to unlink rules and rule groups displayed in the main pane of the Rule Manager. However, you can also unlink rule groups in the **Parent Groups** tab of a rule properties dialog (see [Changing the Properties of a Rule](#) on page 437) or rule group properties dialog (see [Changing the Properties of a Rule Group](#) on page 440).

To unlink rules (or rule groups) from a rule group:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the group containing the objects to be unlinked.
3. Select the check box of each rule (or rule group) to be unlinked.
4. Click  **Unlink**.
5. Specify whether or not to run the Clear Unlinked Groups task on all Unlinked groups in TE. For more information on this task, see [What are Task Types?](#) on page 127.
6. Click **OK**.

Note If you get an error message when trying to unlink objects, an access control (see [What are Access Controls?](#) on page 208) is preventing you from unlinking a descendant object. To determine which objects have access controls, check the Objects tab for the Error log message associated with this operation.

Exporting and Importing Objects in the Rule Manager


Exporting Rules and Rule Groups

This procedure exports and saves selected rules and rule groups in an XML file. As needed, the contents of the XML file may be re-imported at a later date (see [Importing Rules and Rule Groups on the next page](#)).

Notes Criteria sets associated with file system rules, Windows registry rules, or database rules are also exported to rule XML files. In addition, if any actions are directly associated with an exported rule, the actions will be exported to the XML file.

This procedure explains how to export rules and rule groups displayed in the main pane of the Rule Manager. However, you can also export objects in the **Parent Groups** tab of a rule properties dialog (see [Changing the Properties of a Rule on page 437](#)) or rule group properties dialog (see [Changing the Properties of a Rule Group on page 440](#)).

To export rules and rule groups to an XML file:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group containing the rules and rule groups to be exported.
3. (Optional) To export **specific** rules and rule groups, select the appropriate check boxes. Only objects on the same page of the Rule Manager can be selected in a single export operation.
4. Click  **Export**.
5. In the Export Rules dialog, select one of the following options and click **OK**:
 - **All rules and rule groups**. This option exports all rules and rule groups in your Tripwire Enterprise implementation.
 - **Selected rules and rule groups only**. This option exports the selected rules and rule groups only.
6. To export the file to a local directory, complete the standard steps for your system.

Tip If your Web browser is an older version of Internet Explorer, you may need to manually add a **.xml** extension to the end of the file name.

Importing Rules and Rule Groups


This procedure imports rules (and rule groups) from an XML file to your Tripwire Enterprise implementation. (To create an XML file containing rules, see [Exporting Rules and Rule Groups on the previous page](#).)

Caution Prior to this procedure, you should first review the guidelines employed by Tripwire Enterprise when importing the contents of an XML file (see [How Do I Import and Export Tripwire Enterprise Objects? on page 217](#)).

To import the rules and rule groups in an XML file:

1. In the Manager bar, click **RULES**.
2. In the tree pane, click the rule group to which the XML file's contents will be imported. The rule group structure defined in the XML file will be created in this location.

Note Rules downloaded from the Tripwire Customer Center as part of policy content should always be imported into the Root Rule Group.

3. Click  **Import**.
4. In the Import Rules dialog, click **Browse**.
5. To locate and select the XML file, complete the standard steps for your system.
6. In the Import Rules dialog, click **OK**.

Chapter 8. Action Procedures

Viewing and Changing Objects in the Action Manager

Viewing Actions and Action Groups

To view actions and action groups in the Action Manager:

1. In the Manager bar, click **ACTIONS**.
2. In the tree pane, select an action group.
3. In the main pane, review the action group's contents in the Action Manager table (see [Figure 29](#)). [Table 104 on the next page](#) defines each of the columns in the table.
 - To **sort** the contents of the Action Manager table by the values in a column, click the column header. To reverse the order, click the column header a second time.
 - If the Action Manager contains multiple pages, use the navigation controls at the bottom of the Action Manager to **scroll** through the pages.
 - To adjust the Action Manager **maximum table size** setting, see [Changing User Preference Settings on page 262](#).
 - In the tree pane, each conditional action contains a True and False branch. Click either branch to view the associated actions (if any). For more information, see [How Does a Conditional Action Work? on page 125](#).

Figure 29. The Action Manager

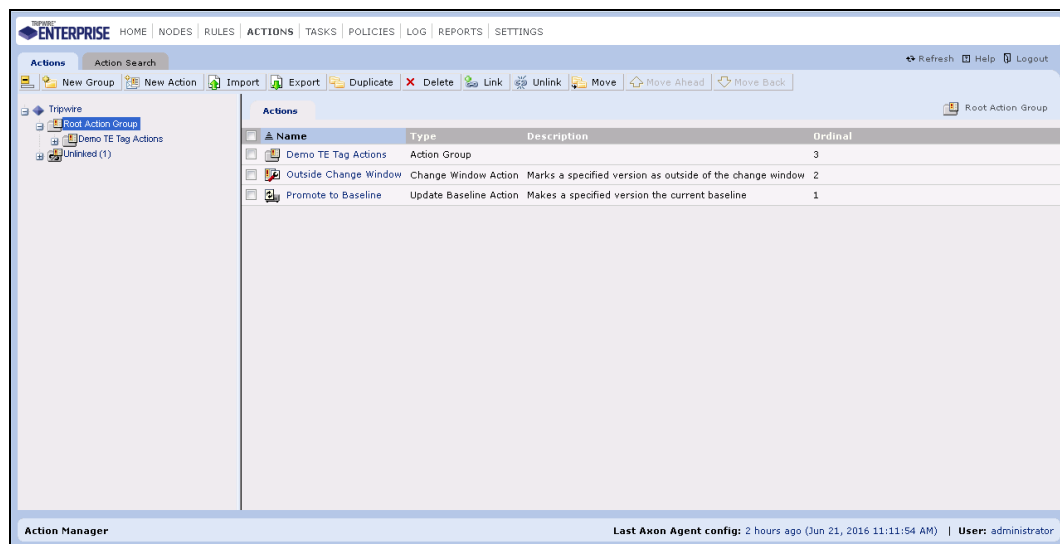


Table 104. Columns in the Action Manager table


Column	Description
Name	The name of an action or action group. To view the object's properties, click the Name link.
Type	This column identifies the type of each Action Manager entry. <ul style="list-style-type: none">• Action. For actions, the Type column identifies the type of action (see What are Actions and Action Types? on page 116).• Action Group
Description	This column displays an optional description for each action and action group. To add or edit a description, see: <ul style="list-style-type: none">• Changing the Properties of an Action (on page 482)• Changing the Properties of an Action Group (on page 487)
Ordinal	This column indicates the current order of the actions and action groups contained in the selected action group. When the selected action group is run, Tripwire Enterprise executes the group's contents in the order indicated here. If the selected group contains a sub-group, TE runs all actions in the sub-group before running the next action in the selected group. To change the order, see Ordering Actions in an Action Group on page 488.

Searching for Actions

Notes For an introduction to common search features such as wildcards, text-field qualifiers, and saved searches, see [How Do I Run a Search? on page 232](#).

In the Action Search tab, the button bar contains many of the same buttons available in the Actions tab. To use these buttons, refer to the procedures in [Chapter 8: Action Procedures \(on page 477\)](#).

To search for actions:

1. In the Manager bar, click **ACTIONS**.
2. Select the **Action Search** tab.
3. From the **Type** list, select (**any action**) or a specific action type. The available search fields vary by action type. For definitions, see [What are Actions and Action Types? on page 116](#).
4. Enter additional search criteria. For guidance, see [Table 105 on the next page](#).
 - Some of the search criteria are based on values that can be edited in action property dialogs (see [Changing the Properties of an Action on page 482](#)).
 - All text-field entries are case-insensitive. For example, ‘Action’ and ‘action’ will return the same results.
 - Any string may be entered in a text field. For example, if you enter a string in the **Action name** field, and select **Contains** as the text-field qualifier, search results will include any action with a name that includes the string.
5. Click  **Search**.

Next If desired, you can save the entered search criteria for future use. For instructions, see [Creating a Saved Search on page 234](#).

Table 105. Action search criteria

Search Criteria	To limit search results to ...
Action description	... actions with specific descriptions: <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial description in the text field.
Action name	... actions with specific names: <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial action name in the text field.
Commands to run	... actions that run commands with specified content. <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a search string in the text field.
Error patterns	... actions that interpret specified command output as indicating a failure of the action's command to run. <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a search string in the text field.
Log output	... actions that have their log-notification setting enabled or disabled.
Reboot after restore	... actions that reboot monitored systems after restoration.
Run commands after restoring files	... actions that run commands with specified content after restoring a monitored system: <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a search string in the text field.
Save Location	... actions that save restored configurations in the primary or secondary storage area of a monitored system.
Type	... actions of a specific type, select a type from the drop-down list. Otherwise, accept the default value (any action).

Changing the Properties of an Action


For an introduction to actions, see:

- [What are Actions and Action Types? \(on page 116\)](#)
- [How Does a Conditional Action Work? \(on page 125\)](#)

Note The Promote to Baseline and Outside Change Window actions cannot be modified.

To view the properties of an action:

1. In the Manager bar, click **ACTIONS**.
2. In the tree pane, click the action group containing the action.
3. In the main pane, select the action in the **Name** column.
4. As needed, modify the tabs in the action properties dialog.
 - For a common or network-device action, see [Table 106 below](#).
 - For a conditional action, see [Table 107 on page 484](#).

Tip For more information, click  **Help** in any tab.

5. Click **OK**.

Table 106. Tabs in properties of common and network-device actions

Tab	Available with these actions	Description
Advanced	E-mail	An e-mail action sends an e-mail notification to one or more recipients in response to detected changes. This tab controls how each change is displayed in the body of these e-mails.
Comment	Promote specific versions Promote-by-match Promote-by-reference	Defines a comment and an approval ID to be saved in the properties of each baseline version created by the action.
Conditions	Promote-by-reference	Defines conditions for version custom properties. If an element version does not meet the specified conditions, TE will not promote the version.

Tab	Available with these actions	Description
Delivery	E-mail Run report SNMP	Specifies the address(es) to which the action sends e-mails, report-output files, or SNMP traps.
Details	Execution Promote-by-match Promote-by-reference Set custom value Syslog Tag	<p>In an execution action, defines the command to be run by the action.</p> <p>In a promote-by-match action, specifies the matching strategy and match file.</p> <p>In a promote-by-reference action, identifies the reference node and a rule (optional) to specify applicable monitored objects.</p> <p>In a set custom value action, defines a value for the custom property assigned to the action.</p> <p>In a syslog action, identifies the host system for the syslog service and provides some control over syslog messages sent by the action.</p> <p>In a tag action, defines the tags applied or unapplied to nodes by the action.</p>
General	All actions	The name and description (optional) of the action.
Options	Run command Some restore actions	<p>In a run command action, defines the commands for the action, along with error patterns in command output.</p> <p>In a restore action, defines a command to be run on each device restored by the action.</p>
Packages	All promote actions	<p>Assigns software-installation packages to the action. If an element version does <i>not</i> represent a monitored object associated with one of the specified packages, TE will not promote the version.</p> <p>Also see the Strict tab.</p>
Parent Groups	All actions	<p>Displays the full path of each action group to which the action is linked.</p> <ul style="list-style-type: none"> This tab includes some of the same buttons that appear in the Action Manager. For guidance in using these buttons, refer to the corresponding procedure in this chapter. To view or edit the properties of an action group, select the group's link. (For more information, see Changing the Properties of an Action Group on page 487.)
Report	Run report	Specifies the report to be run by the action.
Rules	Run rule	Specifies the rule or rule group with which the action runs a version check.
Run Task	Run task	Specifies the task run by the action.
Scope	Run report	If the action is run in response to change versions created by a version check, this tab limits report output to data for nodes, elements, element versions, and/or rules involved in the version check.
Security	All actions	Contains any access controls that have been created for the action. For more information, see Working with Action Access Controls on page 489.

Tab	Available with these actions	Description
Severity Override	Severity override	Defines the severity level that the action will assign to new change versions.
Strict	All promote actions	The installation database of a software-installation package stores the name and unique identifier of each file and directory in the package. This tab contains a setting that prevents the action from promoting a change version if the version's monitored object does not match one of the entries in the installation database for one of the packages assigned to the action.

Table 107. Tabs in properties of conditional actions

Tab	Available with these conditional actions	Description
Attributes	By-reference attributes	Indicates the attributes for the action. <ul style="list-style-type: none"> If a change version and a matching element (specified in the Details tab) have the same values for all specified attributes, the action executes its True response. Otherwise, the action executes its False response.
Change Type	Change type	Indicates the type(s) of change for the action (addition, modification, and/or removal). <ul style="list-style-type: none"> If a change version is of a specified type, the action executes its True response. If a change version of a type that is <i>not</i> specified, the action executes its False response.
Conditions	Attributes Audit trail By-reference Content Custom properties Element name Tag	Defines the condition(s) for the action. <ul style="list-style-type: none"> If the condition(s) is satisfied, the action executes its True response. If the condition(s) is not satisfied, the action executes its False response.

Tab	Available with these conditional actions	Description
Details	By-reference By-reference attributes By-match Policy test result	<p>In a by-reference conditional action, specifies the reference node, rule (or rule group), and other action properties.</p> <p>In a by-reference attributes conditional action, specifies the reference node and the type of matching elements.</p> <p>In a by-match conditional action, specifies the matching strategy and match file.</p> <p>In a policy test result conditional action, specifies the TE policy or policy test group for the action. If a new change version passes all applicable policy tests in the TE policy or group, the action executes its True response.</p>
False	All conditional actions	Determines the response if the action's conditions are <i>not</i> satisfied.
General	All conditional actions	The name and description (optional) of the action.
Out-of-Scope	Policy test result	Determines how the action responds to new change versions that are outside of the scope of the action's TE policy or policy test group.
Packages	Package	<p>Assigns software-installation packages to the action. If a new change version represents a file or directory in a specified package, the action executes its True response.</p> <p>Also see the Strict tab.</p>
Parent Groups	All conditional actions	<p>Displays the full path of each action group to which the action is linked.</p> <ul style="list-style-type: none"> This tab includes some of the same buttons that appear in the Action Manager. For guidance in using these buttons, refer to the corresponding procedure in this chapter. To view or edit the properties of an action group, select the group's link. (For more information, see Changing the Properties of an Action Group on page 487.)
Security	All conditional actions	Contains any access controls that have been created for the action. For more information, see Working with Action Access Controls on page 489.
Severity Range	Severity range	Defines the severity range for the action. If a change version's severity level falls within the specified range, the action executes its True response.
Strict	Package	<p>The installation database of a software-installation package stores the name and unique identifier of each file and directory in the package. This tab contains a setting that will only permit the action to run its True response if both of the following conditions are satisfied:</p> <ul style="list-style-type: none"> A change version represents a file or directory in one of the Packages assigned to the action. The file or directory matches one of the entries in the package's installation database.
Time Windows	Time range	Defines time windows for the action. If a change version is created within one of the time windows, the action executes its True response.

Tab	Available with these conditional actions	Description
True	All conditional actions	Determines the response if the action's conditions are satisfied.

Changing the Properties of an Action Group

Tip This procedure explains how to change the properties of an action group displayed in the main pane of the Action Manager. However, you can also change the properties of an action group in the **Parent Groups** tab of an action properties dialog (see [Changing the Properties of an Action on page 482](#)).

To change the properties of an action group:

1. In the Manager bar, click **ACTIONS**.
2. In the tree pane, click the group containing the action group.
3. In the main pane, select the action group in the **Name** column.
4. As needed, modify the tabs in the action group properties dialog. For tab descriptions, see [Table 108](#).

Tip For more information, click  **Help** in any tab.

5. Click **OK**.



Table 108. Tabs in action group properties

Tab	Description
General	The name and description (optional) of the action group.
Parent Groups	Displays the full path of each action group to which this action group is linked. <ul style="list-style-type: none">• This tab includes some of the same buttons that appear in the Action Manager. For guidance in using these buttons, refer to the corresponding procedure in this chapter.• To view or edit the properties of an action group, select the group's link.
Security	Contains any access controls that have been created for the action group. For more information, see Working with Action Access Controls on page 489 .

Ordering Actions in an Action Group

An action group can contain one or more actions, as well as other action groups. When Tripwire Enterprise runs an action group, it executes the group's actions (and action groups) in the order indicated in the Ordinal column of the main pane.

To re-arrange the order of an action group's contents:

1. In the Manager bar, click **ACTIONS**.
2. In the tree pane, select the action group.
3. In the main pane, the Ordinal column indicates the order in which the action group's contents will be executed when TE runs the group.
 - To move an action or action group up one place in the sequence, select the object's check box and click  **Move Ahead**.
 - To move an action or action group down one place in the sequence, select the object's check box and click  **Move Back**.


Working with Action Access Controls

Creating an Access Control for an Action or Action Group

For an introduction to access controls, see [What are Access Controls? on page 208](#).

Note If one or more access controls have already been created for the action or action group, an additional access control can only be created by the default administrator account or a user account assigned to one of the existing access controls.

To set an access control for an action or action group:

1. In the Manager bar, click **ACTIONS**.
2. In the tree pane, click the group containing the action or action group.
3. In the main pane, click the action or action group in the **Name** column.
4. In the properties dialog, click the **Security** tab.
5. Click  **Add Control**.
6. Select the check box of each **Principal** (user or user group) to be assigned to the access control and click **Next**.
7. Select the user role for the access control and click **Finish**.

Changing an Access Control for an Action or Action Group

For an introduction to access controls, see [What are Access Controls? on page 208](#).

Note An access control can only be changed by the default administrator account or a user account assigned to the control.

To change the user role assigned to an access control:

1. In the Manager bar, click **ACTIONS**.
2. In the tree pane, click the group containing the action or action group associated with the access control.
3. In the main pane, click the action or action group in the **Name** column.
4. In the properties dialog, click the **Security** tab.
5. In the **Access Control** column, select the access control.
6. In the Access Control dialog, select the new user role and click **OK**.

Deleting Access Controls for an Action or Action Group

Note An access control can only be deleted by the default administrator account or a user account assigned to the control.

Caution With an access control, non-Administrators may be granted Administrator-level access to a particular action or action group. If the access control is deleted, the user will no longer be able to modify the properties of the action or action group.

To delete an access control from an action or action group:


1. In the Manager bar, click **ACTIONS**.
2. In the tree pane, click the group containing the action or action group associated with the access control.
3. In the main pane, click the action or action group in the **Name** column.
4. In the properties dialog, select the **Security** tab.
5. Select the check box of each access control to be deleted.
6. Click **✕ Delete**.
7. Click **OK** to confirm.

Creating and Deleting Objects in the Action Manager

Creating an Action Group

For an introduction to action groups, see [About Groups on page 29](#).

To create an action group:

1. In the Manager bar, click **ACTIONS**.
2. In the tree pane, click the action group in which to create the new action group.
3. Click  **New Group**.
4. In the New Action Group Wizard, enter a **Name** and **Description** (optional) for the new group.
5. Click **Finish**.


Next To add existing actions and action groups to the new group, see:


- [Moving Actions and Action Groups \(on page 503\)](#)
- [Linking Actions and Action Groups \(on page 503\)](#)

Creating a Conditional Action

For an introduction to conditional actions, see [How Does a Conditional Action Work? on page 125](#).

To create a conditional action:

1. In the Manager bar, click **ACTIONS**.
2. Click  **New Action**.
3. In the Create Action dialog, select an action type from the **Conditional Actions** folder. Then, click **OK**.
4. In the New Action Wizard, enter a **Name** and **Description** (optional), and click **Next**.
5. Define the conditions for the action. This process will vary, depending on the type of conditional action.

Tip For more information, click  **Help** in any wizard page.

6. In the True Actions wizard page, add any actions and/or action groups to be run if a new change version satisfies the conditions of the conditional action.

7. In the False Actions wizard page, add any actions and/or action groups to be run if a new change version does **not** satisfy the conditions of the conditional action. (To add an action or action group, refer to the instructions in the previous step.)
8. Click **Finish**.

Next To run the conditional action with a version check, you must assign the action to a check rule task or a rule. For further instructions, see:


- [Changing the Properties of a Task \(on page 512\)](#)
- [Changing the Properties of a Rule \(on page 437\)](#)

Creating an E-mail Action

For an introduction to e-mail actions, see [How Does an E-mail Action Work? on page 120](#).

To send e-mail notifications, an e-mail action requires the use of an e-mail server. Therefore, prior to this procedure, you should create at least one e-mail server in the Settings Manager (see [Working with E-mail Servers on page 272](#)).

To create an e-mail action:

1. In the Manager bar, click **ACTIONS**.
2. Click  **New Action**.
3. In the Create Action dialog, select **Common > E-mail Action** and click **OK**.
4. In the New Action Wizard, enter a **Name** and **Description** (optional), and click **Next**.
5. In the delivery information page, use the following methods to specify the recipients (Principals) of e-mail notifications sent by the action:
 - Select the check box of each user or user group to be designated as a recipient.
 - In the **Additional addresses** field, enter the e-mail addresses of any other recipients. To enter multiple e-mail addresses, separate the addresses with a comma (,) or semi-colon (;).
6. Select an **E-mail server** and **E-mail type**, and click **Next**.
7. (Detailed e-mails only) If desired, modify the **Lines of Context** and **Maximum Lines per Block**.
8. Click **Finish**.


Next To run the e-mail action with a version check, you must assign the action to a check rule task or a rule. For further instructions, see:


- [Changing the Properties of a Task \(on page 512\)](#)
- [Changing the Properties of a Rule \(on page 437\)](#)

Creating an Execution Action

For an overview of execution actions, see [How Does an Execution Action Work?](#) on page 121.

To create an execution action:

1. In the Manager bar, click **ACTIONS**.
2. Click  **New Action**.
3. In the Create Action dialog, select **Common > Execution Action** and click **OK**.
4. In the New Action Wizard, enter a **Name** and **Description** (optional), and click **Next**.
5. Enter the **Command line** to be executed when the action runs as part of a version check. The command must be compatible with the shell invoked on the target system. On a UNIX system, `/bin/sh` is invoked; on a Windows system, `cmd.exe` is invoked.

Tip For more information, click  **Help** in any wizard page.

One or more command line variables may be included in the command. A **command line variable** forwards specific data to the executable file when a change is detected. [Table 109 on the next page](#) defines the information forwarded by each command line variable. In addition, the table indicates if the variable can be used in the following situations:

- Once for each action run (Once per Run).
- Once for each detected change (Once per Change).
- Once for each monitored system on which changes are detected (Once per Node).

Note For an introduction to version checking, see [About Version Checks on page 44](#).

Example 1

The following example shows the syntax to execute a command and capture output written to `stdout` when not invoking a shell script. This example echoes the filename (including the full path) of the changed element to the file `test.log`.

UNIX:`echo %v >> /tmp/test.log`

Windows:`echo "%v" >> "c:\temp\test.log"`

Example 2

The following example shows the syntax to execute a command that does not write to `stdout` (in the success case). This example copies the actual file related to the changed element to `<filename>.bak`.

UNIX:`/usr/bin/cp %v %v.bak`

Windows:`copy %v %v.bak`

6. Select an **Execution location**.

Tip **Node** should only be selected for execution actions to be run with version checks of file systems.

7. If you used the %f variable in the **Command line** field to generate a Detailed Changes Report on a Tripwire Enterprise Agent, enter the report criteria in the **Detailed Changes Report** fields.

8. Click **Finish**.

Next To run the execution action with a version check, you must assign the action to a check rule task or a rule. For further instructions, see:

- [Changing the Properties of a Task \(on page 512\)](#)
- [Changing the Properties of a Rule \(on page 437\)](#)

Table 109. Command line variables for execution actions

Variable	If a version check detects a change in a monitored object, this variable sends the following information to the executable file:	Once per Run	Once per Node	Once per Change
%v	The name of the monitored object.			•
%e	The OID of the monitored object's element. Note: An Object Identifier (OID) is a unique code that the application automatically assigns to a Tripwire Enterprise object.			•
%h	The hostname of the monitored system associated with the monitored object.		•	•
%n	The OID of the monitored system's node.		•	•
%r	The OID of the rule that identified the monitored object.			•
%c	The OID of the monitored object's snapshot. Note: A snapshot is a temporary record of the object's current attributes.			•
%b	The OID of the monitored object's current baseline.			•
%s	The hostname of the Tripwire Enterprise Server.	•	•	•
%f	Compiles output for a Detailed Changes Report, and forwards the path of the report output file to the executable file. This option is only valid when run on Tripwire Enterprise Agents. It is not supported on Axon Agents. Note: The report output file is automatically deleted upon completion of the action. To save the file for future reference, you should include a copy command in the command line.		•	•


Creating a Promote Action


With this procedure, you can create the following types of actions:

- Promote specific versions
- Promote-by-match
- Promote-by-reference

For an introduction to these action types, see *What are Actions and Action Types?* on page 116.

To create a promote action:

1. In the Manager bar, click **ACTIONS**.
2. Click  **New Action**.
3. In the Create Action dialog, select a type of promote action in the **Common** folder and click **OK**.
4. In the New Action Wizard, enter a **Name** and **Description** (optional), and click **Next**.
5. Complete the remaining wizard pages.

Tips For further instructions, click  **Help** in any wizard page.

To successfully run a **promote-by-match action**, your match file should be stored in a directory on your Tripwire Enterprise Server.

For promote-by-match actions and promote-by-reference actions, you can enter date and time macros in the **Comment** and **As static string** fields. For example, to include the date and time of promotion with an Approval ID, you could enter the following values in the second wizard page:

Comment: \${Date: DD, MMMM YYYY hh:mm}

As static string: 274B Approved on \${Date}

For macro formats, see:

<http://docs.oracle.com/javase/8/docs/api/java/text/SimpleDateFormat.html>


Next To run the promote action with a version check, you must assign the action to a check rule task or a rule. For further instructions, see:

- *Changing the Properties of a Task* (on page 512)
- *Changing the Properties of a Rule* (on page 437)

Creating a Restore Action

For an introduction to restore actions, see [How Does a Restore Action Work?](#) on page 123.

To create a restore action:

1. In the Manager bar, click **ACTIONS**.
2. Click  **New Action**.
3. In the Create Action dialog, select **Network Device > Restore Actions**, and then select a type of restore action. Click **OK**.
4. In the New Action Wizard, enter a **Name** and **Description** (optional).
5. For some restore actions, click **Next** to set additional parameters for the action.

Tip For further instructions, click  **Help**.

6. Click **Finish**.

Next To run the restore action with a version check, you must assign the action to a check rule task or a rule. For further instructions, see:


- [Changing the Properties of a Task](#) (on page 512)
- [Changing the Properties of a Rule](#) (on page 437)

Caution To restore files manually at your own discretion, you should run restore actions with the Node Manager Run Actions function (rather than with a scheduled check rule task). For more information, see [Restoring a Changed File with the Run Actions Feature](#) (on page 404) and [Restoring Multiple Files with the Run Actions Feature](#) (on page 405).

Creating a Run Command Action

A run command action executes one or more commands on a changed network device.

To create a run command action:

1. In the Manager bar, click **ACTIONS**.
2. Click  **New Action**.
3. In the Create Action dialog, select **Network Device > Run Command Action** and click **OK**.
4. In the New Action Wizard, enter a **Name** and **Description** (optional), and click **Next**.
5. Complete the wizard dialog and click **Finish**.

Tip For more information, click  **Help**.


Next To run the new action with a version check, you must assign the action to a check rule task or a rule. For further instructions, see:

- [Changing the Properties of a Task \(on page 512\)](#)
- [Changing the Properties of a Rule \(on page 437\)](#)

Creating a Run Report Action

For an introduction to run report actions, see [How Does a Run Report Action Work? on page 188](#).

To create a run report action:

1. In the Manager bar, click **ACTIONS**.
2. Click  **New Action**.
3. In the Create Action dialog, select **Common > Run Report Action** and click **OK**.
4. In the New Action Wizard, enter a **Name** and **Description** (optional), and click **Next**.
5. Complete the wizard dialog and click **Finish**.

Tip For more information, click  **Help**.



Next To run the new action with a version check, you must assign the action to a check rule task or a rule. For further instructions, see:

- [Changing the Properties of a Task \(on page 512\)](#)
- [Changing the Properties of a Rule \(on page 437\)](#)

Creating a Run Rule Action

For an introduction to run rule actions, see [How Does a Run Rule Action Work? on page 123](#).

To create a run rule action:

1. In the Manager bar, click **ACTIONS**.
2. Click  **New Action**.
3. In the Create Action dialog, select **Common > Run Rule Action** and click **OK**.
4. In the New Action Wizard, enter a **Name** and **Description** (optional), and click **Next**.
5. Click  **Chooser**.
6. In the Select Rule or Rule Group dialog, select the rule or group for this action and click **OK**.
7. Click **Finish**.



Next To run the new action with a version check, you must assign the action to a check rule task or a rule. For further instructions, see:

- [Changing the Properties of a Task \(on page 512\)](#)
- [Changing the Properties of a Rule \(on page 437\)](#)

Creating a Run Task Action

For an introduction to run task actions, see [What are Actions and Action Types? on page 116](#).

To create a run task action:

1. In the Manager bar, click **ACTIONS**.
2. Click  **New Action**.
3. In the Create Action dialog, select **Common > Run Task Action** and click **OK**.
4. In the New Action Wizard, enter a **Name** and **Description** (optional), and click **Next**.
5. Click  **Chooser**.
6. In the Select Task dialog, select a task and click **OK**.
7. Click **Finish**.


Next To run the new action with a version check, you must assign the action to a check rule task or a rule. For further instructions, see:

- [Changing the Properties of a Task \(on page 512\)](#)
- [Changing the Properties of a Rule \(on page 437\)](#)

Creating a Set Custom Value Action

For an introduction to set custom value actions, see [How Does a Set Custom Value Action Work? on page 124](#). To create a set custom value action, you must first create a custom property in the Settings Manager. For more information, see [What are Custom Properties? on page 197](#).

To create a set custom value action:

1. In the Manager bar, click **ACTIONS**.
2. Click  **New Action**.
3. In the Create Action dialog, select **Common > Set Custom Value Action** and click **OK**.
4. In the New Action Wizard, enter a **Name** and **Description** (optional), and click **Next**.
5. From the **Property Type** drop-down, select the type of custom property.
6. Select the radio button for the desired custom property, and enter the custom value in the displayed fields.
7. Click **Finish**.


Next To run the set custom value action with a version check, you must assign the action to a check rule task or a rule. For further instructions, see:

- [Changing the Properties of a Task \(on page 512\)](#)
- [Changing the Properties of a Rule \(on page 437\)](#)

Creating a Severity Override Action

For an introduction to severity override actions, see [What are Actions and Action Types? on page 116](#).

To create a severity override action:

1. In the Manager bar, click **ACTIONS**.
2. Click  **New Action**.
3. In the Create Action dialog, select **Common > Severity Override Action** and click **OK**.
4. In the New Action Wizard, enter a **Name** and **Description** (optional), and click **Next**.
5. Enter the severity level and click **Finish**.


Next To run the severity override action with a version check, you must assign the action to a check rule task or a rule. For further instructions, see:

- [Changing the Properties of a Task \(on page 512\)](#)
- [Changing the Properties of a Rule \(on page 437\)](#)

Creating an SNMP Action

An SNMP action sends an SNMP trap to a trap receiver, such as an Enterprise Management System (EMS). For more information, see [How Does an SNMP Action Work? on page 124](#).

To create an SNMP action:

1. In the Manager bar, click **ACTIONS**.
2. Click  **New Action**.
3. In the Create Action dialog, select **Common > SNMP Action** and click **OK**.
4. In the New Action Wizard, enter a **Name** and **Description** (optional), and click **Next**.
5. Enter the SNMP delivery information.
6. Click **Finish**.


Next To run the SNMP action with a version check, you must assign the action to a check rule task or a rule. For further instructions, see:

- [Changing the Properties of a Task \(on page 512\)](#)
- [Changing the Properties of a Rule \(on page 437\)](#)

Creating a Syslog Action

A syslog action sends an event notification to a system log.

To create a syslog action:

1. In the Manager bar, click **ACTIONS**.
2. Click  **New Action**.
3. In the Create Action dialog, select **Common > Syslog Action** and click **OK**.
4. In the New Action Wizard, enter a **Name** and **Description** (optional), and click **Next**.
5. Enter the syslog delivery information.
6. Click **Finish**.


Next To run the syslog action with a version check, you must assign the action to a check rule task or a rule. For further instructions, see:

- [Changing the Properties of a Task \(on page 512\)](#)
- [Changing the Properties of a Rule \(on page 437\)](#)

Duplicating Actions

With this procedure, you can either duplicate specified actions in a selected action group, or all actions in a selected action group.

To create copies of existing actions:

1. In the Manager bar, click **ACTIONS**.
2. In the tree pane, click the action group containing the actions to be duplicated.
3. (Optional) To duplicate specific actions, select the check box of each action.
4. Click  **Duplicate**.
5. Click **OK** in the confirmation dialog.

Tripwire Enterprise uses the following convention to name a duplicate action:

```
<original_action>(<#>)
```

where:

<original_action> is the name of the action that was duplicated.

<#> is a number that increments each time the original action is duplicated (beginning with 1) - for example, action(1), action(2), etc.

Next To run the duplicated action with a version check, you must assign the action to a check rule task or a rule. For further instructions, see:

- [Changing the Properties of a Task \(on page 512\)](#)
- [Changing the Properties of a Rule \(on page 437\)](#)

Deleting Actions and Action Groups

This procedure permanently deletes all instances of selected actions and/or action groups. To remove an object from an action group *without* deletion, see [Unlinking Actions and Action Groups](#) on page 504.

Notes To delete an object, your user account must have Delete permissions for that object, and (for groups) all objects descended from that object. For more information, see [What are User Permissions and User Roles?](#) on page 204.

The Promote to Baseline and Outside Change Window actions cannot be deleted.

To delete actions and/or action groups:

1. In the Manager bar, click **ACTIONS**.
2. In the tree pane, click the action group containing the objects to be deleted.
3. Select the check box for each object to be deleted.
4. Click **✖ Delete**.
5. Specify whether or not to run the Clear Unlinked Groups task on all Unlinked groups in TE. For more information on this task, see [What are Task Types?](#) on page 127.
6. Click **OK**.


Note If you get an error message when trying to delete objects, an access control (see [What are Access Controls?](#) on page 208) is preventing you from deleting a descendant object. To determine which objects have access controls, check the Objects tab for the Error log message associated with this operation.

Moving, Linking, and Unlinking Objects in the Action Manager

Moving Actions and Action Groups

With this procedure, you can move selected actions and/or action groups from one action group to another. For example, you can move an action from the **Unlinked** group to another action group

To move actions and/or action groups:

1. In the Manager bar, click **ACTIONS**.
2. In the tree pane, click the group containing the objects to be moved.
3. In the main pane, select the check box of each action (or action group) to be moved.
4. Click  **Move**.
5. In the Move Actions dialog, select the destination action group and click **OK**.


Linking Actions and Action Groups


When you create an action or action group, the object is linked to the action group in which it was created. As needed, the object may also be linked to other action groups. For more information, see [What are Links and Linked Objects? on page 213](#).

Tips If you link an action in the **Unlinked** action group, Tripwire Enterprise *moves* the action to the destination action group.

This procedure explains how to link actions and action groups displayed in the main pane of the Action Manager. However, you can also link action groups in the **Parent Groups** tab of an action properties dialog (see [Changing the Properties of an Action on page 482](#)).

To link actions and/or action groups to another action group:

1. In the Manager bar, click **ACTIONS**.
2. In the tree pane, click the group containing the objects to be linked.
3. Select the check box of each action (or action group) to be linked.
4. Click  **Link**.
5. Select the destination action group and click **OK**.

Note In the Action Manager, a link  emblem overlays the icon of each action or action group that is linked to multiple action groups.

Unlinking Actions and Action Groups


This procedure unlinks an action (or action group) from an action group. For more information, see [What are Links and Linked Objects?](#) on page 213.

If you unlink an action (or action group) from the only action group with which it is linked, Tripwire Enterprise moves the action to the **Unlinked** action group. To retrieve an object from the **Unlinked** group, see [Moving Actions and Action Groups on the previous page](#).

Tip To unlink an object, your user account must have Delete and Link permissions for that object, and (for groups) all objects descended from that object. For more information, see [What are User Permissions and User Roles?](#) on page 204.

This procedure explains how to unlink actions and action groups displayed in the main pane of the Action Manager. However, you can also unlink action groups in the **Parent Groups** tab of an action properties dialog (see [Changing the Properties of an Action on page 482](#)).

To unlink actions and/or action groups from an action group:

1. In the Manager bar, click **ACTIONS**.
2. In the tree pane, click the group containing the objects to be unlinked.
3. Select the check box of each object to be unlinked.
4. Click  **Unlink**.
5. Specify whether or not to run the Clear Unlinked Groups task on all Unlinked groups in TE. For more information on this task, see [What are Task Types?](#) on page 127.
6. Click **OK**.

Note If you get an error message when trying to unlink objects, an access control (see [What are Access Controls?](#) on page 208) is preventing you from unlinking a descendant object. To determine which objects have access controls, check the Objects tab for the Error log message associated with this operation.


Exporting and Importing Objects in the Action Manager

Exporting Actions and Action Groups

This procedure exports selected actions and action groups to an XML file. As needed, the contents of the XML file may be re-imported at a later date (see [Importing Actions and Action Groups on the next page](#)).

Tip This procedure explains how to export actions and action groups displayed in the main pane of the Action Manager. However, you can also export action groups in the **Parent Groups** tab of an action properties dialog (see [Changing the Properties of an Action on page 482](#)).

To export actions and/or action groups to an XML file:

1. In the Manager bar, click **ACTIONS**.
2. In the tree pane, click the action group containing the actions and action groups to be exported.
3. (Optional) To export **specific** actions and action groups, select the appropriate check boxes. Only objects on the same page of the Action Manager can be selected in a single export operation.
4. Click  **Export**.
5. In the Export Actions dialog, select one of the following options and click **OK**:
 - **All actions and action groups**. This option exports all actions and action groups in your TE implementation.
 - **Selected actions and action groups only**. This option exports the selected actions and action groups only.
6. To export the XML file to a local directory, complete the standard steps for your system.


Tip If your Web browser is an older version of Internet Explorer, you may need to manually add a **.xml** extension to the end of the file name.

Importing Actions and Action Groups

This procedure imports actions (and action groups) from an XML file to your Tripwire Enterprise implementation. (To create an XML file containing actions, see [Exporting Actions and Action Groups on the previous page](#).)

Caution Prior to this procedure, you should first review the guidelines employed by Tripwire Enterprise when importing the contents of an XML file (see [How Do I Import and Export Tripwire Enterprise Objects? on page 217](#)).

To import the actions and action groups in an XML file:

1. In the Manager bar, click **ACTIONS**.
2. In the tree pane, click the action group to which the XML file's contents will be imported. The action group structure defined in the XML file will be created in this location.
3. Click  **Import**.
4. In the Import Actions dialog, click **Browse**.
5. To locate and select the XML file, complete the standard steps for your system.
6. In the Import Actions dialog, click **OK**.

Chapter 9. Task Procedures

Viewing and Changing Objects in the Task Manager

Viewing Tasks and Task Groups

To view tasks and task groups in the Task Manager:

1. In the Manager bar, click **TASKS**.
2. In the tree pane, select a task group.
3. In the main pane, review the task group's contents in the Task Manager table (see [Figure 30](#)). For column definitions, see [Table 110](#).
 - To **sort** the contents of the Task Manager table by the values in a column, click the column header. To reverse the order, click the column header a second time.
 - If the Task Manager contains multiple pages, use the navigation controls at the bottom of the Task Manager to **scroll** through the pages.
 - To adjust the Task Manager **refresh rate** or **maximum table size** settings, see [Changing User Preference Settings on page 262](#).

Figure 30. The Task Manager

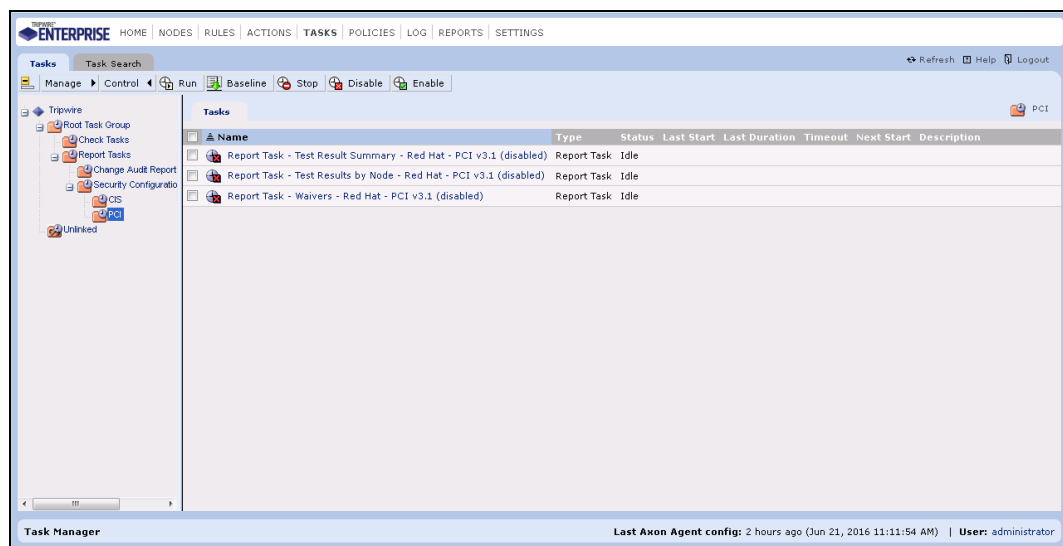


Table 110. Columns in the Task Manager table


Column	Description
Name	The Name column lists the names of tasks and task groups in the selected group. To view the properties of a task or task group, click a Name link. For more information, see: <ul style="list-style-type: none"> • Changing the Properties of a Task on page 512 • Changing the Properties of a Task Group on page 514
Type	This column identifies the type of each Task Manager object. <ul style="list-style-type: none"> • Task. For tasks, the Type column identifies the type of task (see What are Task Types? on page 127). • Task Group
Status	This column indicates the current status of a task: <ul style="list-style-type: none"> • Idle. The task has yet to be run. • Running. The task is currently running. • Complete. The last run of the task completed successfully. • Stopped. A user manually stopped the last run of the task. • Timed Out. TE stopped the last run of the task before it completed. This status only occurs for tasks that include TE Agents when the task run time exceeds the task's timeout limit on one or more TE Agent nodes.
Last Start	This column shows the last time a task started running.
Last Duration	This column shows the total run time for the last completed run of a task. If a task is currently running, this field is blank.
Timeout	If the timeout setting is enabled for a task, this column displays the specified timeout value.
Next Start	If a schedule has been defined for a task, this column shows the next scheduled run time. If a schedule has not been defined for a task, this field is blank. To schedule a task, see Changing the Properties of a Task on page 512 .
Description	This column provides an optional description of each task or task group. To add or edit descriptions, see: <ul style="list-style-type: none"> • Changing the Properties of a Task on page 512 • Changing the Properties of a Task Group on page 514

Searching for Tasks

Notes For an introduction to common search features such as wildcards, text-field qualifiers, and saved searches, see [How Do I Run a Search? on page 232](#).




In the Task Search tab, the button bar contains many of the same buttons available in the Tasks tab. To use these buttons, refer to the procedures in [Chapter 9: Task Procedures \(on page 507\)](#).

To search for tasks:

1. In the Manager bar, click **TASKS**.
2. Select the **Task Search** tab.
3. From the **Type** list, select (**any task**) or a specific task type. The available search fields vary by task type. For task type definitions, see [Table 40 on page 127](#).
4. Enter additional search criteria. For guidance, see [Table 111 on the next page](#).
 - Some of the search criteria are based on values that can be edited in task property dialogs (see [Changing the Properties of a Task on page 512](#)).
 - All text-field entries are case-insensitive. For example, ‘Task’ and ‘task’ will return the same results.
 - Any string may be entered in a text field. For example, if you enter a string in the **Task name** field, and select **Contains** as the text-field qualifier, search results will include any task with a name that includes the string.
5. Click  **Search**.

Next If desired, you can save the entered search criteria for future use. For instructions, see [Creating a Saved Search on page 234](#).

Table 111. Task search criteria

Search Criteria	To limit search results to ...
Has timeout	... baseline rule tasks and check rule tasks with a specific timeout setting (on, off, or any).
Is enabled	... enabled and/or disabled tasks.
Node or node group	<p>... tasks associated with a specific node or node group:</p> <ol style="list-style-type: none"> 1. Click  Chooser. 2. Select the node or group, and click OK. <p>Note: If you select a node group, search results will include rule tasks associated with the node group itself, or with nodes or node groups descended from the group.</p>
Rule or rule group	<p>... tasks associated with a specific rule or rule group:</p> <ol style="list-style-type: none"> 1. Click  Chooser. 2. Select the rule or group, and click OK. <p>Note: If you select a rule group, search results will include rule tasks associated with the rule group itself, or with rules or rule groups descended from the group.</p>
Saved searches in Log Manager	<p>... tasks specified by a saved search in the Log Manager:</p> <ol style="list-style-type: none"> 1. Click  Chooser. 2. Select the saved search and click OK.
Task description	<p>... tasks with specific descriptions:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial description in the text field.
Task name	<p>... tasks with specific names:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial task name in the text field.
Type	... tasks of a specific type, select a type from the drop-down list. Otherwise, accept the default value (any task).


Changing the Properties of a Task

For an introduction to tasks, see:

- [How Does a Baseline Rule Task Work?](#) (on page 128)
- [How Does a Check Rule Task Work?](#) (on page 129)
- [How Does the Compact Element Versions Task Work?](#) (on page 130)
- [How Does the Archive Log Messages Task Work?](#) (on page 170)
- [How Does a Report Task Work?](#) (on page 186)

To change the properties of a task:

1. In the Manager bar, click **TASKS**.
2. In the tree pane, click the task group containing the task.
3. In the main pane, select the task in the **Name** column.
4. As needed, modify the tabs in the task properties dialog. For tab descriptions, see [Table 112 on the next page](#).

Tip For more information, click  **Help** in any tab.

5. Click **OK**.

Next If you modified a check rule task, you should create new baselines for the elements monitored by the task. For instructions, see [Creating Current Baselines for a Check Rule Task on page 522](#).

Table 112. Tabs in task properties

Tab	Available with these types of tasks ...	Description
Actions	Check rule	Specifies any actions or action groups to be run when a change is detected by the task.
Delivery	Report	Identifies the recipients and format of report output e-mailed by the task.
Details	Archive Log Messages Compact Element Versions	In the Archive Log Messages Task, this tab defines criteria that determine which TE log messages are archived by the task. In the Compact Element Versions Task, this tab defines criteria that determine which element versions are compacted and archived by the task.
General	All tasks	Specifies the task's name, description (optional), and other properties. Note: The default names of the Archive Log Messages Task and Compact Element Versions Task should not be changed. If you change the name of either task, the task name will no longer match Tripwire Enterprise documentation.
Nodes	Baseline rule Check rule	Specifies the node or node group to be baselined or version checked by the task.
Parent Groups	All tasks	Displays the full path of each task group to which the task is linked. <ul style="list-style-type: none"> This tab includes some of the same buttons that appear in the Task Manager. For guidance in using these buttons, refer to the corresponding procedure in this chapter. To view or edit the properties of a task group, select the group's link. (For more information, see Changing the Properties of a Task Group on the next page.)
Report	Report	Specifies the report or dashboard to be run by the task.
Rules	Baseline rule Check rule	Specifies the rule or rule group that identifies the monitored objects to be baselined or version checked by the task.
Schedule	All tasks	Defines a schedule that runs the task at regular intervals or at specific times. Notes: Compacting and creating element versions concurrently may result in deadlocking your TE Console database. Therefore, you should not schedule the Compact Element Versions Task to run at the same time as a baseline rule task or check rule task. If a task is disabled, TE ignores the task's schedule. To enable a task, see Enabling Tasks on page 523.
Scope	Baseline rule	This tab determines if the task will create current baselines for all monitored objects, or just monitored objects that lack a current baseline.
Security	All tasks	Contains any access controls that have been created for the task. For more information, see Working with Task Access Controls on page 515.

Changing the Properties of a Task Group

Tip This procedure explains how to change the properties of a task group displayed in the main pane of the Task Manager. However, you can also change the properties of a task group in the **Parent Groups** tab of a task properties dialog (see [Changing the Properties of a Task on page 512](#)).

To change the properties of a task group:

1. In the Manager bar, click **TASKS**.
2. In the tree pane, click the group containing the task group.
3. In the **Name** column, select the task group.
4. As needed, modify the tabs in the task group properties dialog. For tab descriptions, see [Table 113](#).

Tip For more information, click  **Help** in any tab.

5. Click **OK**.

Table 113. Tabs in task group properties

Tab	Description
General	The name and description (optional) of the task group.
Parent Groups	Displays the full path of each task group to which this task group is linked. <ul style="list-style-type: none">• This tab includes some of the same buttons that appear in the Task Manager. For guidance in using these buttons, refer to the corresponding procedure in this chapter.• To view or edit the properties of a task group, select the group's link.
Security	Contains any access controls that have been created for the task group. For more information, see Working with Task Access Controls on the next page .


Working with Task Access Controls

Creating an Access Control for a Task or Task Group

For an introduction to access controls, see [What are Access Controls? on page 208](#).

Note If one or more access controls have already been created for the task or task group, an additional access control can only be created by the default administrator account or a user account assigned to one of the existing access controls.

To set an access control for a task or task group:

1. In the Manager bar, click **TASKS**.
2. In the tree pane, click the group containing the task or task group.
3. In the main pane, click the task or task group in the **Name** column.
4. In the properties dialog, click the **Security** tab.
5. Click  **Add Control**.
6. Select the check box of each **Principal** (user or user group) to be assigned to the access control and click **Next**.
7. Select the user role for the access control and click **Finish**.

Changing an Access Control for a Task or Task Group

For an introduction to access controls, see [What are Access Controls? on page 208](#).

Note An access control can only be changed by the default administrator account or a user account assigned to the control.

To change the user role assigned to an access control:

1. In the Manager bar, click **TASKS**.
2. In the tree pane, click the group containing the task or task group associated with the access control.
3. In the main pane, click the task or task group in the **Name** column.
4. In the properties dialog, click the **Security** tab.
5. In the **Access Control** column, select the access control.
6. In the Access Control dialog, select the new user role and click **OK**.

Deleting Access Controls for a Task or Task Group

Note An access control can only be deleted by the default administrator account or a user account assigned to the control.

Caution With an access control, non-Administrators may be granted Administrator-level access to a particular task or task group. If the access control is deleted, the user will no longer be able to modify the properties of the task or task group.

To delete an access control from a task or task group:

1. In the Manager bar, click **TASKS**.
2. In the tree pane, click the group containing the task or task group associated with the access control.
3. In the main pane, click the task or task group in the **Name** column.
4. In the properties dialog, select the **Security** tab.
5. Select the check box of each access control to be deleted.
6. Click **✕ Delete**.
7. Click **OK** to confirm.


Creating and Deleting Objects in the Task Manager


Creating a Baseline Rule Task

For an introduction to baseline rule tasks, see [How Does a Baseline Rule Task Work?](#) on page 128.

To create a baseline rule task, the **Create Tasks** permission must be assigned to your user account. For more information, see [What are User Permissions and User Roles?](#) on page 204.

To create a baseline rule task:

1. In the Manager bar, click **TASKS**.
2. In the tree pane, click the task group in which the new task will be created.
3. Click **Manage** >  **New Task**.
4. In the New Task dialog, select **Baseline Rule Task** and click **OK**.
5. Complete the New Baseline Rule Task Wizard.

Tips For more information, click  **Help** in any wizard page.

If you select **Selected nodes with currently assigned rules** in the Rules page of the wizard, the task can only baseline a node if the node has been baselined prior to running the task for the first time. If a node has not been previously baselined when the task is run, the task will have no effect on the node.

For rule descriptions, see [What are Rule Types?](#) on page 79.

Next To run the task now, see [Running Tasks and Task Groups Manually](#) (on page 523).


To create a schedule for the task, see [Changing the Properties of a Task](#) (on page 512).


Creating a Check Rule Task

For an introduction to check rule tasks, see [How Does a Check Rule Task Work? on page 129](#).

To create a check rule task, the **Create Tasks** permission must be assigned to your user account. For more information, see [What are User Permissions and User Roles? on page 204](#).

To create a check rule task:

1. In the Manager bar, click **TASKS**.
2. In the tree pane, click the task group in which the new task will be created.
3. Click **Manage** >  **New Task**.
4. In the New Task dialog, select **Check Rule Task** and click **OK**.
5. Complete the New Check Rule Task Wizard.

Tips For more information, click  **Help** in any wizard page.

If you select **Selected nodes with currently assigned rules** in the Rules page of the wizard, the task can only version check a node if the node has been baselined prior to running the task for the first time. If a node has not been previously baselined when the task is run, the task will have no effect on the node.

For rule descriptions, see [What are Rule Types? on page 79](#). For action descriptions, see [What are Actions and Action Types? on page 116](#).

Next If you did *not* initialize baselines in the wizard, you must first create current baselines before running the task. For instructions, see [Creating Current Baselines for a Check Rule Task on page 522](#).

If you did initialize baselines, you may now run or schedule the task.


- To run the task now, see [Running Tasks and Task Groups Manually \(on page 523\)](#).
- To create a schedule for the task, see [Changing the Properties of a Task \(on page 512\)](#).


Creating a Report Task

For an introduction to report tasks, see [How Does a Report Task Work? on page 186](#). For report descriptions, see [What are Reports and Report Types? on page 172](#).

To create a report task, the **Create Tasks** permission must be assigned to your user account. For more information, see [What are User Permissions and User Roles? on page 204](#).

To create a new report task:

1. In the Manager bar, click **TASKS**.
2. In the tree pane, click the task group in which the new task will be created.
3. Click **Manage** >  **New Task**.
4. In the New Task dialog, select **Report Task** and click **OK**.
5. In the New Report Task Wizard, enter a **Name** and **Description** (optional) for the task. Then, click **Next**.
6. Complete the remaining wizard pages.


Tip For more information, click  **Help** in any wizard page.

Next To run the task now, see [Running Tasks and Task Groups Manually \(on page 523\)](#).
To create a schedule for the task, see [Changing the Properties of a Task \(on page 512\)](#).

Creating a Task Group

For an introduction to task groups, see [About Groups on page 29](#).

To create a task group:

1. In the Manager bar, click **TASKS**.
2. In the tree pane, click the task group in which to create the new task group.
3. Click **Manage** >  **New Group**.
4. In the New Task Group Wizard, enter a **Name** and **Description** (optional) for the new task group.
5. Click **Finish**.


Next To add existing tasks and task groups to the new group, see:

- [Moving Tasks and Task Groups \(on page 525\)](#)
- [Linking Tasks and Task Groups \(on page 525\)](#)

Duplicating Tasks

With this procedure, you can either duplicate specified tasks in a selected task group, or all tasks in a selected task group.

To create copies of existing tasks:

1. In the Manager bar, click **TASKS**.
2. In the tree pane, click the task group containing the tasks to be duplicated.
3. (Optional) To duplicate specific tasks, select the check box of each task.
4. Click **Manage** >  **Duplicate**.
5. Click **OK** in the confirmation dialog.

Tripwire Enterprise uses the following convention to name a duplicate task:

`<original_task>(<#>)`

where:

`<original_task>` is the name of the task that was duplicated.

`<#>` is a number that increments each time the original task is duplicated (beginning with 1) - for example, `task(1)`, `task(2)`, etc.

Next To run the duplicated task now, see [Running Tasks and Task Groups Manually](#) (on page 523).

To create a schedule for the duplicated task, see [Changing the Properties of a Task](#) (on page 512).

Deleting Tasks and Task Groups

Deletion completely removes a task or task group from your Tripwire Enterprise implementation.

- To deactivate a task without deleting it, see [Disabling Tasks on page 524](#).
- To remove a task or task group from a group *without* deletion, see [Unlinking Tasks and Task Groups on page 526](#).

Note To delete an object, your user account must have Delete permissions for that object, and (for groups) all objects descended from that object. For more information, see [What are User Permissions and User Roles? on page 204](#).

To delete tasks and/or task groups:

1. In the Manager bar, click **TASKS**.
2. In the tree pane, click the task group containing the objects to be deleted.
3. Select the check box for each object to be deleted.
4. Click **Manage > X Delete**.
5. Specify whether or not to run the Clear Unlinked Groups task on all Unlinked groups in TE. For more information on this task, see [What are Task Types? on page 127](#).
6. Click **OK**.

Note If you get an error message when trying to delete objects, an access control (see [What are Access Controls? on page 208](#)) is preventing you from deleting a descendant object. To determine which objects have access controls, check the Objects tab for the Error log message associated with this operation.

Working with Objects in the Task Manager


Creating Current Baselines for a Check Rule Task

Prior to running a **check rule task**, a current baseline must exist for each monitored object checked by the task. When the task is run, Tripwire Enterprise detects changes by comparing the current state of the object with the object's current baseline.

New current baselines should be created in the following cases:

- If you create a new check rule task without initializing baselines (see [Creating a Check Rule Task on page 518](#)).
- If you assign a different node(s) or rule(s) to an existing check rule task (see [Changing the Properties of a Task on page 512](#)).

To create current baselines for a check rule task:

1. In the Manager bar, click **TASKS**.
2. In the tree pane, click the task group containing the check rule task.
3. Select the check box for the task.
4. Click **Control** >  **Baseline**.
5. Select **New baselines only** or **All baselines**.

Tip For more information, click  **Help**.

6. Click **OK**.


Next To run the check rule task now, see [Running Tasks and Task Groups Manually on the next page](#).

To define a schedule for the task, see [Changing the Properties of a Task on page 512](#).

Running Tasks and Task Groups Manually

Caution Compacting and creating element versions concurrently may result in deadlocking your TE Console database. Therefore, you should not run the Compact Element Versions Task at the same time as a baseline rule task or check rule task.


To manually run tasks and/or task groups:

1. In the Manager bar, click **TASKS**.
2. In the tree pane, click the task group containing the objects to be run.
3. Select the check box of each object to be run.
4. Click **Control** >  **Run**.


Stopping Tasks and Task Groups Manually

With this procedure, you can stop a running baseline rule task(s) and/or check rule task(s).


To stop running tasks:

1. In the Manager bar, click **TASKS**.
2. In the tree pane, click the task group containing the tasks and/or a task group containing the tasks to be stopped.
3. Select the check box of each task and/or task group.
4. Click **Control** >  **Stop**.

Enabling Tasks


When a task is enabled, the **enable emblem** overlays the task icon  in the Task Manager.

To enable tasks:

1. In the Manager bar, click **TASKS**.
2. In the tree pane, click the task group containing the tasks to be enabled.
3. Select the check box for each task to be enabled.
4. Click **Control** >  **Enable**.


Next To run the task now, see [Running Tasks and Task Groups Manually](#) above.
To define a schedule for the task, see [Changing the Properties of a Task on page 512](#).

Disabling Tasks

When a task is disabled, the **disable emblem** overlays the task icon  in the Task Manager.

Caution If you disable a task for which a schedule has been defined, the task will not run at its scheduled times.

To disable tasks:


1. In the Manager bar, click **TASKS**.
2. In the tree pane, click the task group containing the tasks to be disabled.
3. Select the check box for each task to be disabled.
4. Click **Control** >  **Disable**.

Moving, Linking, and Unlinking Objects in the Task Manager

Moving Tasks and Task Groups

With this procedure, you can move a task or task group from one task group to another. For example, you can move a task from the **Unlinked** group to another task group.

To move tasks or task groups:

1. In the Manager bar, click **TASKS**.
2. In the tree pane, click the group containing the objects to be moved.
3. In the main pane, select the check box of each task or task group to be moved.
4. Click **Manage** >  **Move**.
5. In the Move Tasks dialog, select the destination task group and click **OK**.


Linking Tasks and Task Groups


When you create a task or task group, the object is linked to the task group in which it was created. As needed, the object may also be linked to other task groups. For more information, see [What are Links and Linked Objects?](#) on page 213.

Tips If you link a task in the **Unlinked** task group, Tripwire Enterprise *moves* the task to the destination task group.

This procedure explains how to link tasks and task groups displayed in the main pane of the Task Manager. However, you can also link task groups in the **Parent Groups** tab of a task properties dialog (see [Changing the Properties of a Task](#) on page 512).

To link tasks and task groups to another task group:

1. In the Manager bar, click **TASKS**.
2. In the tree pane, click the group containing the objects to be linked.
3. Select the check box of each task or task group to be linked.
4. Click **Manage** >  **Link**.
5. Select the destination task group and click **OK**.

Note In the Task Manager, a link  emblem overlays the icon of each task (or task group) that is linked to multiple task groups.

Unlinking Tasks and Task Groups


This procedure unlinks a task or task group from a task group. For more information, see [What are Links and Linked Objects?](#) on page 213.

If you unlink a task or task group from the only task group with which it is linked, Tripwire Enterprise moves the task to the **Unlinked** task group. To retrieve an object from the **Unlinked** group, see [Moving Tasks and Task Groups](#) on the previous page.

Tips To unlink an object, your user account must have Delete and Link permissions for that object, and (for groups) all objects descended from that object. For more information, see [What are User Permissions and User Roles?](#) on page 204.

This procedure explains how to unlink tasks and task groups displayed in the main pane of the Task Manager. However, you can also unlink task groups in the **Parent Groups** tab of a task properties dialog (see [Changing the Properties of a Task](#) on page 512).

To unlink tasks or task groups from a task group:

1. In the Manager bar, click **TASKS**.
2. In the tree pane, click the group containing the objects to be unlinked.
3. Select the check box of each task or task group to be unlinked.
4. Click **Manage** >  **Unlink**.
5. Specify whether or not to run the Clear Unlinked Groups task on all Unlinked groups in TE. For more information on this task, see [What are Task Types?](#) on page 127.
6. Click **OK**.

Note If you get an error message when trying to unlink objects, an access control (see [What are Access Controls?](#) on page 208) is preventing you from unlinking a descendant object. To determine which objects have access controls, check the Objects tab for the Error log message associated with this operation.


Exporting and Importing Objects in the Task Manager

Exporting Tasks and Task Groups

This procedure exports selected tasks and task groups to an XML file. As needed, the contents of the XML file may be re-imported at a later date (see [Importing Tasks and Task Groups on the next page](#)).

Note This procedure explains how to export tasks and task groups displayed in the main pane of the Task Manager. However, you can also export objects in the **Parent Groups** tab of a task properties dialog (see [Changing the Properties of a Task on page 512](#)).

To export tasks and task groups to an XML file:

1. In the Manager bar, click **TASKS**.
2. In the tree pane, click the task group containing the tasks and task groups to be exported.
3. (Optional) To export **specific** tasks and task groups, select the appropriate check boxes. Only objects on the same page of the Task Manager can be selected in a single export operation.
4. Click **Manage** >  **Export**.
5. In the Export Tasks dialog, select one of the following options and click **OK**:
 - **All tasks and task groups**. This option exports all tasks and task groups in your Tripwire Enterprise implementation.
 - **Selected tasks and task groups only**. This option exports the selected tasks and task groups only.
6. To export the XML file to a local directory, complete the standard steps for your system.


Tip If your Web browser is an older version of Internet Explorer, you may need to manually add a **.xml** extension to the end of the file name.

Importing Tasks and Task Groups

This procedure imports the tasks and task groups from an XML file to your Tripwire Enterprise implementation. (To create an XML file containing tasks, see [Exporting Tasks and Task Groups on the previous page](#).)

Caution Prior to this procedure, you should first review the guidelines employed by Tripwire Enterprise when importing the contents of an XML file (see [How Do I Import and Export Tripwire Enterprise Objects? on page 217](#)).

To import the tasks and task groups in an XML file:

1. In the Manager bar, click **TASKS**.
2. In the tree pane, click the task group to which the XML file's contents will be imported. The task group structure defined in the XML file will be created in this location.
3. Click **Manage** >  **Import**.
4. In the Import Tasks dialog, click **Browse**.
5. To locate and select the XML file, complete the standard steps for your system.
6. In the Import Tasks dialog, click **OK**.

Chapter 10. Policy Procedures

Viewing and Changing Objects in the Tests Tab

Viewing Policy Manager Objects in the Tests Tab

For an introduction to Policy Manager objects, see [What are Policy Manager Objects?](#) on page 131.

To view Policy Manager objects in the Tests tab of the Policy Manager:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, select a TE policy or policy test group.
3. In the main pane, select the **Tests** tab (see [Figure 31 below](#)) and review the contents of the selected TE policy or group. [Table 114 \(on the next page\)](#) defines each of the columns in the Tests tab.
 - To **sort** the contents of the Tests tab by the values in a column, click the column header. To reverse the order, click the column header a second time.
 - If the Tests tab contains multiple pages, use the navigation controls at the bottom of the main pane to **scroll** through the pages.
 - To adjust the **maximum table size** setting, see [Changing User Preference Settings](#) on page 262.

Figure 31. The Tests tab in the Policy Manager

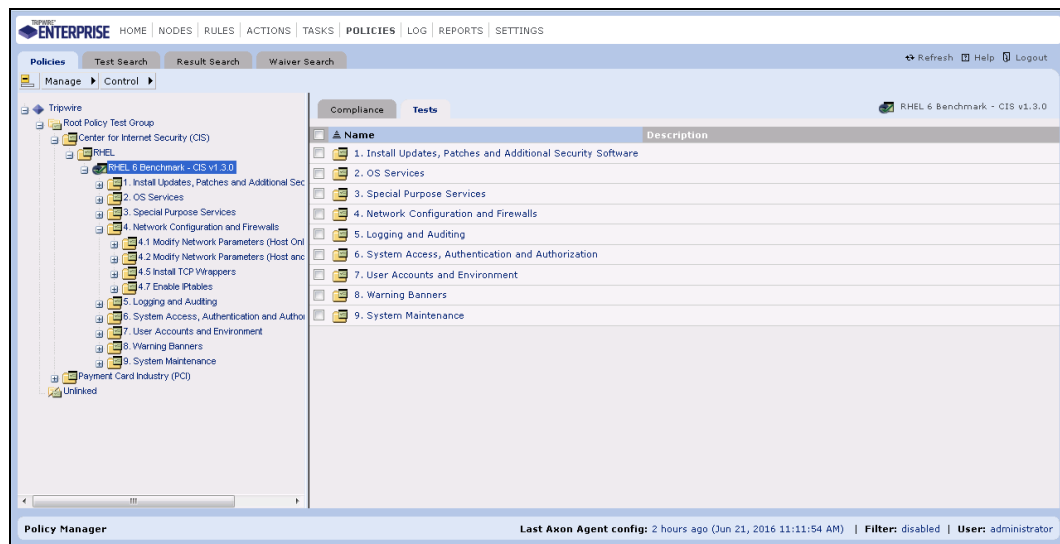


Table 114. Columns in the Tests tab


Column	Description
Name	The Name column lists the names of Policy Manager objects in the selected TE policy or policy test group. To view or change the properties of a Policy Manager object, click a Name link. For more information, see: <ul style="list-style-type: none">• Changing the Properties of a TE Policy on page 534• Changing the Properties of a Policy Test on page 536• Changing the Properties of a Policy Test Group on page 538
Description	This column provides an optional description of each Policy Manager object.

Searching for Policy Tests

Notes For an introduction to common search features such as wildcards, text-field qualifiers, and saved searches, see [How Do I Run a Search? on page 232](#).



In the Test Search tab, the button bar contains many of the same buttons available in the Policies tab. To use these buttons, refer to the procedures in [Chapter 10: Policy Procedures \(on page 529\)](#).



To search for policy tests:

1. In the Manager bar, click **POLICIES**.
2. Select the **Test Search** tab.
3. Enter search criteria. For guidance, see [Table 115 below](#).
 - Some of the search criteria are based on values that can be edited in policy test property dialogs (see [Changing the Properties of a Policy Test on page 536](#)).
 - All text-field entries are case-insensitive. For example, ‘Policy’ and ‘policy’ will return the same results.
 - Any string may be entered in a text field. For example, if you enter a string in the **Name** field, and select **Contains** as the text-field qualifier, search results will include any policy test with a name that includes the string.
4. Click  **Search**.

Next If desired, you can save the entered search criteria for future use. For instructions, see [Creating a Saved Search on page 234](#).

Table 115. Policy test search criteria

Search Criteria	To limit search results to ...
Associated with rule	<p>... policy tests associated with a specific rule or rule group:</p> <ol style="list-style-type: none"> 1. Click  Chooser. 2. Select the rule or group, and click OK. <p>Note: If you select a rule group, search results will include policy tests associated with any rules descended from the group.</p>
Descends from test group	<p>... policy tests that descend from a specific test group:</p> <ol style="list-style-type: none"> 1. Click  Chooser. 2. Select the test group and click OK.

Search Criteria	To limit search results to ...
Description	... policy tests with specific descriptions: <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial description in the text field.
Element name scope	... policy tests that generated results associated with elements that have specific names: <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial element name in the text field.
Has current failures	... policy tests for which at least one current policy test result failed, select Yes policy tests for which all current policy test results passed, select No .
Has current waivers	... policy tests that have at least one waiver, select Yes policy tests that do not have any waivers, select No .
Has remediator	... policy tests that have automated remediation, select Yes policy tests that do not have automated remediation, select No . For more information about automated remediation, see How Does Automated Remediation Work? on page 151.
Name	... policy tests with specific names: <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial name in the text field.
Policy	... policy tests descended from a specified policy: <ol style="list-style-type: none"> 1. Click  Chooser. 2. Select the policy and click OK.
Type	... policy tests of a specific type, select a type from the drop-down list.
With results for node	... policy tests that have generated results for a specific node or node group: <ol style="list-style-type: none"> 1. Click  Chooser. 2. Select the node or node group, and click OK. <p>Note: If you select a node group, search results will include policy tests with results generated for any node descended from the node group.</p>
With weights	... policy tests that have a weight within a specified range, enter values in the fields provided (any range from 1 to 10).

Changing the Properties of a TE Policy

Tip This procedure explains how to change the properties of a TE policy displayed in the Tests tab of the Policy Manager. However, you can also change the properties of a TE policy in the **Parent Groups** tab of a properties dialog for a policy test (see [Changing the Properties of a Policy Test on page 536](#)) or policy test group (see [Changing the Properties of a Policy Test Group on page 538](#)).

For an introduction to TE policies and scopes, see:

- [What are Policy Manager Objects? on page 131](#)
- [What are Scopes and Effective Scopes? on page 133](#)

To change the properties of a TE policy:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the policy test group containing the TE policy.
3. In the main pane, select the **Tests** tab.
4. In the **Name** column, select the link for the TE policy.
5. As needed, modify the tabs in the TE policy properties dialog. For tab descriptions, see [Table 116 on the next page](#).

In the Nodes tab, you can specify nodes and/or node groups for the scope of the TE policy.

- To add a node or node group, click the **Add** button.
- To remove a node or node group, select the object's check box and click **Remove**.
- To remove all nodes and node groups from the scope, click **Clear**.

In the Node Properties tab, you can define one or more conditions.

- To add a condition, click the **Add Condition** button.
- To remove a condition, select the condition's check box and click **Delete**.
- To remove all conditions from the scope, click **Clear**.
- To change a condition's position in the list, select the condition's check box and click **Move Up** or **Move Down**.

6. Click **OK**.

Table 116. Tabs in TE policy properties

Tab	Description
General	Specifies the TE policy's name and description (optional). Also includes a setting that applies or removes a Tracking Identifier to/from the TE policy (see What are Tracking Identifiers? on page 223).
Nodes	Limits the TE policy's scope to specified nodes and/or node groups.
Node Names	Specifies a string in the names of nodes to be included in or excluded from the TE policy's scope.
Node Properties	Limits the TE policy's scope to nodes with custom properties that have specified values.
Parent Groups	<p>Displays the full path of each policy test group that contains the TE policy.</p> <ul style="list-style-type: none"> This tab includes some of the same buttons that appear in the Policy Manager. For guidance in using these buttons, refer to the corresponding procedure in this chapter. To view or edit the properties of a policy test group, select the group's link. (For more information, see Changing the Properties of a Policy Test Group on page 538.)
Purge Settings	Determines if TE will regularly purge old test results and waivers for the TE policy and, if so, defines the associated purge criteria. For more information, see How Do I Purge Policy Data from Tripwire Enterprise? on page 145 .
Scoring Thresholds	Contains all scoring thresholds defined for the TE policy. For more information, see What are Scoring Thresholds? (on page 142) and Working with Scoring Thresholds (on page 555) .
Security	Contains any access controls for the TE policy. For more information, see What are Access Controls? (on page 208) and Working with Policy Access Controls (on page 541) .
Waivers	Contains all waivers defined for the TE policy. For more information, see What are Policy Scores? (on page 138) .
Weights	Specifies the weight of each policy test and/or policy test group nested on the top level of the TE policy. For more information, see What are Policy Scores? (on page 138) .

Changing the Properties of a Policy Test

For an introduction to policy tests and scopes, see:

- [What are Policy Manager Objects? on page 131](#)
- [What are Scopes and Effective Scopes? on page 133](#)

To change the properties of a policy test:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the TE policy or policy test group containing the policy test.
3. In the main pane, select the **Tests** tab.
4. In the **Name** column, select the link for the policy test.
5. As needed, modify the tabs in the policy test properties dialog. For tab descriptions, see [Table 117 on the next page](#).

In the Excluded Nodes and Rules tabs, you can specify TE objects for the scope of the policy test.

- To add an object, click the **Add** button.
- To remove an object, select the object's check box and click **Remove**.
- To remove all objects from the scope, click **Clear**.

In the Conditions and Included Node Properties criteria, you can define one or more conditions for the policy test.

- To add a condition, click the **Add Condition** button.
- To remove a condition, select the condition's check box and click **Delete**.
- To remove all conditions from the test, click **Clear**.
- To change a condition's position in the list, select the condition's check box and click **Move Up** or **Move Down**.

6. Click **OK**.

Table 117. Tabs in policy test properties

Tab	Available with ...	Description
Conditions	... all policy tests	Conditions that define pass/fail criteria for the policy test. Pass/fail criteria vary between policy test types (see Table 41 on page 132).
Details	... Windows ACL tests	Includes settings that determine how conditions defined in the Conditions tab will be evaluated when the test runs.
Excluded Nodes	... all policy tests	Specifies nodes and/or node groups to be excluded from the scope of the policy test. Tip: To modify this tab for multiple policy tests, see Changing the List of Excluded Nodes for Multiple Policy Tests on page 540 .
General	... all policy tests	Specifies the policy test's name, description (optional), and severity level. Also includes a setting that applies or removes a Tracking Identifier to/from the test (see What are Tracking Identifiers? on page 223).
Included Node Properties	... all policy tests	Limits the policy test's scope to nodes with custom properties that have specified values. Tip: To modify this tab for multiple policy tests, see Changing the Included Node Properties of Multiple Policy Tests on page 539 .
Parent Groups	... all policy tests	Displays the full path of each TE policy and policy test group that contains the policy test. <ul style="list-style-type: none"> This tab includes some of the same buttons that appear in the Policy Manager. For guidance in using these buttons, refer to the corresponding procedure in this chapter. To view or edit the properties of a TE policy or policy test group, select the object's link. For more information, see Changing the Properties of a TE Policy (on page 534) and Changing the Properties of a Policy Test Group (on the next page).
Remediation	... all policy tests	May include manual remediation instructions for the policy test. For more information, see About Remediation on page 151 .
Remediator	... all policy tests	May include automated remediation information for the policy test. For more information, see About Remediation on page 151 .
Rules	... all policy tests	Limits the policy test's scope to elements that represent monitored objects identified by one or more specified rules.
Scope	... all policy tests	Limits the policy test's scope to elements with names that satisfy a specified criterion.
Security	... all policy tests	Contains any access controls that have been created for the test. For more information, see What are Access Controls? (on page 208) and Working with Policy Access Controls (on page 541) .
Waivers	... all policy tests	Displays all waivers defined for the policy test by the test's parent policies. For more information, see What are Policy Scores? (on page 138) .

Changing the Properties of a Policy Test Group

Tip This procedure explains how to change the properties of a policy test group displayed in the Tests tab of the Policy Manager. However, you can also change the properties of a group in the **Parent Groups** tab of a properties dialog for a TE policy (see [Changing the Properties of a TE Policy on page 534](#)) or policy test (see [Changing the Properties of a Policy Test on page 536](#)).

To change the properties of a policy test group:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the group or TE policy containing the policy test group to be modified.
3. In the main pane, select the **Tests** tab.
4. In the **Name** column, select the link for the policy test group.
5. As needed, modify the tabs in the group properties dialog. For tab descriptions, see [Table 118](#).

Tip For more information, click  **Help** in any tab.

6. Click **OK**.

Table 118. Tabs in policy test group properties

Tab	Description
General	The name and description (optional) of the policy test group.
Parent Groups	Displays the full path of each TE policy and policy test group that contains the group. <ul style="list-style-type: none">• This tab includes some of the same buttons that appear in the Policy Manager. For guidance in using these buttons, refer to the corresponding procedure in this chapter.• To view or edit the properties of a TE policy or policy test group, select the object's link. For more information, see this procedure and Changing the Properties of a TE Policy (on page 534).
Security	Contains any access controls that have been created for the policy test group. For more information, see What are Access Controls? (on page 208) and Working with Policy Access Controls (on page 541) .
Weights	Specifies the weight of each policy test and/or policy test group nested on the top level of the group. For more information, see What are Policy Scores? (on page 138) .

Changing the Properties of Multiple Policy Tests

Changing the Included Node Properties of Multiple Policy Tests

With this procedure, you can modify the conditions defined in the Included Node Properties tab (see [Table 117 on page 537](#)) of one or more policy tests. Specifically, you can create new conditions that will either replace or be added to the existing conditions for the specified tests.


Tip This procedure explains how to modify the conditions of tests in the Tests tab of the Policies tab in the Policy Manager. However, you can also modify the conditions of multiple tests in:


- The Test Search tab of the Policy Manager (see [Searching for Policy Tests on page 532](#))
- The Result Search tab of the Policy Manager (see [Searching for Policy Test Results on page 559](#))

To change the conditions defined for node custom properties in multiple policy tests:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the TE policy or policy test group containing the policy tests to be modified.
3. In the main pane, select the **Tests** tab.
4. To modify all policy tests descended from the selected TE policy or group, proceed to [step 5](#) below.

To modify specific policy tests, or all tests in specific TE policies and/or groups, select the appropriate check boxes. (Only Policy Manager objects on the same page of the Tests tab can be selected in a single operation.)

5. Click  **Nodes**.
6. If TE presents a confirmation dialog, read the text and click **OK**.
7. In the Update Selected Tests dialog, select **Update included node properties** and click **OK**.
8. Complete the Change Test Included Node Properties Wizard.

Tip For more information, click  **Help** in any wizard page.


Changing the List of Excluded Nodes for Multiple Policy Tests


With this procedure, you can modify the list of nodes and node groups in the Excluded Nodes tab (see [Table 117 on page 537](#)) of one or more policy tests. Specifically, you can specify nodes and/or node groups that will either replace or be added to the existing list in the Excluded Nodes tab of each specified test.

To change the list of excluded nodes for multiple policy tests:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the TE policy or policy test group containing the policy tests to be modified.
3. In the main pane, select the **Tests** tab.
4. To modify all policy tests descended from the selected TE policy or group, proceed to [step 5](#) below.

To modify specific policy tests, or all tests in specific TE policies and/or groups, select the appropriate check boxes. (Only Policy Manager objects on the same page of the Tests tab can be selected in a single operation.)

5. Click  **Nodes**.
6. If TE presents a confirmation dialog, read the text and click **OK**.
7. In the Update Selected Tests dialog, select **Update excluded nodes** and click **OK**.
8. Complete the Change Test Excluded Nodes Wizard.

Tip For more information, click  **Help** in any wizard page.


Working with Policy Access Controls

Creating Access Controls for a Policy Manager Object

For an introduction to access controls, see [What are Access Controls? on page 208](#).

Note If one or more access controls have already been created for the Policy Manager object, an additional access control can only be created by the default administrator account or a user account assigned to one of the existing access controls.

To create access controls for a Policy Manager object:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the TE policy or group containing the Policy Manager object.
3. In the main pane, select the **Tests** tab.
4. In the **Name** column, select the link for the Policy Manager object.
5. In the properties dialog, select the **Security** tab.
6. Click  **Add Control**.
7. Select the check box of each **Principal** (user or user group) to be assigned to an access control and click **Next**.
8. Select the user role for the access controls and click **Finish**.

Changing an Access Control for a Policy Manager Object

For an introduction to access controls, see [What are Access Controls? on page 208](#).

Note An access control can only be changed by the default administrator account or a user account assigned to the control.

To change the user role assigned to an access control for a Policy Manager object:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the TE policy or policy test group containing the Policy Manager object.
3. In the main pane, select the **Tests** tab.
4. In the **Name** column, select the link for the Policy Manager object.
5. In the properties dialog, click the **Security** tab.
6. In the **Access Control** column, select the access control.
7. In the Access Control dialog, select the new role and click **OK**.

Deleting Access Controls for a Policy Manager Object

Note An access control can only be deleted by the default administrator account or a user account assigned to the control.

Caution With an access control, non-Administrators may be granted Administrator-level access to a particular Policy Manager object. If the access control is deleted, the user will no longer be able to modify the properties of the Policy Manager object.

To delete an access control from a Policy Manager object:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the group containing the Policy Manager object.
3. In the main pane, select the **Tests** tab.
4. In the **Name** column, select the link for the Policy Manager object.
5. In the properties dialog, select the **Security** tab.
6. Select the check box of each access control to be deleted.
7. Click **✖ Delete**.
8. Click **OK** to confirm.


Creating and Deleting Objects in the Policy Manager


Creating a TE Policy


For an introduction to TE policies, see:



- [What are Policy Manager Objects?](#) (on page 131)
- [What are Scopes and Effective Scopes?](#) (on page 133)
- [What are Scoring Thresholds?](#) (on page 142)

To create a TE policy:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the policy group in which to create the new TE policy.
3. In the main pane, select the **Tests** tab.
4. Click  **New Policy**.
5. In the New Policy Wizard:
 - a. Enter a **Name** and **Description** (optional).
 - b. (Optional) To assign a Tracking Identifier to the TE policy, select **Enable Tracking Identifier** (see [What are Tracking Identifiers?](#) on page 223).
 - c. Click **Next**.

Tip For more information, click  **Help** in any wizard page.

6. (Optional) To limit the TE policy's scope to specific nodes and/or node groups, complete the following steps and click **Next**.
 - a. Click  **Add**.
 - b. In the Chooser dialog, select a node or node group.
 - c. Click **Add**.
 - d. Repeat steps **b** and **c** above to add further nodes and/or node groups. Then, click **OK**.
7. (Optional) To limit the scope to nodes with names that include or exclude a specified string, select a qualifier from the drop-down and enter the string in the text field. Then, click **Next**.

8. (Optional) To limit the scope to nodes with conditional properties that have specific values, add one or more conditions and click **Next**.
 - a. Click  **Add Condition**.
 - b. In the new line, enter the parameters for the condition.
 - c. Repeat steps a and b to add all desired conditions.
9. Specify the purge settings for test results generated by the TE policy's tests, and click **Next**.
10. Define the scoring thresholds for the TE policy. To add a threshold:
 - a. Click  **New Threshold**.
 - b. In the New Scoring Threshold Wizard, enter a **Name** and **Description** (optional), and click **Next**.
 - c. Specify a **Score** and **Color** for the threshold.
 - d. Click **Finish**.
11. Once all scoring thresholds have been defined for the TE policy, click **Finish** in the New Policy Wizard.


Next To add existing policy tests and policy test groups to the new TE policy, see:


- [Moving Policy Manager Objects \(on page 570\)](#)
- [Linking Policy Manager Objects \(on page 571\)](#)


Creating a Policy Test




For an introduction to policy tests, see [What are Policy Manager Objects? on page 131](#).

To create a content policy test, attribute policy test, or Windows ACL policy test:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the TE policy or policy test group in which to create the new test.
3. In the main pane, select the **Tests** tab.
4. Click  **New Policy Test**.
5. In the Create Policy Test dialog, select a test type and click **OK**.
6. In the New Test Wizard:
 - a. Enter a **Name**, **Description** (optional), and **Default Severity**.
 - b. (Optional) To assign a Tracking Identifier to the policy test, select **Enable Tracking Identifier** (see [What are Tracking Identifiers? on page 223](#)).
 - c. Click **Next**.

Tip For more information, click  **Help** in any wizard page.

7. To assign one or more rules to the test's scope:
 - a. Click  **Add**.
 - b. In the Chooser dialog, select a rule.
 - c. Click **Add**.
 - d. Repeat steps **b** and **c** above to assign any additional rules to the test's scope. Then, click **OK**.
 - e. In the New Test Wizard, click **Next**.
8. (Optional) To limit the test's scope to elements with names that include or exclude a specified string, select a qualifier from the drop-down and enter the string in the text field. Then, click **Next**.
9. (Windows ACL policy tests only) Select SACL or DACL from the **Type** drop-down, complete the remaining fields, and click **Next**.

10. To define pass/fail conditions for the test:
 - a. From the first drop-down on this page, select an option to indicate how the test should respond to element versions that lack content or attributes specified by the test's conditions.
 - b. (Policy content tests only) Select a **Style**.
 - c. Create the conditions that define the pass/fail criteria for the test.
To create a condition, click  **Add Condition** and define the condition's parameters in the new line.
 - d. Once all conditions have been added, click **Next**.
11. (Optional) To limit the test's scope to nodes with conditional properties that have specific values, add one or more conditions and click **Next**.
 - a. Click  **Add Condition**.
 - b. In the new line, enter the parameters for the condition.
 - c. Repeat steps **a** and **b** to add all desired conditions.
12. (Optional) To exclude specific nodes and/or node groups from the test's scope, complete the following steps and click **Next**.
 - a. Click  **Add**.
 - b. In the Chooser dialog, select a node and/or node group.
 - c. Click **Add**.
 - d. Repeat steps **b** and **c** above to add any other nodes and node groups. Then, click **OK**.
13. (Optional) Enter manual remediation instructions for the test, and click **Next**.
14. (Optional) Enter automated remediation information for the test and click **Finish**.


Next To add the policy test to existing TE policies and policy test groups, see:

- [Moving Policy Manager Objects \(on page 570\)](#)
- [Linking Policy Manager Objects \(on page 571\)](#)

Creating a Policy Test Group

For an introduction to policy test groups, see [What are Policy Manager Objects? \(on page 131\)](#) and [About Groups \(on page 29\)](#).

To create a policy test group:


1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the TE policy or policy test group in which to create the new group.
3. In the main pane, select the **Tests** tab.
4. Click  **New Group**.
5. In the New Policy Test Group Wizard:
 - a. Enter a **Name** and **Description** (optional).
 - b. (Optional) To assign a Tracking Identifier to the group, select **Enable Tracking Identifier** (see [What are Tracking Identifiers? on page 223](#)).
6. Click **Finish**.

Next To add existing TE policies, policy tests, and test groups to the new group, see:

- [Moving Policy Manager Objects \(on page 570\)](#)
- [Linking Policy Manager Objects \(on page 571\)](#)

Duplicating Policy Tests

To create copies of existing policy tests:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the TE policy or policy test group containing the policy tests to be duplicated.
3. In the main pane, select the **Tests** tab.
4. Select the check box of each test to be duplicated.
5. Click  **Duplicate**.
6. Click **OK** in the confirmation dialog.

Tripwire Enterprise creates each duplicated test in the selected TE policy or policy test group, and uses the following convention to name the test:

```
<original_test>(<#>)
```

where:

<original_test> is the name of the policy test that was duplicated.

<#> is a number that increments each time the original policy test is duplicated (beginning with 1) - for example, test(1), test(2), etc.

Deleting Policy Manager Objects

Deletion completely removes a Policy Manager object from your Tripwire Enterprise implementation. In other words, deletion will remove the object from all TE policies and policy test groups with which it is linked. To remove a Policy Manager object from a TE policy or policy test group *without* deletion, see [Unlinking Policy Manager Objects on page 572](#).

Note To delete an object, your user account must have Delete permissions for that object, and (for groups) all objects descended from that object. For more information, see [What are User Permissions and User Roles? on page 204](#).

To delete Policy Manager objects:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the TE policy or policy test group containing the objects to be deleted.
3. In the main pane, select the **Tests** tab.
4. To delete all Policy Manager objects in the current view, proceed to [step 5](#) below.

To delete **specific** Policy Manager objects, select the check box for each object. (In this case, only objects on the same page of the Policy Manager can be deleted in a single operation.)

5. Click **✘ Delete**.
6. Specify whether or not to run the Clear Unlinked Groups task on all Unlinked groups in TE. For more information on this task, see [What are Task Types? on page 127](#).
7. Click **OK**.

Note If you get an error message when trying to delete objects, an access control (see [What are Access Controls? on page 208](#)) is preventing you from deleting a descendant object. To determine which objects have access controls, check the Objects tab for the Error log message associated with this operation.

Viewing Results in the Compliance Tab

Viewing Policy Manager Objects in the Compliance Tab

With this procedure, you can review the compliance statistics for Policy Manager objects. For an introduction to compliance statistics, see [How Do I Monitor Compliance Statistics? on page 137](#).

To view objects in the Compliance tab of the Policy Manager:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, select a Policy Manager object.
3. In the main pane, select the **Compliance** tab. This tab displays the compliance statistics for the selected Policy Manager object, as well as a table of nodes with relevant test results.
 - If you selected a **policy test**, the Compliance tab ([Figure 32 on the next page](#)) displays the data described in [Table 119 on the next page](#).
 - If you selected a **policy test group**, the Compliance tab ([Figure 33 on page 552](#)) shows the data described in [Table 120 on page 552](#).
 - If you selected a **TE policy**, the Compliance tab ([Figure 34 on page 553](#)) presents the data described in [Table 121 on page 553](#). (For further details, see [What are Policy Scores? on page 138](#).)

To sort nodes in the Compliance tab, you can select the following column headers in the node table:

- If you selected a **policy test** or **policy test group**, click the column header for the Node or Type columns. To reverse the order, click the column header a second time.
- If you selected a **TE policy**, click the column header for the Node, Score, Without Waivers, or Waived Tests columns. To reverse the order, click the column header a second time.

Tips If the Compliance tab contains multiple pages of nodes, use the navigation controls at the bottom of the main pane to **scroll** through the pages.

To adjust the Policy Manager **refresh rate** or **maximum table size** settings, see [Changing User Preference Settings on page 262](#).

Note If the Policy Manager filter is enabled with the **Only consider nodes in the scope of the selected policy** check box selected, Compliance tab data may be limited to nodes in the scopes of TE policies.

- If you selected a **policy test** or **policy test group** that is not descended from a TE policy, this filter setting has no effect on the data.
- If you selected a **TE policy**, or a policy test or policy test group descended from a TE policy, the data will be limited to nodes in the scope of the TE policy.

Figure 32. Compliance tab for a policy test

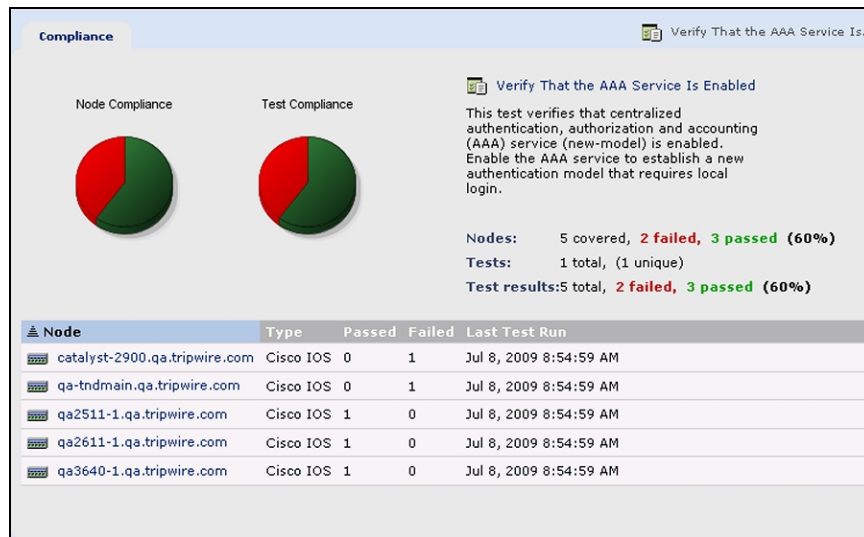


Table 119. Compliance statistics for a policy test

Statistics	Description
Node Compliance	Of all nodes for which the selected test has generated at least one policy test result, these figures indicate the total number and percentage that are in full compliance with the test. (A node is in full compliance when it has no elements that failed the last run of the policy test.)
Test Compliance	Of all the policy test results generated from the last run of the policy test, these figures indicate the total number and percentage of results that passed and failed.
Node table	This table contains a list of all nodes for which the selected policy test has generated at least one test result. For each node, the table indicates the number of policy tests that passed or failed the last run of the test.

Figure 33. Compliance tab for a policy test group

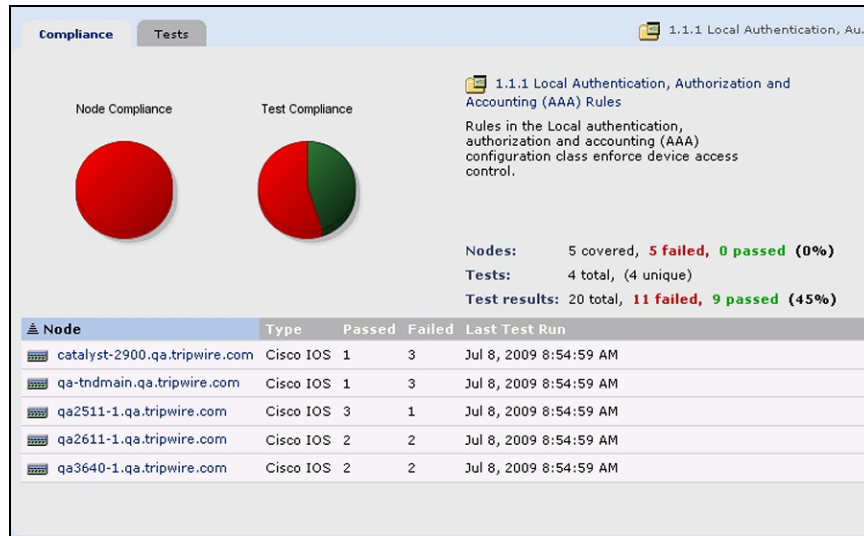


Table 120. Compliance statistics for a policy test group

Statistics	Description
Node Compliance	Of all nodes for which at least one of the policy tests in the selected group has generated a test result, these figures indicate the total number and percentage that are in full compliance with the group. (A node is in full compliance when it has no elements that failed the last run of any policy test in the group.)
Test Compliance	Of all the policy test results generated by the last run of the policy tests in the selected group, these figures indicate the total number and percentage of results that passed and failed.
Node table	This table contains a list of all nodes for which the policy tests in the selected group have generated at least one test result. For each node, the table indicates the number of policy tests that passed and failed the last run of their respective tests.

Figure 34. Compliance tab for a TE policy

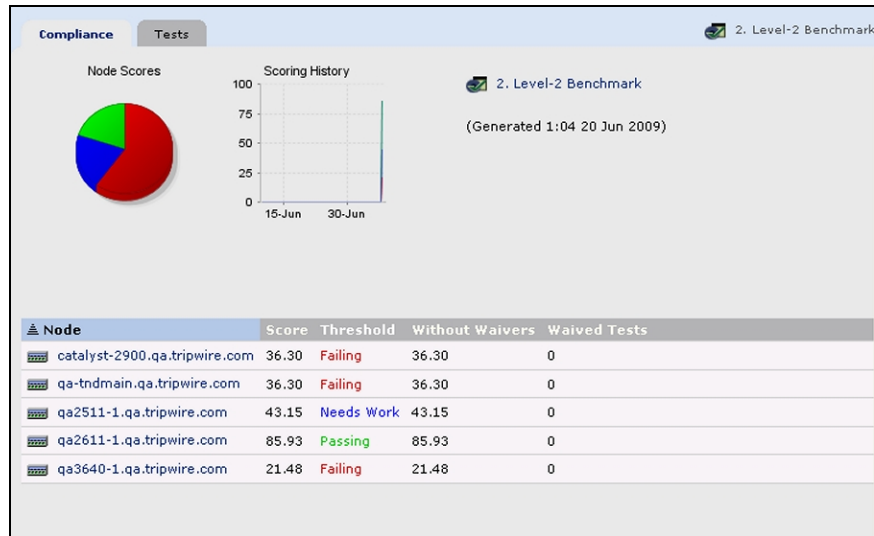


Table 121. Compliance statistics for a TE policy

Statistics	Description
Node Scores	Of all nodes for which at least one policy test result has been generated by the TE policy's tests, this chart indicates the percentage with a policy score that exceeds each of the policy's scoring thresholds. In the chart, each color represents a scoring threshold. For more information, see What are Policy Scores? (on page 138) and What are Scoring Thresholds? (on page 142) .
Scoring History	Of all nodes for which at least one policy test result has been generated by the TE policy's tests, this graph displays three historic trendlines that represent the following data: <ul style="list-style-type: none"> • The highest policy score generated for any of the nodes. • The lowest policy score generated for any of the nodes. • The weighted average of the policy scores for all of the nodes. To adjust the time units and span presented in Scoring History graphs, see Filtering Compliance Statistics in the Policy Manager (on page 557) . For more information, see What are Policy Scores? (on page 138) .
Node table	This table contains a list of all nodes for which at least one policy test result has been generated by the TE policy's tests. For each node, the table presents the following columns. <ul style="list-style-type: none"> • Score indicates the node's current policy score. • Threshold presents the name of the highest scoring threshold exceeded by the node's current policy score. • Without Waivers displays the node's current policy score if all applicable waivers are omitted from the calculation. • Waived Tests indicates the number of failed test results waived by TE in calculating the node's current policy score.

Viewing Policy Test Results from the Compliance Tab

With this procedure, you can review the details of policy test results that have been generated for a node. For an introduction to policy test results, see [How Does a Policy Test Work?](#) on page 135.

To view a node's policy test results from the Compliance tab:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, select a Policy Manager object that contains at least one policy test result for the node.
3. In the main pane, select the **Compliance** tab. This tab displays the compliance statistics for the selected Policy Manager object, as well as a list of nodes with relevant test results. (For more information about compliance statistics, see [How Do I Monitor Compliance Statistics?](#) on page 137.)
4. In the list of nodes, select the node's link in the **Node** column. The **Test Results** tab of the node's properties dialog opens (see [Figure 35](#) below).
5. To view the properties of a policy test result, complete the following steps:
 - a. In the tree pane of the Test Results tab, select a policy test.
 - b. In the main pane, select the policy result in the **Date** column.
 - c. Review the tabs in the policy result properties dialog (see [Figure 36](#) on the next page). For tab descriptions, see [Table 122](#) on the next page.


Tip For more information, click  **Help** in any tab.

Figure 35. Test Results tab in node properties dialog

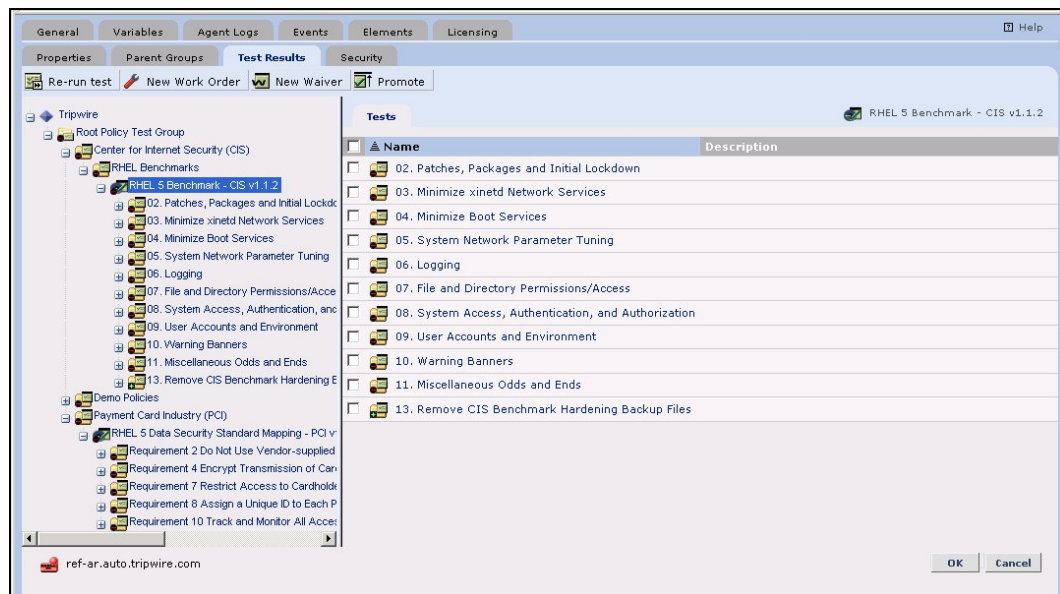


Figure 36. A test result properties dialog



Table 122. Tabs in a Policy Result Properties dialog


Tab	Description
General	Displays general information about the objects associated with the policy test results.
Actual Values	Shows the element's content or attribute values at the time the test was run.
History	Lists all of the test results that have been generated for the element.

Working with Scoring Thresholds

Creating a Scoring Threshold for a TE Policy

For an introduction to scoring thresholds, see [What are Scoring Thresholds? on page 142](#).


To create a scoring threshold for a TE policy:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the group containing the TE policy.
3. In the main pane, select the **Tests** tab.
4. In the **Name** column, select the link for the TE policy.
5. In the properties dialog, select the **Scoring Thresholds** tab.
6. Click  **New Threshold**.
7. Enter a **Name** and **Description** (optional) for the threshold, and click **Next**.
8. Specify a **Score** and **Color** for the threshold, and click **Finish**.

Changing a Scoring Threshold for a TE Policy

To change the properties of a scoring threshold for a TE policy:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the group containing the TE policy.
3. In the main pane, select the **Tests** tab.
4. In the **Name** column, select the link for the TE policy.
5. In the properties dialog, select the **Scoring Thresholds** tab.
6. In the **Name** column, select the link for the scoring threshold.
7. In the threshold properties dialog, edit the tabs and click **OK**.

Tip For more information, click  **Help** in any tab.

Deleting Scoring Thresholds for a TE Policy

For an introduction to scoring thresholds, see [What are Scoring Thresholds?](#) on page 142.

To delete scoring thresholds for a TE policy:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the group containing the TE policy.
3. In the main pane, select the **Tests** tab.
4. In the **Name** column, select the link for the TE policy.
5. In the properties dialog, select the **Scoring Thresholds** tab.
6. Select the check box of each scoring threshold to be deleted.

Note The default Failing threshold cannot be deleted.

7. Click  **Delete**.
8. Click **OK** to confirm.

Filtering Compliance Statistics in the Policy Manager

In you enable filtering in the Policy Manager, specified filter criteria influence the calculations of compliance statistics in the Compliance tab (see [How Do I Monitor Compliance Statistics?](#) on page 137).


To enable or disable filtering:

1. In the Manager bar, click **POLICIES**.
2. In the lower right-hand corner of the Policy Manager, click the **Filter** link.
3. In the Policy Filter dialog, select the **General** tab.
4. Select or clear the **Filter enabled** check box.
5. Click **OK**.

If the Policy Manager filter is enabled, filter criteria influence the calculation of compliance statistics displayed in the Compliance tab of the Policy Manager.

To change filter criteria for the Policy Manager:

1. In the Manager bar, click **POLICIES**.
2. In the lower right-hand corner of the Policy Manager, click the **Filter** link.
3. As needed, modify the filter criteria in the Filter Settings dialog (see [Table 123 on the next page](#)).

Tip For more information, click  **Help** in any tab.

4. In the Filter Settings dialog, click **OK**.

Table 123. Tabs in the Filter Settings dialog of the Policy Manager


Tab	Description
General	<p>This tab consists of the following fields:</p> <ul style="list-style-type: none">• Filter enabled. Enables or disables filtering.• Only consider nodes in the scope of the selected policy. If a Policy Manager object is a TE policy, or is contained in a TE policy, this setting limits compliance statistics to nodes in the scope of the TE policy. For more information, see What are Scopes and Effective Scopes? on page 133.• Show scores in charts and calculate ranges without considering waivers. This setting omits waivers from policy score calculations (see What are Policy Scores? on page 138).• Scoring history includes last. Specifies the time period displayed in Scoring History charts in the Compliance tabs of TE policies (see How Do I Monitor Compliance Statistics? on page 137).
Nodes	<p>This tab may specify one or more nodes or groups to limit the calculation of compliance statistics.</p> <ul style="list-style-type: none">• If no nodes are specified, the Compliance tab displays compliance statistics for all nodes with test results for the Policy Manager object selected in the tree pane.• If one or more nodes are specified, the Compliance tab limits compliance statistics to nodes that are 1) specified here, and 2) have test results for the selected Policy Manager object.

Searching for Policy Test Results

Notes For an introduction to common search features such as wildcards, text-field qualifiers, and saved searches, see [How Do I Run a Search? on page 232](#).






In the Result Search tab, the button bar contains many of the same buttons available in the Policies tab. To use these buttons, refer to the procedures in [Chapter 10: Policy Procedures \(on page 529\)](#).

To search for policy test results:

1. In the Manager bar, click **POLICIES**.
2. Select the **Result Search** tab.
3. Enter search criteria. For guidance, see [Table 124 on the next page](#).
 - Some of the search criteria are based on values that can be edited in policy test property dialogs (see [Changing the Properties of a Policy Test on page 536](#)).
 - All text-field entries are case-insensitive. For example, 'Policy' and 'policy' will return the same results.
 - Any string may be entered in a text field. For example, if you enter a string in the **Test name** field, and select **Contains** as the text-field qualifier, search results will include any results for a policy test with a name that includes the string.
4. Click  **Search**.

Next If desired, you can save the entered search criteria for future use. For instructions, see [Creating a Saved Search on page 234](#).

Table 124. Policy test result search criteria

Search Criteria	To limit search results to ...
Current results only	... only the latest results generated for policy tests, select Yes .
Element name scope	... results associated with elements that have specific names: <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial element name in the text field.
Has remediator	... results generated by policy tests that have automated remediation, select Yes results generated by policy tests that do not have automated remediation, select No . For more information about automated remediation, see How Does Automated Remediation Work? on page 151 .
Has waiver	... results generated by policy tests that have at least one waiver, select Yes results generated by policy tests that do not have any waivers, select No .
Node or node group	... results generated by policy tests associated with a specific node or descended from a node group: <ol style="list-style-type: none"> 1. Click  Chooser. 2. Select the node or group, and click OK.
Policy	... results of policy tests descended from a specific policy: <ol style="list-style-type: none"> 1. Click  Chooser. 2. Select the policy and click OK.
Status	... policy test results that passed, select Passed policy test results that failed, select Failed .
Test name	... results of policy tests with specific names: <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial test name in the text field.
Test or test group	... results generated by a specified policy test or test group: <ol style="list-style-type: none"> 1. Click  Chooser. 2. Select the policy test or test group, and click OK. <p>Note: If you select a test group, search results will include results generated by any policy test descended from the group.</p>
Time of result	... results generated within a specified time range: <ol style="list-style-type: none"> 1. Click  Time Chooser. 2. Complete the Time Chooser dialog and click OK. <p>Tip: Click  Help for more information.</p>

Running, Promoting, and Waiving Policy Tests

Running Policy Tests Manually

For an introduction to policy tests, see [What are Policy Manager Objects?](#) on page 131.

Note Since a policy test runs automatically when TE creates a change version for an element in the effective scope of the test, Tripwire recommends that you only run a policy test manually in the following cases:

1. When a new policy test is created or imported.
2. If you change the properties of a policy test and want to update the related compliance statistics.


Tip This procedure explains how to run policy tests in the Tests tab of the Policies tab in the Policy Manager. However, you can also run tests in:

- The Test Search tab of the Policy Manager (see [Searching for Policy Tests](#) on page 532)
- The Result Search tab of the Policy Manager (see [Searching for Policy Test Results](#) on page 559)
- The Test Results tab of a node properties dialog (see [Promoting Policy Test Results Generated for a Node](#) on page 337)

To manually run policy tests and/or policy test groups:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the policy test group containing the policy tests to be run.
3. In the main pane, select the **Tests** tab.
4. To run all policy tests and/or groups in the current view, proceed to [step 5](#) below.

To run **specific** policy tests and/or groups, select the appropriate check boxes. (Only tests on the same page of the Policy Manager can be selected in a single operation.)

5. Click  **Run**.
6. If a confirmation dialog opens, click **OK**.

Promoting Policy Test Results


With this procedure, you can modify the conditions that define the pass/fail criteria for one or more policy tests that have generated results. Specifically, you can either modify a test's conditions based on values reflected in the most recent result generated by the test, or enter customized conditions of your choosing. For more information, see [What is Policy Test Promotion?](#) on page 146.

- Tip** This procedure explains how to promote test results in the Tests tab of the Policies tab in the Policy Manager. However, you can also promote results in:
- The Test Search tab of the Policy Manager (see [Searching for Policy Tests on page 532](#))
 - The Result Search tab of the Policy Manager (see [Searching for Policy Test Results on page 559](#))
 - The Test Results tab of a node properties dialog (see [Promoting Policy Test Results Generated for a Node on page 337](#))

To modify the pass/fail conditions of policy tests that have generated results:

1. In the Manager bar, click **POLICIES**.
2. In the main pane, select the **Tests** tab.
3. In the tree pane, select the TE policy or policy test group containing the policy tests to be modified.
4. To modify the pass/fail conditions of any policy tests descended from the selected TE policy or group, proceed to [step 5](#) below.

To modify the pass/fail conditions of specific policy tests, or all tests descended from specific TE policies or groups, select the check box of each object in the main pane.

5. Click  **Promote**.
6. The Promote Test Results dialog presents a complete list of all specified policy tests that have generated results. For a description of each column in this dialog, see [Table 125 on the next page](#).

[Table 126 \(on page 564\)](#) defines each of the promotion options that may be available from the Action drop-down for each test. By default, TE enters Ignore as the promotion option for each test. To change this setting for a test, select another option from the **Action** drop-down.

- If you select the **Customize** promotion option for a policy test, TE presents a dialog with the current pass/fail conditions of the test. Modify the conditions as needed, and click **OK**.

- The **Expand** and **Restrict** promotion options are only available if the current result of the test includes values that would support the option. For instance, if a test result does not include a value for which a new condition may be added to the test, TE excludes the Expand option from the Action drop-down menu.
7. When you finish specifying promotion methods for the listed policy tests, click **Next**.
 8. (Optional) As a precautionary measure, you can now export the selected tests to an XML file. If your changes have undesirable or unintended consequences, you can simply re-import the XML file at a later time to return the policy tests to their original states.
To export the existing (i.e. pre-promotion) versions of the tests to an XML file:
 - a. Click **Export**.
 - b. Complete the appropriate steps for your system.
 9. In the Promote Test Results Wizard, click **Finish**.

Table 125. Columns in the Promote Test Results dialog

Column	Description
Action	Presents the available promotion options for a policy test.
Test	The name of a policy test.
Observed	<p>To review the values from tested element versions saved in the latest results generated by a policy test, click the test's More button. In a pop-up dialog, Tripwire Enterprise presents a list of the test's pass/fail conditions. For each condition, TE displays the value(s) saved in the test's results.</p> <ul style="list-style-type: none"> • If the test's results contain multiple values for a single condition, the values are separated by commas. • 'No Value Extracted' indicates a condition for which the tested element version(s) lacked a value. • 'No Values Were Available' indicates a condition for which the tested element version(s) lacked applicable data for the type of policy test; for instance, a version that lacks archived content for a content policy test, or a version that represents a file that does not exist. • 'Untested' indicates a condition that was not used to assess the pass/fail status of the element version(s). <p>Note: For an attribute test, the name of a condition is the name of the corresponding attribute. For a content test, the name of a condition is defined in the Conditions tab of the policy test properties dialog (see Changing the Properties of a Policy Test on page 536).</p>
Old Condition	Displays the pass/fail conditions that are currently defined in the properties of a policy test.
New Condition	Based on the promotion option selected from the Action drop-down menu, this column displays what the new pass/fail conditions will be for a policy test. (If you select Ignore from the Action menu, no conditions are displayed. However, TE will preserve the existing conditions.)

Table 126. Promotion options for policy test results

Option	Select this option to ...
Customize	... open a dialog in which you can modify the test's pass/fail conditions however you like.
Expand	... supplement the test's existing pass/fail conditions with conditions that specify the value (s) reflected in the latest result generated by the test for the node. To specify the result value(s), TE will add a new condition(s) to the policy test.
Ignore	... retain the test's existing pass/fail conditions as currently defined.
Restrict	... replace the test's existing pass/fail conditions with conditions that specify the value(s) reflected in the latest result generated by the test for the node.

Creating a Waiver

For an introduction to waivers, see [What are Policy Scores? on page 138](#).

- Tip** This procedure explains how to create waivers in the Tests tab of the Policies tab in the Policy Manager. However, you can also create waivers in:
- The Test Search tab of the Policy Manager (see [Searching for Policy Tests on page 532](#))
 - The Result Search tab of the Policy Manager (see [Searching for Policy Test Results on page 559](#))
 - The Waiver Search tab of the Policy Manager (see [Searching for Waivers on page 567](#))
 - The Waivers tab of a TE policy (see [Changing the Properties of a TE Policy on page 534](#))
 - The Test Results tab of a node properties dialog (see [Promoting Policy Test Results Generated for a Node on page 337](#))


To create a waiver for a TE policy:

1. In the Manager bar, click **POLICIES**.
2. In the main pane, select the **Tests** tab.
3. In the tree pane, select the TE policy or policy test group containing the policy tests for which you want to create the waiver.
4. To create a waiver for all policy tests in the selected object that have current test results that failed, proceed to [step 5](#) below.

To create a waiver for specific policy tests, select the check box of each Policy Manager object in the main pane. (In this case, only objects on the same page of the Policy Manager can be selected in a single operation.)


5. Click  **New Waiver**.

6. In the general waiver information page:
 - a. Enter a **Name** for the waiver.
 - b. Select a TE **Policy** for the waiver.
 - c. Complete the remaining fields and click **Next**.


Tip For more information, click  **Help** in any wizard page.

7. Based on the selected objects in the Tests tab, the wizard presents a list of all applicable test/node pairs that have a current test result that failed. Modify the list, as needed.


To **remove** specific test/node pairs from the waiver:

- a. Select the check box of each pair.
- b. Click  **Delete**.
- c. In the confirmation dialog, click **OK**.

To add test/node pairs for other tests with current failures:

- a. Click  **Add tests with failures**.
- b. In the Chooser dialog, select a Policy Manager object.
- c. Click **Add**.
- d. Repeat steps **b** and **c** above to add any other Policy Manager objects. Then, click **OK**.

To add test/node pairs for other nodes with current failures:

- a. Click  **Add nodes with failures**.
- b. In the Chooser dialog, select a node or node group.
- c. Click **Add**.
- d. Repeat steps **b** and **c** above to add any other nodes or node groups. Then, click **OK**.


8. Click **Next**. TE presents a list of specified test/node pairs involving nodes that do not fall under the scope of the specified TE policy (if any). These pairs will be omitted from the waiver.
9. To complete the wizard, click **Finish**.

Changing the Properties of a Waiver

For an introduction to waivers, see [What are Policy Scores?](#) on page 138.

To change the properties of a waiver for a TE policy:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the group containing the TE policy.
3. In the main pane, select the **Tests** tab.
4. In the **Name** column, select the link for the TE policy.
5. In the properties dialog, click the **Waivers** tab.
6. In the **Name** column, select the link for the waiver.
7. As needed, modify the tabs in the waiver properties dialog and click **OK**.


Tip For more information, click  **Help** in any tab.

Searching for Waivers

Notes For an introduction to common search features such as wildcards, text-field qualifiers, and saved searches, see [How Do I Run a Search? on page 232](#).








In the Waiver Search tab, the button bar contains many of the same buttons available in the Policies tab. To use these buttons, refer to the procedures in [Chapter 10: Policy Procedures \(on page 529\)](#).

To search for waivers:

1. In the Manager bar, click **POLICIES**.
2. Select the **Waiver Search** tab.
3. Enter search criteria. For guidance, see [Table 127 on the next page](#).
 - Some of the search criteria are based on values that can be edited in policy test property dialogs (see [Changing the Properties of a Policy Test on page 536](#)).
 - All text-field entries are case-insensitive. For example, 'Policy' and 'policy' will return the same results.
 - Any string may be entered in a text field. For example, if you enter a string in the **Test Name** field, and select **Contains** as the text-field qualifier, search results will include any waivers for a policy test with a name that includes the string.
4. Click  **Search**.

Next If desired, you can save the entered search criteria for future use. For instructions, see [Creating a Saved Search on page 234](#).

Table 127. Waiver search criteria



Search Criteria	To limit search results to ...
Creation Date	<p>... waivers created within a specified time range:</p> <ol style="list-style-type: none"> 1. Click  Time Chooser. 2. Complete the Time Chooser dialog and click OK. <p>Tip: Click  Help for more information.</p>
Expiration Date	<p>... waivers scheduled to expire within a specified time range:</p> <ol style="list-style-type: none"> 1. Click  Time Chooser. 2. Complete the Time Chooser dialog and click OK. <p>Tip: Click  Help for more information.</p>
Granted by	<p>... waivers granted by a user account with a specific name:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial user name in the text field.
Name	<p>... waivers with specific names:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial waiver name in the text field.
Node or node group	<p>... waivers that identify a specific node or node group:</p> <ol style="list-style-type: none"> 1. Click  Chooser. 2. Select the node or group, and click OK.
Policy	<p>... waivers of policy tests in a specific policy:</p> <ol style="list-style-type: none"> 1. Click  Chooser. 2. Select the policy and click OK.
Responsible	<p>... waivers for which a user account with a specific name is responsible for remediating failed test results:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial name in the text field.
Test Name	<p>... waivers of policy tests with specific names:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial test name in the text field.
Test or test group	<p>... waivers of a specified policy test or test group:</p> <ol style="list-style-type: none"> 1. Click  Chooser. 2. Select the policy test or test group, and click OK. <p>Note: If you select a test group, search results will include waivers assigned to any policy test descended from the group.</p>

Closing Waivers

For an introduction to waivers, see [What are Policy Scores? on page 138](#).

Tips This procedure explains how to close waivers for TE policies displayed in the Waiver Search tab of the Policy Manager. However, you can also close waivers in the properties dialog of a TE policy (see [Changing the Properties of a TE Policy on page 534](#)).


To close waivers:

1. In the Manager bar, click **POLICIES**.
2. In the main pane, select the **Waiver Search** tab.
3. Enter waiver search criteria, as described in [Searching for Waivers on page 567](#). For descriptions of search criteria, see [Table 127 on the previous page](#).
4. Click  **Search**. In the main pane, Tripwire Enterprise presents the waivers that satisfy the specified criteria.
5. To close specific waivers, select the check box of each waiver.
To close all of the waivers, select the check box adjacent to the **Name** column header.
6. Click  **Close**.

Deleting Waivers

For an introduction to waivers, see [What are Policy Scores? on page 138](#).

To delete waivers for a TE policy:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the group containing the TE policy.
3. In the main pane, select the **Tests** tab.
4. In the **Name** column, select the link for the TE policy.
5. In the properties dialog, click the **Waivers** tab.
6. To delete specific waivers, select the check box of each waiver.
To delete all waivers, select the check box adjacent to the **Name** column header.
7. Click  **Delete**.


Moving, Linking, and Unlinking Objects in the Policy Manager

Moving Policy Manager Objects

With this procedure, you can move Policy Manager objects from:

- A TE policy to a policy test group or another TE policy.
- A policy test group to a TE policy or another policy test group.

To move Policy Manager objects:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the TE policy or policy test group containing the objects to be moved.
3. In the main pane, select the **Tests** tab.
4. In the main pane, specify the Policy Manager objects to be moved.
 - To move all objects in the current view, proceed to [step 5](#).
 - To move specific objects, select the check box of each object.
5. Click  **Move**.
6. In the Move Tests dialog, select the destination TE policy or policy test group, and click **OK**.

Linking Policy Manager Objects

When you create a Policy Manager object, the object is linked to the TE policy or policy test group in which it was created. As needed, the object may also be linked to other TE policies and policy test groups. For more information, see [What are Links and Linked Objects?](#) on page 213.

Tips A TE policy cannot be linked under another TE policy.

If you link a policy test in the **Unlinked** group, Tripwire Enterprise *moves* the test to the destination TE policy or policy test group.


This procedure explains how to link Policy Manager objects displayed in the Tests tab of the Policies tab in the Policy Manager. However, you can also link Policy Manager objects in:


- The Test Search tab of the Policy Manager (see [Searching for Policy Tests](#) on page 532)
- The Parent Groups tab of a TE policy (see [Changing the Properties of a TE Policy](#) on page 534)
- The Parent Groups tab of a policy test (see [Changing the Properties of a Policy Test](#) on page 536)
- The Parent Groups tab of a policy test group (see [Changing the Properties of a Policy Test Group](#) on page 538)

To link Policy Manager objects to a TE policy or policy test group:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the TE policy or policy test group containing the objects to be linked.
3. In the main pane, select the **Tests** tab.
4. To link all Policy Manager objects in the current view, proceed to [step 5](#) below.

To link **specific** Policy Manager objects, select the check box of each object. (In this case, only objects on the same page of the Policy Manager can be linked in a single operation.)

5. Click  **Link**.
6. Select the destination TE policy or policy test group, and click **OK**.

Note In the Policy Manager, a link  emblem overlays the icon of each Policy Manager object that is linked to multiple TE policies and/or policy test groups.

Unlinking Policy Manager Objects

This procedure unlinks Policy Manager objects from a TE policy or policy test group. For more information, see [What are Links and Linked Objects?](#) on page 213.

If you unlink a Policy Manager object from the only TE policy or group with which it is linked, Tripwire Enterprise moves the object to the **Unlinked** group. To retrieve an object from the **Unlinked** group, see [Moving Policy Manager Objects](#) on page 570.

Tip To unlink an object, your user account must have Delete and Link permissions for that object, and (for groups) all objects descended from that object. For more information, see [What are User Permissions and User Roles?](#) on page 204.


This procedure explains how to unlink Policy Manager objects displayed in the Tests tab of the Policies tab in the Policy Manager. However, you can also unlink Policy Manager objects in:

- The Parent Groups tab of a TE policy (see [Changing the Properties of a TE Policy](#) on page 534)
- The Parent Groups tab of a policy test (see [Changing the Properties of a Policy Test](#) on page 536)
- The Parent Groups tab of a policy test group (see [Changing the Properties of a Policy Test Group](#) on page 538)

To unlink Policy Manager objects from a TE policy or policy test group:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the TE policy or policy test group containing the objects to be unlinked.
3. In the main pane, select the **Tests** tab.
4. To unlink all Policy Manager objects in the current view from the selected TE policy or group, proceed to [step 5](#) below.

To unlink **specific** Policy Manager objects, select the check box of each object. (Only objects on the same page of the Policy Manager can be unlinked in a single operation.)

5. Click  **Unlink**.
6. Specify whether or not to run the Clear Unlinked Groups task on all Unlinked groups in TE. For more information on this task, see [What are Task Types?](#) on page 127.
7. Click **OK**.

Note If you get an error message when unlinking objects, an access control (see [What are Access Controls?](#) on page 208) is preventing you from unlinking a descendant object. To determine which objects have access controls, check the Objects tab for the Error log message associated with this operation.

Exporting and Importing Policy Manager Objects


Exporting Policy Manager Objects

This procedure exports selected Policy Manager objects to an XML file. As needed, the contents of the XML file may be re-imported at a later date (see [Importing Policy Manager Objects on the next page](#)).

Tip This procedure explains how to export Policy Manager objects displayed in the Tests tab of the Policies tab in the Policy Manager. However, you can also export Policy Manager objects in:

- The Parent Groups tab of a TE policy (see [Changing the Properties of a TE Policy on page 534](#))
- The Parent Groups tab of a policy test (see [Changing the Properties of a Policy Test on page 536](#))
- The Parent Groups tab of a policy test group (see [Changing the Properties of a Policy Test Group on page 538](#))
- The Test Search tab of the Policy Manager (see [Searching for Policy Tests on page 532](#))

To export Policy Manager objects to an XML file:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the TE policy or policy test group containing the objects to be exported.
3. In the main pane, select the **Tests** tab.
4. (Optional) To export **specific** Policy Manager objects, select the check box for each object. Only objects on the same page of the Policy Manager can be selected in a single export operation.
5. Click  **Export**.
6. Select one of the following options and click **OK**:
 - **All tests and test groups**. This option exports all Policy Manager objects in your TE installation.
 - **Selected tests and test groups only**. This option exports the selected Policy Manager objects only.
7. To export the XML file to a local directory, complete the standard steps for your system.

Tip If your Web browser is an older version of Internet Explorer, you may need to manually add a **.xml** extension to the end of the file name.

Importing Policy Manager Objects

This procedure imports Policy Manager objects from an XML file to your Tripwire Enterprise implementation. (To create an XML file, see [Exporting Policy Manager Objects on the previous page](#).)

Caution Prior to this procedure, you should first review the guidelines employed by Tripwire Enterprise when importing the contents of an XML file (see [How Do I Import and Export Tripwire Enterprise Objects? on page 217](#)).


If you are importing the updated versions of pre-configured Policy Manager objects that were previously imported in your TE installation, you should import all of the XML files in the related zip file at the same time. If you fail to do so, some policy tests may fail to run properly. For more information, see [What are Pre-Configured Rules and Policies? on page 219](#).

To import the Policy Manager objects in an XML file:

1. In the Manager bar, click **POLICIES**.
2. In the tree pane, click the **Root Policy Group**.

Note Policies downloaded from the Tripwire Customer Center should always be imported into the Root Policy Group. It is possible to import policy objects into other policy groups, but the OIDs in the policies being imported must exactly match the OIDs on the TE Console system they are imported into. If the OIDs don't match, a duplicate folder structure will be created.

For more information on the policy import process, see [XML-File Import of Rules, Actions, Tasks, Policy Tests, Reports, and Dashboards on page 230](#).

3. In the main pane, select the **Tests** tab.
4. Click  **Import**.
5. In the Import Tests dialog, click **Browse**.
6. To locate and select the XML file, complete the standard steps for your system.
7. In the Import Tests dialog, click **OK**.

Chapter 11. Log Message Procedures

Viewing, Sorting, and Filtering TE Log Messages

Viewing TE Log Messages in the Log Manager

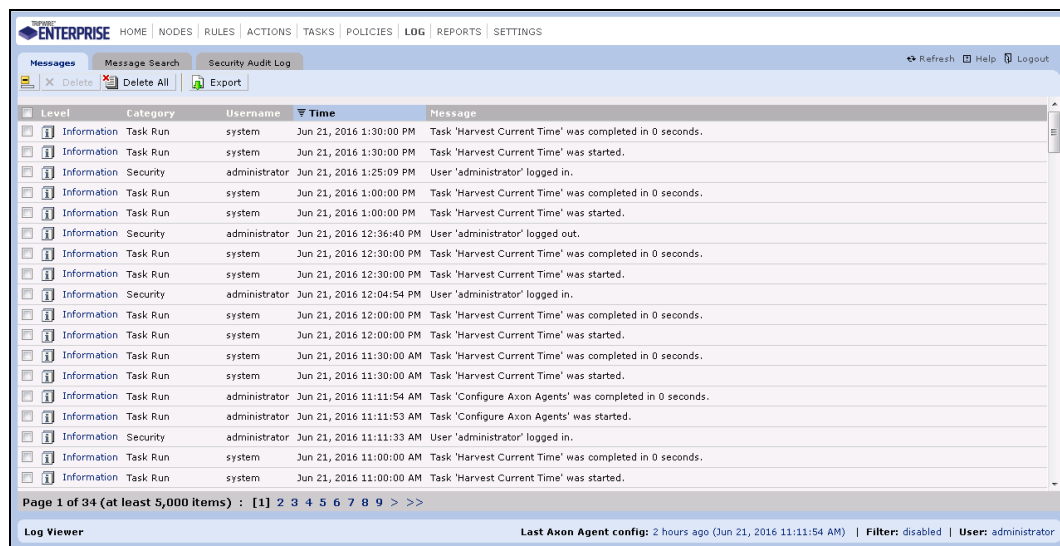
To view TE log messages in the Log Manager:

1. In the Manager bar, click **LOG**.
2. Review the list of TE log messages in the Log Manager table (see [Figure 37 below](#)). [Table 128 on the next page](#) defines each of the columns in the Log Manager table.
 - To **sort** log messages by the contents of a column, click the column header. To reverse the order, click the column header a second time.

Note The Message column cannot be sorted.

- If the Log Manager contains multiple pages, use the navigation controls at the bottom of the Log Manager to **scroll** through the pages.
- To adjust the Log Manager **maximum table size** settings, see [Changing User Preference Settings on page 262](#).
- To **shorten the list** of visible log messages, apply filtering criteria to the Log Manager. For instructions, see [Filtering Log Messages on page 578](#).



Figure 37. The Log Manager



The screenshot shows the Tripwire Enterprise Log Manager interface. At the top, there is a navigation bar with links for HOME, NODES, RULES, ACTIONS, TASKS, POLICIES, LOG, REPORTS, and SETTINGS. Below this is a sub-header for 'Messages' with options for Message Search, Security Audit Log, Refresh, Help, and Logout. A toolbar contains Delete, Delete All, and Export buttons. The main area is a table with columns: Level, Category, Username, Time, and Message. The table contains 15 rows of log entries. At the bottom, there is a pagination control showing 'Page 1 of 34 (at least 5,000 items)' and a status bar indicating 'Last Axon Agent config: 2 hours ago (Jun 21, 2016 11:11:54 AM) | Filter: disabled | User: administrator'.

Level	Category	Username	Time	Message
Information	Task Run	system	Jun 21, 2016 1:30:00 PM	Task 'Harvest Current Time' was completed in 0 seconds.
Information	Task Run	system	Jun 21, 2016 1:30:00 PM	Task 'Harvest Current Time' was started.
Information	Security	administrator	Jun 21, 2016 1:25:09 PM	User 'administrator' logged in.
Information	Task Run	system	Jun 21, 2016 1:00:00 PM	Task 'Harvest Current Time' was completed in 0 seconds.
Information	Task Run	system	Jun 21, 2016 1:00:00 PM	Task 'Harvest Current Time' was started.
Information	Security	administrator	Jun 21, 2016 12:36:40 PM	User 'administrator' logged out.
Information	Task Run	system	Jun 21, 2016 12:30:00 PM	Task 'Harvest Current Time' was completed in 0 seconds.
Information	Task Run	system	Jun 21, 2016 12:30:00 PM	Task 'Harvest Current Time' was started.
Information	Security	administrator	Jun 21, 2016 12:04:54 PM	User 'administrator' logged in.
Information	Task Run	system	Jun 21, 2016 12:00:00 PM	Task 'Harvest Current Time' was completed in 0 seconds.
Information	Task Run	system	Jun 21, 2016 12:00:00 PM	Task 'Harvest Current Time' was started.
Information	Task Run	system	Jun 21, 2016 11:30:00 AM	Task 'Harvest Current Time' was completed in 0 seconds.
Information	Task Run	system	Jun 21, 2016 11:30:00 AM	Task 'Harvest Current Time' was started.
Information	Task Run	administrator	Jun 21, 2016 11:11:54 AM	Task 'Configure Axon Agents' was completed in 0 seconds.
Information	Task Run	administrator	Jun 21, 2016 11:11:53 AM	Task 'Configure Axon Agents' was started.
Information	Security	administrator	Jun 21, 2016 11:11:33 AM	User 'administrator' logged in.
Information	Task Run	system	Jun 21, 2016 11:00:00 AM	Task 'Harvest Current Time' was completed in 0 seconds.
Information	Task Run	system	Jun 21, 2016 11:00:00 AM	Task 'Harvest Current Time' was started.

Table 128. Columns in the Log Manager table

Column	Description
Level	<p>The Level column indicates the type of TE log message.</p> <ul style="list-style-type: none">  Information messages document a standard Tripwire Enterprise event, such as the completion of a task. These messages include the source of the event (user or system), the time of the event, and the Tripwire Enterprise objects associated with the event (if any).  Error messages document internal system errors or schedule overrun errors. Error messages include the source of the error (user or system), the time of the error, and the Tripwire Enterprise objects affected by the error (if any). <p>To view the properties of a log message, select a Level link.</p>
Category	A category indicates the type of activity or event that generated a TE log message. For a definition of each category, see Table 47 on page 167 .
Username	<p>The Username column indicates if a log message was generated by a system-initiated event or a user-initiated event.</p> <ul style="list-style-type: none"> System indicates a system-initiated event, such as a scheduled task. A username indicates that a log message was triggered by the activity of a specific user.
Time	This column provides the date and time when a log message was created.
Message	This column provides a summary of the activity or event associated with a log message.

Viewing the Properties of a Log Message

To review the properties of TLC log messages, you can run a search in the Log Center Events tab ([Searching for TLC Log Messages on page 581](#)).

To review the properties of a TE log message, you can either run a search in the Log Messages tab (see [Searching for TE Log Messages on page 579](#)) or follow the steps below.

To review the properties of a TE log message:

1. In the Manager bar, click **LOG**.
2. In the Log Manager, locate the log message.
3. In the **Level** column, select the log message link.
4. In the log message properties dialog, review the **General** and **Objects** tabs.
5. Click **OK**.

Table 129. Tabs in TE log message properties

Tab	Description
General	General information about the log message, including the message's creation time and content.
Objects	Displays the TE objects associated with the event that generated the log message.

Filtering Log Messages


Filter criteria determine which TE log messages appear in the Messages tab of the Log Manager. To filter log messages, the filter function must be enabled. If filtering is disabled, the Log Manager will display all TE log messages currently in the system.

To enable or disable filtering:

1. In the Manager bar, click **LOG**.
2. In the lower right-hand corner of the Log Manager, click the **Filter** link.
3. In the Log Message Filter dialog, select the **General** tab.
4. Select or clear the **Enable filtering of log messages** check box.
5. Click **OK**.

To change log message filter criteria:

1. In the Manager bar, click **LOG**.
2. In the lower right-hand corner of the Log Manager, click the **Filter** link.
3. In the Log Message Filter dialog, enter filtering criteria in the **Levels**, **Categories**, **Users**, and **Time** tabs.

Tip For field and menu definitions, click  **Help**.

4. Click **OK**. The Log Message Filter dialog closes, and the Log Manager refreshes with the filtered TE log messages.


Searching for TE Log Messages

By running a TE log message search, you can quickly identify all TE log messages that meet specific search criteria. A search can retrieve any TE log message in the system, including those that have been filtered from view.

Notes For an introduction to common search features such as wildcards, text-field qualifiers, and saved searches, see [How Do I Run a Search? on page 232](#).






In the Message Search tab, the button bar contains some of the same buttons available in the Messages tab. To use these buttons, refer to the procedures in [Chapter 11: Log Message Procedures \(on page 575\)](#).

To search for TE log messages:

1. In the Manager bar, click **LOG**.
2. Select the **Message Search** tab.
3. Enter search criteria. For guidance, see [Table 130 on the next page](#).
 - All text-field entries are case-insensitive. For example, ‘Check’ and ‘check’ will return the same results.
 - Any string may be entered in a text field. For example, if you enter a string in the **Node name** field, and select **Contains** as the text-field qualifier, search results will include any log message created for a node with a name that includes the string.
4. Click  **Search**.

Next If desired, you can save entered search criteria for future use. For instructions, see [Creating a Saved Search on page 234](#).

Table 130. TE log message search criteria

Search Criteria	To limit search results to ...
Categories	<p>... log messages with a specific category, select an option from the list. For category definitions, see Table 47 on page 167.</p> <p>Note: To select multiple options, use the standard selection convention for your operating system. For example, in Windows, hold the CTRL key while making your selections.</p>
Level	<p>... log messages of a specific type, select Information or Error. For more information, see What are Log Messages? on page 166.</p>
Message	<p>... log messages that include or exclude specific content:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a search string in the text field.
Node name	<p>... log messages associated with nodes that have specific names:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial node name in the text field.
Node or node group	<p>... log messages associated with a specific node or node group:</p> <ol style="list-style-type: none"> 1. Click  Chooser. 2. Select the node or group, and click OK.
Policy, Test or Test Group	<p>... log messages associated with a specific policy, policy test, or policy test group:</p> <ol style="list-style-type: none"> 1. Click  Chooser. 2. Select the Policy Manager object and click OK.
Task name	<p>... log messages associated with tasks that have specific names:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial task name in the text field.
Task or task group	<p>... tasks associated with a specific task or task group:</p> <ol style="list-style-type: none"> 1. Click  Chooser. 2. Select the task or group, and click OK.
Time	<p>... log messages generated within a specified time range:</p> <ol style="list-style-type: none"> 1. Click  Time Chooser. 2. Complete the Time Chooser dialog and click OK. <p>Tip: Click  Help for more information.</p>
User name	<p>... log messages associated with user accounts that have specific names:</p> <ol style="list-style-type: none"> 1. Select a text-field qualifier. 2. Enter a complete or partial user name in the text field.

Searching for TLC Log Messages

By following the steps below, you can identify all TLC log messages that meet specific search criteria. A search can retrieve any log message from your TLC Server, including those that have been filtered from view.

To search for TLC log messages:

1. In the Manager bar, click **LOG**.
2. Select the **Log Center Events** tab.

Note This tab only appears in the Log Manager if the **Allow TE to use information from TE Log Center** setting is configured (see [Changing Log Management Settings on page 268](#)).





3. Enter search criteria. For guidance, see [Table 131 \(below\)](#).
 - All text-field entries are case-insensitive. For example, ‘Check’ and ‘check’ will return the same results.
 - Any string may be entered in a text field. For example, if you enter a string in the **With a name containing** field, search results will include any applicable TLC log message created for a node with a name that includes the string.
4. Click  **Search**.

Table 131. TLC log message search criteria

Search Criteria	To limit search results to ...
Message	... TLC log messages that include specified content, enter a search string in the text field.
Node or node group	... TLC log messages associated with a specific node or node group: 1. Click  Chooser . 2. Select the node or group, and click OK .
Time	... TLC log messages generated within a specified time range: 1. Click  Time Chooser . 2. Complete the Time Chooser dialog and click OK . Tip: Click  Help for more information.
With a name containing	... TLC log messages associated with nodes that have specific names, enter a complete or partial node name in the text field.

Exporting and Deleting Log Messages


Exporting Log Messages

To save log information for future reference, you can export TE or TLC log messages to an XML file. Log message XML files may be integrated with other applications and reporting tools. For instance, some applications can use XML files to generate reports or charts.


Notes If filtering is enabled, you can only export TE log messages that meet the filtering criteria. To export all TE log messages in the system, filtering must be disabled (see [Filtering Log Messages on page 578](#)).

You can also export TE log messages in search results. For more information, see [Searching for TE Log Messages \(on page 579\)](#).

To export TE log messages to an XML file:

1. In the Manager bar, click **LOG**.
2. In the Messages tab, indicate the log messages to be exported.
 - (Applies only if filter is disabled) To export **all** TE log messages in the system, do **not** select any check boxes.
 - (Applies only if filter is enabled) To export all TE log messages that meet the current filtering criteria, do **not** select any check boxes.
 - To export **specific** log messages, select the appropriate check boxes. With this option, only TE log messages displayed on the same page of the Log Manager can be exported at the same time.
3. Click  **Export**.
4. In the Export Log Messages dialog, select one of the following options and click **OK**:
 - **All log messages** (applies only if filter is disabled). This option exports all TE log messages in the system.
 - **All log messages satisfying the current filter** (applies only if filter is enabled). This option exports all TE log messages that meet the current filter settings.
 - **Selected log messages only**. This option exports selected TE log messages only.
5. In the File Download dialog, click **Save**.
6. Browse to the directory where the XML file will be exported. If desired, change the default name of the XML file.
7. Click **Save**.

To export TLC log messages to an XML file:


1. In the Manager bar, click **LOG**.
2. In the Log Center Event tab, run a search for TLC log messages (see [Searching for TLC Log Messages on page 581](#)).
3. Click  **Export**.
4. In the Export Log Center Messages dialog, select one of these options and click **OK**:
 - **The current page of log messages** exports all currently displayed search results.
 - **Up to 10,000 log messages in the current search** exports up to 10,000 TLC log messages identified by the current search criteria.
5. In the File Download dialog, click **Save**.
6. Browse to the directory where the XML file will be exported. If desired, change the default name of the XML file.
7. Click **Save**.

Deleting TE Log Messages


Deletion permanently removes TE log messages from your Tripwire Enterprise implementation. If you would rather save copies of TE log messages for future reference, run the Archive Log Messages Task. For more information, see [How Does the Archive Log Messages Task Work? on page 170](#).

Note If filtering is enabled, only displayed TE log messages can be deleted. To delete all TE log messages in the system, filtering must be disabled. For instructions, see [Filtering Log Messages on page 578](#).

To delete specific TE log messages:

1. In the Manager bar, click **LOG**.
2. In the **Messages** tab, select the check box of each log message to be deleted. Log messages on different pages in the Log Manager cannot be deleted at the same time.
3. Click  **Delete**.
4. Click **OK** to confirm.

To delete all unfiltered TE log messages:

1. In the Manager bar, click **LOG**.
2. In the **Messages** tab, click  **Delete All**.
3. Select **Confirm delete all operation**.
4. Click **OK**.

Chapter 12. Report Procedures

Viewing and Changing Objects in the Report Manager

Viewing Reports, Report Groups, and Dashboards

To view objects in the Report Manager:

1. In the Manager bar, click **REPORTS**.
2. The Report Manager contains all reports, report groups, and dashboards in your TE implementation (see [Figure 38](#)). To view the contents of a report group, select the group in the tree pane.
 - [Table 132](#) defines each column in the Report Manager main pane.
 - If the contents of the selected report group span multiple pages, use the navigation controls at the bottom of the main pane to **scroll** through the pages.
 - To **sort** objects in the main pane by the values in a column, click the column header. To reverse the order, click the column header a second time.
 - To change the Report Manager **maximum table size** setting, see [Changing User Preference Settings](#) on page 262.

Figure 38. The Report Manager

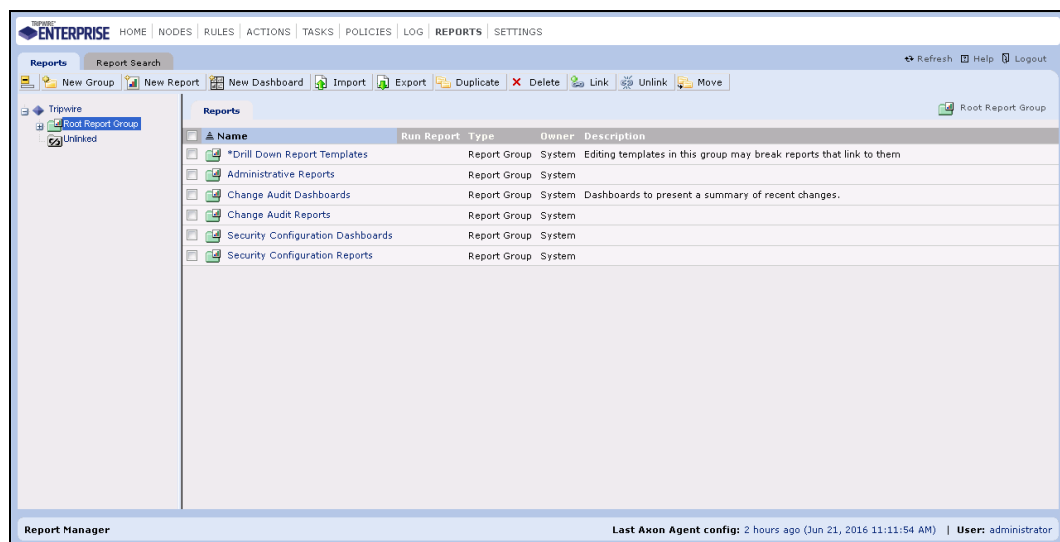



Table 132. Columns in the Report Manager main pane


Column	Description
Name	<p>This column lists the names of reports, report groups, and dashboards. A small padlock emblem  overlays the icon of a user report, user report group, or user dashboard.</p> <p>To change the properties of a report, report group, or dashboard, click a Name link. For more information, see:</p> <ul style="list-style-type: none"> • Changing the Properties of a Report (on page 589) • Changing the Properties of a Report Group (on page 590) • Changing the Properties of a Dashboard (on page 591)
Run Report	<p>To run a report or dashboard, click a Run Report link. For more information, see:</p> <ul style="list-style-type: none"> • Running a Report Manually (on page 601) • Running a Dashboard (on page 607)
Type	<p>This column identifies the type of each object in the Report Manager.</p> <ul style="list-style-type: none"> • Report. For reports, the Type column identifies the report type. For report type definitions, see What are Reports and Report Types? on page 172. • Report Group • Dashboard
Owner	<p>This column indicates if a report, report group, or dashboard is available to all users (System) or the current user only (User). For more information, see What are System Reports and User Reports? on page 184.</p>
Description	<p>This column provides an optional description of each report, report group, or dashboard. To add or edit descriptions, see:</p> <ul style="list-style-type: none"> • Changing the Properties of a Report (on page 589) • Changing the Properties of a Report Group (on page 590) • Changing the Properties of a Dashboard (on page 591)

Searching for Reports

Notes For an introduction to common search features such as wildcards, text-field qualifiers, and saved searches, see [How Do I Run a Search? on page 232](#).

In the Report Search tab, the button bar contains some of the same buttons available in the Reports tab. To use these buttons, refer to the procedures in [Chapter 12: Report Procedures \(on page 584\)](#).

To search for reports:

1. In the Manager bar, click **REPORTS**.
2. Select the **Report Search** tab.
3. From the **Type** list, select **(any report)** or a specific report type. For report type definitions, see [Table 48 on page 173](#).
4. Enter additional search criteria. For guidance, see [Table 133 on the next page](#).
 - Some of the search criteria are based on values that can be edited in report property dialogs (see [Changing the Properties of a Report on page 589](#)).
 - All text-field entries are case-insensitive. For example, 'Report' and 'report' will return the same results.
 - Any string may be entered in a text field. For example, if you enter a string in the **Report name** field, and select **Contains** as the text-field qualifier, search results will include any report with a name that includes the string.
5. Click  **Search**

Next If desired, you can save entered search criteria for future use. For instructions, see [Creating a Saved Search on page 234](#).

Table 133. Report search criteria

Search Criteria	To limit search results to ...
Is system report	... system reports, select Yes user reports, select No . For more information, see What are System Reports and User Reports? on page 184 .
Report description	... reports with specific descriptions: 1. Select a text-field qualifier. 2. Enter a complete or partial description in the text field.
Report name	... reports with specific names: 1. Select a text-field qualifier. 2. Enter a complete or partial report name in the text field.
Type	... reports of a specific type, select a type from the drop-down list. Otherwise, accept the default value (any report).


Changing the Properties of a Report


With this procedure, you can change the name, description, availability, and criteria of a report.

To change the properties of a **system report**, the Manage System Reports permission must be assigned to your user account. For more information, see [What are System Reports and User Reports? \(on page 184\)](#) and [What are User Permissions and User Roles? \(on page 204\)](#).

To change the properties of a report:

1. In the Manager bar, click **REPORTS**.
2. In the tree pane, select the report group containing the report.
3. In the main pane, select the report in the **Name** column.

Note A padlock emblem overlays the icon  of a user report.

4. As needed, modify the tabs in the report properties dialog.
 - For tab descriptions, see [Table 134 below](#).
 - For more information, click  **Help** in any tab.

Caution The **Version Attributes** and **Version Content** criteria can greatly slow the compilation of report output. Therefore, you should narrow the scope of the report with other criteria to the greatest possible extent.

5. When you finish changing the report's properties, click **OK**.

Table 134. Tabs in report properties


Tab	Description
General	Defines the name, description (optional), and output format of the report. In addition, this tab includes a setting that determines if the report is a system report (available to all users) or a user report (available to the current user only).
Criteria	Contains the criteria available with this type of report. Criteria settings determine the data to be included in report output.
Archive	Contains any previously compiled output that was saved for this report.
Parent Groups	Displays the full path of each report group to which the report is linked. <ul style="list-style-type: none">• This tab includes some of the same buttons that appear in the Report Manager. For guidance in using these buttons, refer to the corresponding procedure in this chapter.• To view or edit the properties of a report group, select the group's link. (For more information, see Changing the Properties of a Report Group on the next page.)


Changing the Properties of a Report Group

To change the properties of a **system report group**, the Manage System Reports permission must be assigned to your user account. For more information, see [What are System Reports and User Reports?](#) (on page 184) and [What are User Permissions and User Roles?](#) (on page 204).


Tip This procedure explains how to change the properties of a report group displayed in the main pane of the Report Manager. However, you can also change the properties of a report group in the **Parent Groups** tab of a report properties dialog (see [Changing the Properties of a Report on the previous page](#)) or report group properties dialog (accessed below).

To change the properties of a report group:

1. In the Manager bar, click **REPORTS**.
2. In the tree pane, click the group containing the report group.
3. In the main pane, select the  group link in the **Name** column.

Note A padlock emblem  overlays the icon of a user report group.

4. As needed, modify the report group properties dialog (see [Table 135](#)).

Tip For more information, click  **Help** in any tab.

5. Click **OK**.

Table 135. Tabs in report group properties


Tab	Description
General	The name and description (optional) of the report group.
Parent Groups	Displays the full path of each node group to which this report group is linked. <ul style="list-style-type: none">• This tab includes some of the same buttons that appear in the Report Manager. For guidance in using these buttons, refer to the corresponding procedure in this chapter.• To view or edit the properties of a report group, select the group's link.

Changing the Properties of a Dashboard


To change the properties of a **system dashboard**, the Manage System Reports permission must be assigned to your user account. For more information, see *What are System Reports and User Reports?* (on page 184) and *What are User Permissions and User Roles?* (on page 204).

To change the properties of a dashboard:

1. In the Manager bar, click **REPORTS**.
2. In the tree pane, select the report group containing the dashboard.
3. In the main pane, select the  dashboard link in the **Name** column.





Note A padlock emblem  overlays the icon of a user dashboard.

4. As needed, modify the tabs in the dashboard properties dialog. For tab descriptions, see [Table 136 below](#).

Tip For more information, click  **Help** in any tab.

5. Click **OK**.

Table 136. Tabs in dashboard properties

Tab	Description
General	The name, description (optional), and refresh rate of the dashboard. In addition, this tab includes a setting that determines if the dashboard is a system dashboard (available to all users) or a user dashboard (available to the current user only).
Reports	<p>Specifies the reports to be compiled by the dashboard.</p> <ul style="list-style-type: none"> • To remove a report, select the report's check box and click  Remove Report. • To add a report, click  Add Report. <p>When the dashboard is run, TE will present the reports (in the Dashboard Viewer) in the order defined here. To change a report's position in the order, select the report's check box and click one of the following buttons:</p> <ul style="list-style-type: none"> • Click  Move Up to move the report up one position in the order. • Click  Move Down to move the report down in the order. <p>Note: Only report types with the Chart criterion may be added to a dashboard.</p>
Layout	Controls the number of columns in the dashboard's output, along with the size of each report thumbnail.


Creating and Deleting Objects in the Report Manager

Creating a Report

For an introduction to reports, see [What are Reports and Report Types?](#) on page 172.


To create a **system report**, the Manage System Reports permission must be assigned to your user account. For more information, see [What are System Reports and User Reports?](#) (on page 184) and [What are User Permissions and User Roles?](#) (on page 204).

To create a report:

1. In the Manager bar, click **REPORTS**.
2. In the tree pane, select a report group in which to create the report.
3. Click  **New Report**.
4. In the New Report dialog, select a **Report Type**.
5. Enter a **Name** and **Description** (optional).
6. (Optional) To create a system report, select **Report is available to all users**.

Note The **Report is available to all users** check box can only be selected by users with the **Manage System Reports** permission. If your user account lacks this permission and you select this check box, an error message will open when you click **OK**.

7. Click **OK**.
8. In the Criteria tab, select and edit the criteria for the report. Available criteria vary by report type.

Tip For descriptions of report criteria, click  **Help**.

9. Once all desired report criteria have been configured, click **OK**.


Next To run the report now, see [Running a Report Manually](#) (on page 601).
To schedule the report, create a report task (see [Creating a Report Task](#) on page 519).

Creating a Report Group

For an introduction to report groups, see [About Groups \(on page 29\)](#).

To create a **system report group**, the Manage System Reports permission must be assigned to your user account. For more information, see [What are System Reports and User Reports? \(on page 184\)](#) and [What are User Permissions and User Roles? \(on page 204\)](#).

To create a report group:

1. In the Manager bar, click **REPORTS**.
2. In the tree pane, select an existing report group in which to create the new report group.
3. Click  **New Group**.
4. Complete the New Report Group Wizard and click **Finish**.

Note The **Group is available to all users** check box is only available to users with the **Manage System Reports** permission. If your user account lacks this permission and you select this check box, an error message will open when you click **Finish**.

Next To add existing reports and dashboards to the report group, see:


- [Moving Reports, Report Groups, and Dashboards \(on page 597\)](#)
- [Linking Reports, Report Groups, and Dashboards \(on page 597\)](#)


Creating a Dashboard


For an introduction to dashboards, see *What are Dashboards?* on page 182.

To create a **system dashboard**, the Manage System Reports permission must be assigned to your user account. For more information, see *What are System Reports and User Reports?* (on page 184) and *What are User Permissions and User Roles?* (on page 204).

To create a dashboard:

1. In the Manager bar, click **REPORTS**.
2. In the tree pane, select a report group in which to create the dashboard.
3. Click  **New Dashboard**.
4. In the New Dashboard Wizard:
 - a. Enter a **Name**, **Description** (optional), and **Refresh Rate**.
 - b. If applicable, select **Make dashboard available to all users**. If this check box is not selected, only the current user will be able to access the dashboard.
 - c. Click **Next**.

Tip For field definitions, click  **Help** in any wizard page.

5. To add a report to the dashboard:
 - a. Click  **Add Report**.
 - b. In the Add Report dialog, select the report.
 - c. Click **Add**.
 - d. Once all desired reports have been added, click **OK**.
6. In the New Dashboard Wizard, click **Next**.
7. Enter a **Width** and **Height** for each report thumbnail in the dashboard (in pixels), as well as the number of **Columns**. The number of columns determine the maximum number of report thumbnails that will appear in each row of the dashboard.


To display a legend for each report thumbnail in the dashboard, select **Show chart legend**.
8. Click **Finish**.

Duplicating Reports and Dashboards

With this procedure, you can either duplicate:

- Specified reports and/or dashboards in a selected report group.
- All reports and dashboards in a selected report group.

To create a copy of existing reports and dashboards:

1. In the Manager bar, click **REPORTS**.
2. In the tree pane, click the report group containing the objects to be duplicated.
3. (Optional) To duplicate specific reports and/or dashboards, select the check box of each object.
4. Click  **Duplicate**.
5. Click **OK** in the confirmation dialog. Tripwire Enterprise uses the following convention to name a duplicate report or dashboard:

<original object>(<#>)

where:

<original object> is the name of the report or dashboard that was duplicated.

<#> is a number that increments each time the original report or dashboard is duplicated (beginning with 1) - for example, report (1), report (2), etc.

Next To run a duplicated report or dashboard now, see:

- [Running a Report Manually \(on page 601\)](#)
- [Running a Dashboard \(on page 607\)](#)

To schedule a duplicated report or dashboard, create a report task (see [Creating a Report Task on page 519](#)).

Deleting Reports, Report Groups, and Dashboards

To delete a **system report**, **system report group**, or **system dashboard**, the Manage System Reports permission must be assigned to your user account. For more information, see [What are System Reports and User Reports? \(on page 184\)](#) and [What are User Permissions and User Roles? \(on page 204\)](#).

To delete reports, report groups, and/or dashboards:

1. In the Manager bar, click **REPORTS**.
2. In the tree pane, click the report group containing the objects to be deleted.
3. Select the check box for each object to be deleted.
4. Click **✖ Delete**.
5. Specify whether or not to run the Clear Unlinked Groups task on all Unlinked groups in TE. For more information on this task, see [What are Task Types? on page 127](#).
6. Click **OK**.

Note If you get an error message when trying to delete objects, you may not have permission to delete a descendant system report, system report group, or system dashboard. Contact your TE administrator to determine which objects may be causing the problem.


Moving, Linking, and Unlinking Objects in the Report Manager

Moving Reports, Report Groups, and Dashboards

With this procedure, you can move a report, report group, or dashboard from one report group to another. For instance, you can move a report from the **Unlinked** group to another report group.

To move a **system report**, **system report group**, or **system dashboard**, the Manage System Reports permission must be assigned to your user account. For more information, see [What are System Reports and User Reports?](#) (on page 184) and [What are User Permissions and User Roles?](#) (on page 204).

To move reports, report groups, and/or dashboards:


1. In the Manager bar, click **REPORTS**.
2. In the tree pane, select the group containing the objects to be moved.
3. In the main pane, select the check box for each object to be moved.
4. Click  **Move**.
5. In the Move Report Objects dialog, select the destination report group and click **OK**.

Linking Reports, Report Groups, and Dashboards

When you create a report, report group, or dashboard, the object is linked to the report group in which it was created. As needed, these objects may be linked to additional report groups. For an introduction to links, see [What are Links and Linked Objects?](#) on page 213.

To link a **system report**, **system report group**, or **system dashboard** to any report group, the Manage System Reports permission must be assigned to your user account. For more information, see [What are System Reports and User Reports?](#) (on page 184) and [What are User Permissions and User Roles?](#) (on page 204).

To link reports, report groups, and/or dashboards to a report group:


1. In the Manager bar, click **REPORTS**.
2. In the tree pane, select the group containing the objects to be linked.
3. In the main pane, select the check box for each object to be linked.
4. Click  **Link**.
5. Select the destination report group and click **OK**.

Unlinking Reports, Report Groups, and Dashboards

For an introduction to links, see [What are Links and Linked Objects?](#) on page 213.

To unlink a **system report**, **system report group**, or **system dashboard** from any report group, the Manage System Reports permission must be assigned to your user account. For more information, see [What are System Reports and User Reports?](#) (on page 184) and [What are User Permissions and User Roles?](#) (on page 204).

To unlink reports, report groups, and/or dashboards from a report group:

1. In the Manager bar, click **REPORTS**.
2. In the tree pane, select the group from which the objects will be unlinked.
3. In the main pane, select the check box for each object to be unlinked.
4. Click  **Unlink**.
5. Specify whether or not to run the Clear Unlinked Groups task on all Unlinked groups in TE. For more information on this task, see [What are Task Types?](#) on page 127.
6. Click **OK**.

Note If you get an error message when trying to unlink objects, you may not have permission to unlink a descendant system report, system report group, or system dashboard. Contact your TE administrator to determine which objects may be causing the problem.


Exporting and Importing Objects in the Report Manager

Exporting Reports, Report Groups, and Dashboards

This procedure exports selected reports, report groups, and dashboards to an XML file. As needed, the contents of the XML file may be re-imported at a later date (see [Importing Reports, Report Groups, and Dashboards on the next page](#)).

Tip This procedure explains how to export objects displayed in the main pane of the Report Manager. However, you can also export report groups in the **Parent Groups** tab of a report properties dialog (see [Changing the Properties of a Report on page 589](#)) or report group properties dialog (see [Changing the Properties of a Report Group on page 590](#)).

To export reports, report groups, and/or dashboards to an XML file:


1. In the Manager bar, click **REPORTS**.
2. In the tree pane, click the report group containing the objects to be exported.
3. (Optional) To export **specific** objects, select the appropriate check boxes in the main pane. Only objects on the same page of the Report Manager can be selected in a single export operation.
4. Click  **Export**.
5. In the Export Reports dialog, select one of the following options and click **OK**:
 - **All reports, report groups, and dashboards.** This option exports all reports, report groups, and dashboards in your Tripwire Enterprise implementation.
 - **Selected reports, report groups, and dashboards only.** This option exports the selected objects only.
6. To export the XML file to a local directory, complete the standard steps for your operating system.

Importing Reports, Report Groups, and Dashboards

This procedure imports the contents of an XML file to your Tripwire Enterprise implementation. (To create an XML file containing reports, report groups, and dashboards, see [Exporting Reports, Report Groups, and Dashboards on the previous page](#).)

Caution Prior to this procedure, you should first review the guidelines employed by Tripwire Enterprise when importing the contents of an XML file (see [How Do I Import and Export Tripwire Enterprise Objects? on page 217](#)).

To import the reports, report groups, and/or dashboards in an XML file:

1. In the Manager bar, click **REPORTS**.
2. In the tree pane, click the report group to which the XML file's contents will be imported. The report group hierarchy specified in the file will be created in this location.
3. Click  **Import**.
4. In the Import Reports dialog, click **Browse**.
5. To locate and select the XML file, complete the standard steps for your operating system.
6. In the Import Reports dialog, click **OK**.

Working with the Output of Reports and Dashboards

Running a Report Manually


To schedule reports, you must create a report task. For more information, see [How Does a Report Task Work?](#) on page 186.

If the time required to compile a report exceeds the **session timeout** setting, Tripwire Enterprise will automatically terminate your session when the report run is complete, and the report output will be lost. To adjust the session timeout, see [Changing System Preferences](#) on page 266.

By default, Tripwire Enterprise displays all report criteria values at the top of the output generated for a report.

- To limit this content to criteria for which a value(s) has been specified, select the **Show only applied report criteria** check box on the System Preferences page in the Settings Manager (see [Changing System Preferences](#) on page 266).
- To display report criteria at the bottom of generated output, select the **Display criteria at end** check box in the report's General criterion (see [Changing the Properties of a Report](#) on page 589).








To run a report manually:

1. In the Manager bar, click **REPORTS**.
2. In the tree pane, click the report group containing the report.
3. In the main pane, select the  **Run Report** link for the report.
4. When the report finishes, TE presents the output in the Report Viewer. [Table 137 \(on the next page\)](#) describes each of the buttons available in standard Report View. In some reports, you can also access alternative views of report output.
 - In **Nodes View**, TE presents a list of all nodes in the report's output. For descriptions of available buttons in this view, see [Table 138 on page 604](#).
 - In **Elements View**, TE presents a list of all elements in the report's output. For descriptions of available buttons in this view, see [Table 139 on page 605](#).
 - In **Versions View**, TE presents a list of all element versions in the report's output. For descriptions of available buttons in this view, see [Table 140 on page 606](#).
 - In **Test Results View**, TE presents a list of all policy test results in the report's output. For descriptions of available buttons in this view, see [Table 141 on page 606](#).

Tip For more information, click  **Help**.

5. Click **OK**.

Table 137. Report Viewer buttons in standard Report View

Button	Available with ...	Description
 Archive Report	All reports	Saves an archived version of the output. <ul style="list-style-type: none"> For an introduction to report archives, see How Do I Manage Report Output? on page 181. To archive the output of a system report, the Create Archived Reports permission must be assigned to your user account
 PDF Export	All reports	Exports the report output to a PDF file.
 XML Export	All reports	Exports the report output to an XML file.
 CSV Export	Changed Elements Reports Changes by Rule or Group Reports Detailed Changes Reports Detailed Test Inventory Reports Detailed Test Results Reports Device Inventory Reports Last Node Check Status Reports Tasks Reports Test Results By Node Reports Unmonitored Nodes Reports Unreconciled Change Aging Reports	Exports the report output to a CSV file.
 E-mail	All reports	E-mails the report output to specified recipients.
 Print	All reports	Prints a hard copy of the report output.
 Nodes View	Nodes with Changes Reports	Converts the report output to Nodes View (see Table 138 on page 604).




Button	Available with ...	Description
 Elements View	Changed Elements Reports Elements Reports	Converts the report output to Elements View (see Table 139 on page 605).
 Versions View	Changed Elements Reports	Converts the report output to Versions View (see Table 140 on page 606).
 Test Results View	Detailed Test Results Test Results By Node	Converts the report output to Test Results View (see Table 141 on page 606).

Table 138. Report Viewer buttons in Nodes View












Button	Description
 Report View	Reverts report output to standard Report View.
 Export	Exports selected nodes to an XML file (see How Do I Import and Export Tripwire Enterprise Objects? on page 217).
Manage Set	
 Delete	Deletes selected nodes.
 Link	Links selected nodes to a specified node group (see What are Links and Linked Objects? on page 213).
Control Set	
 Check	Runs a version check of selected nodes (see About Version Checks on page 44).
 Baseline	Runs a baseline operation on selected nodes (see About Baselines on page 43).
 Promote	Promotes all current versions for each selected node (see What is Promotion? on page 47).
 Run Actions	Runs specified actions on the selected nodes (see Running Actions with the Run Actions Feature on page 119).
Modify Set	
 Properties	Defines the values of custom properties for selected nodes (see What are Custom Properties? on page 197).
 Restart Agents	Restarts the services of selected TE Agent nodes (see Restarting Tripwire Enterprise Agents on page 412).
 Configure	Modifies TE Agent configuration properties for selected TE Agent nodes (see Changing TE Agent Configuration Properties on page 417).

Table 139. Report Viewer buttons in Elements View










Button	Description
 Report View	Reverts report output to standard Report View.
 Versions View	Converts report output to Versions View (see Table 140 on the next page).
Control Set	
 Check	Runs a version check of the monitored object represented by each selected element (see About Version Checks on page 44).
 Baseline	Runs a baseline operation for the monitored object represented by each selected element (see About Baselines on page 43).
 Promote	Promotes the current version of each selected element (see What is Promotion? on page 47).
 Run Actions	Runs specified actions for each of the selected elements (see Running Actions with the Run Actions Feature on page 119).
Modify Set	
 Adjust Rule	Modifies the start points and stop points of the rule that identified the monitored object represented by a selected element (see What is the Adjust Rule Feature? on page 84).
 Properties	Defines the values of custom properties for a selected element (see What are Custom Properties? on page 197).
 Delete	Deletes selected elements.

Table 140. Report Viewer buttons in Versions View














Button	Description
 Report View	Reverts report output to standard Report View.
 Elements View	Converts report output to Elements View (see Table 139 on the previous page).
Control Set	
 Check	Runs a version check of the monitored object represented by each selected element version (see About Version Checks on page 44).
 Baseline	Runs a baseline operation for the monitored object represented by each selected element version (see About Baselines on page 43).
 Promote	Promotes each selected element version (see What is Promotion? on page 47). Note: If a selected version is a current baseline, no action is taken.
 Run Actions	Runs specified actions for each of the selected element versions (see Running Actions with the Run Actions Feature on page 119).
Modify Set	
 Properties	Defines the values of custom properties for a selected element version (see What are Custom Properties? on page 197).

Table 141. Report Viewer buttons in Test Results View

Button	Description
 Report View	Reverts report output to standard Report View.
 Re-run test	Runs the policy test for each selected policy test result (see How Does a Policy Test Work? on page 135).
 New Work Order	Creates a remediation work order for the selected policy test results (see Working with Remediation Work Orders on page 255).
 New Waiver	Creates a waiver for each selected policy test result (see What are Policy Scores? on page 138).
 Promote	Promotes each selected policy test result (see What is Policy Test Promotion? on page 146).

Running a Dashboard

To run a dashboard:

1. In the Manager bar, click **REPORTS**.
2. In the tree pane, select the report group containing the dashboard.
3. In the main pane, select the  **Run Report** link for the dashboard.
4. In the Dashboard Viewer, review the dashboard's report output.
 - To open a report in the Report Viewer, click the report's thumbnail.
 - If desired, select a **Refresh rate**. The refresh rate determines the frequency with which Tripwire Enterprise updates the displayed report output in the dashboard.


Note If the dashboard's **refresh rate** setting is less than the system **session timeout** setting, and you leave the Dashboard Viewer open in the TE interface, Tripwire Enterprise will not terminate the session after the specified period of inactivity. This is because dashboards are subject to data refreshes, and each data refresh resets the session timeout clock. To adjust the timeout setting, see [Changing System Preferences on page 266](#).

5. To close the Dashboard Viewer, click **Close**.

Archiving Report Output

For an introduction to report archives, see [How Do I Manage Report Output? on page 181](#).

To run a report and archive the output:

1. In the Manager bar, click **REPORTS**.
2. In the tree pane, click the report group containing the report.
3. In the main pane, select the  **Run Report** link for the report.


When the report finishes, TE presents the output in the Report Viewer.

4. Click  **Archive Report**.


Working with Archived Report Output

For an introduction to report archives, see [How Do I Manage Report Output?](#) on page 181.

To access the archived output of a report:






1. In the Manager bar, click **REPORTS**.
2. In the tree pane, select the report group containing the report.
3. In the main pane, select the report in the **Name** column.
4. In the report properties dialog, select the **Archive** tab.
5. Select the  **View Report** link for the desired output.

The archived output opens in the Report Viewer. [Table 142 \(below\)](#) describes each of the available buttons in the Report Viewer.

Note For an archived report, the  **Archive Report** button is disabled.

6. Click **Close**.

Table 142. Available Report Viewer buttons for archived report output

Button	Description
 CSV Export	Exports the report output to a CSV file. Note: This button is only available with the following report types: <ul style="list-style-type: none">• Changed Elements• Changes by Rule or Group• Detailed Changes• Detailed Test Inventory• Detailed Test Results• Device Inventory• Last Node Check Status• Tasks• Test Results By Node• Unmonitored Nodes• Unreconciled Change Aging
 PDF Export	Exports the report output to a PDF file.
 XML Export	Exports the report output to an XML file.
 E-mail	E-mails the report output to specified recipients.
 Print	Prints a hard copy of the report output.

Deleting Archived Report Output

To delete the archived output of a **system report**, the Delete Archived Reports permission must be assigned to your user account. For more information, see *What are System Reports and User Reports?* (on page 184) and *What are User Permissions and User Roles?* (on page 204).

To delete the archived output of a report:

1. In the Manager bar, click **REPORTS**.
2. In the tree pane, select the report group containing the report.
3. In the main pane, click the report in the **Name** column.
4. In the report properties dialog, select the **Archive** tab.
5. Select the check box for each report archive to be deleted.
6. Click **✕ Delete**.
7. Click **OK** to confirm.

Appendices

Appendix I: Definitions of User Permissions

For an introduction to user permissions, see [What are User Permissions and User Roles?](#) on page 204. Table 143 defines each user permission in Tripwire Enterprise.

Appendix II: User Permissions for Procedures (in the Tripwire Enterprise online help) lists the required user permissions for each procedure in the *Tripwire Enterprise User Guide*.

Notes	<p>To enable the Create or Delete permissions for a Manager, a user's effective role must also have the associated Link permission.</p> <p>For example, if a user's effective role has the Create permission for the Action Manager, but not the Manager's Link permission, the user will be unable to create actions. To create actions, the effective role must also have the Link permission.</p> <p>In addition:</p> <ul style="list-style-type: none"> • To modify the order of actions in an action group, the Action Manager's Update and Link permissions are required. • To change the weights for a TE policy or policy test group, the Policy Manager's Update and Link permissions are required.
--------------	--

Table 143. Definitions of user permissions

Action Management Permissions	This permission grants users the ability to ...
Create	... create (or import) actions and action groups. Note: To create an execution action, a user must also have the Create Execution Actions permission.
Create ACL	... create, edit, and delete access controls for actions and action groups.
Create Execution Actions	... create execution actions.
Delete	... delete actions and action groups.
Link	... link/unlink actions and action groups.
Load	... view the Action Manager.
Run Execution Actions	... run execution actions.
Update	... edit the properties of actions and action groups. Note: To edit an execution action, a user must also have the Update Execution Actions permission.
Update Execution Actions	... edit the properties of execution actions.
Criteria Set Management Permissions	This permission grants users the ability to ...

Create	... create criteria sets.
Delete	... delete criteria sets.
Load	... view the Criteria Sets page in the Settings Manager.
Update	... edit the properties of existing criteria sets.
Custom Node Settings Permissions	This permission grants users the ability to ...
Create	... create custom node types.
Delete	... delete custom node types.
Load	... view the Custom Node Types page in the Settings Manager.
Update	... edit the properties of custom node types.
E-mail Server Management Permissions	This permission grants users the ability to ...
Create	... create e-mail servers in TE.
Delete	... delete e-mail servers in TE.
Load	... view the E-mail Servers page in the Settings Manager.
Update	... edit the properties of e-mail servers.
Element Management Permissions	This permission grants users the ability to ...
Check	... run version checks of monitored objects.
Delete	... delete elements in TE.
Update	<p>... perform the following tasks:</p> <ul style="list-style-type: none"> • Change the properties of an element version. • Promote an element version. • Baseline an element. • Run an action with the Run Actions feature in the Node Manager.
Home Page Management Permissions	This permission grants users the ability to ...
Manage	... create, configure, and delete any home page.
Manage Own	... create, configure, and delete any home page for which the user's account is the only one assigned.
License Management Permissions	This permission grants users the ability to ...
Add	... add license files.
Delete	... delete license files.
Load	... view the Licenses page in the Settings Manager.

Log Management Permissions	This permission grants users the ability to ...
Delete	... delete log messages.
Load	... view the Log Manager.
Miscellaneous Permissions	This permission grants users the ability to ...
Collect Support Data	... create a support archive file with the Support Data feature in the Settings Manager.
Edit Active Directory Preferences	... modify the Active Directories page in the Settings Manager.
Edit LDAP directory Preferences	... modify the LDAP Directories page in the Settings Manager.
Edit Log Management Preferences	... modify the Log Management page in the Settings Manager.
Edit Server Preferences	... modify the Server Preferences page in the Settings Manager.
Edit System Preferences	... modify the System Preferences page in the Settings Manager.
Export Passwords	... export passwords when exporting TE objects to an XML file. (The passwords are encrypted in the file.)
Export Settings	... export all settings from the Settings Manager to an XML file.
Import Settings	... import an XML settings file to the Settings Manager.
Manage Custom Property Definitions	... create, modify, or delete custom properties in the Settings Manager.
Manage Custom Property Values	... modify the values of custom properties assigned to nodes, elements, and element versions.
Manage Database	... regenerate the TE Console database indices.
Manage Login Methods	... modify the Login Method page in the Settings Manager.
Manage Promotion Approval Templates	... modify the Approval Templates page in the Settings Manager.
Manage System Searches	... create saves searches that are available to all users.
Update Server Configuration	... modify the Configure TE Console settings in the Settings Manager.
Node Management Permissions	This permission grants users the ability to ...
Create	... create (or import) nodes and node groups.
Create ACL	... create, edit, and delete access controls for nodes and node groups.
Delete	... delete nodes and node groups.
Link	... link/unlink nodes and node groups.

Load	... view the Node Manager.
Restart Agent Nodes	... restart TE Agents with the Restart Agents button in the Node Manager.
Update	... edit nodes and node groups.
Update Agent Configurations	... modify TE Agent configurations with the Configure button in the Node Manager.
Upgrade	... upgrade TE Agent systems with the Upgrade button in the Node Manager.
View	... view the properties of a node or node group.
Policy Test Management Permissions	This permission grants users the ability to ...
Create	... create (or import) policies, policy tests, and policy test groups.
Create ACL	... create, edit, and delete access controls for policies, policy tests, and policy test groups.
Create Waiver	... create waivers.
Delete	... delete policies, policy tests, and policy test groups.
Execute Policy Based Remediation	... execute automated remediation on a node.
Link	... link/unlink policies, policy tests, and policy test groups.
Load	... view the Policy Manager.
Run Policy Test	... run policy tests.
Update	... edit policies, policy tests, and policy test groups.
Update Policy Based Remediation	... update automated remediation information in policy tests.
Update Waiver	... edit waivers.
Post-Remediation Service Command Permissions	This permission grants users the ability to ...
Update	... update post-remediation service commands in the Settings Manager.
Remediation Work Orders Permissions	This permission grants users the ability to ...
Approve	... approve an entry in a remediation work order.
Assign	... assign a remediation work order to a user.
Close	... close a remediation work order.
Create	... create a remediation work order.
Delete	... delete a remediation work order.
Update	... update a remediation work order.
Report Management Permissions	This permission grants users the ability to ...

Create Archived	... archive the output of system reports.
Delete Archived	... delete existing archived output of system reports.
Load	... view the Report Manager.
Manage System Reports	... create, edit, delete, and link/unlink system reports.
Rule Management Permissions	This permission grants users the ability to ...
Create	... create (or import) rules and rule groups. Note: To create a COVR, COCR, or COHR, a user must also have the Create Command Output Rules permission.
Create ACL	... create, edit, and delete access controls for rules and rule groups.
Create Command Output Rules	... create COVRs, COCRs, and COHRs.
Delete	... delete rules and rule groups.
Link	... link/unlink rules and rule groups.
Load	... view the Rule Manager.
Update	... edit rules and rule groups. Note: To edit a COVR, COCR, or COHR, a user must also have the Update Command Output Rules permission.
Update Command Output Rules	... edit the properties of COVRs, COCRs, and COHRs.
Use	... use rules to baseline or version check monitored systems. Notes: Baselining also requires the Update Elements permission, and version checking requires the Check Elements permission. To use a COVR, COCR, or COHR, a user must also have the Use Command Output Rules permission.
Use Command Output Rules	... use COVRs, COCRs, and COHRs.
Severity Management Permissions	This permission grants users the ability to ...
Create	... create severity ranges.
Delete	... delete severity ranges.
Load	... view the Severity Ranges page in the Settings Manager.
Update	... edit the properties of existing severity ranges.
Task Management Permissions	This permission grants users the ability to ...
Create	... create (or import) tasks and task groups.
Create ACL	... create, edit, and delete access controls for tasks and task groups.
Delete	... delete tasks and task groups.

Link	... link/unlink tasks and task groups.
Load	... view the Task Manager.
Run	... run tasks and task groups.
Stop	... stop running tasks and task groups.
Update	... edit tasks and task groups.
User Management Permissions	This permission grants users the ability to ...
Create	... create user accounts, groups, and roles.
Delete	... delete user accounts, groups, and roles.
Load	... view the Users, User Groups, and Roles pages in the Settings Manager.
Update	... edit user accounts, groups, and roles.
Variable Management Permissions	This permission grants users the ability to ...
Create	... create global variables.
Delete	... delete global variables.
Load	... view the Global Variables page in the Settings Manager.
Update	... edit global variables.

Index

A

AAA Log Monitoring Tool

- about 237

access controls

- about 208

- and the administrator account 208

- and user roles 208

- changing for a node or node group 333

- changing for a Policy Manager object 541

- changing for a rule or rule group 443

- changing for a task or task group 515

- changing for an action or action group 489

- creating for a node or node group 333

- creating for a Policy Manager object 541

- creating for a rule or rule group 443

- creating for a task or task group 515

- creating for an action or action group 489

- defined 208

- deleting for a node or node group 334

- deleting for a Policy Manager object 542

- deleting for a rule or rule group 444

- deleting for a task or task group 516

- deleting for an action or action group 490

- example 211

- for TE objects in pre-configured XML files 221

- helpful hints 211

- inheritance rules 210

- restricting node visibility with 212

action groups

- about 120

- changing properties 487

- creating 491

- deleting 502

- exporting 505

- importing 506

- linking 503
- moving 503
- ordering actions in 488
- tabs in action group property dialogs 487
- unlinking 504
- viewing 478

Action Manager

- about 116
- columns in Action Manager table 479
- defined 27

actions

- about 116
- about conditional actions 125
- about e-mail actions 120
- about execution actions 121
- about restore actions 123
- about run report actions 188
- about run rule actions 123
- about running actions 119
- about set custom value actions 124
- about SNMP actions 124
- changing properties 482
- creating a conditional action 491
- creating a promote action 495
- creating a restore action 496
- creating a run command action 497
- creating a run report action 497
- creating a run rule action 498
- creating a run task action 498
- creating a set custom value action 499
- creating a severity override action 499
- creating a syslog action 500
- creating an e-mail action 492
- creating an execution action 493
- creating an SNMP action 500
- deleting 502
- duplicating 501
- exporting 505
- import from XML files 230

- importing 506
- linking 503
- moving 503
- ordering in an action group 488
- Outside Change Window Action 122
- running with version checks 119
- search criteria 481
- searching for 480
- tabs in action property dialogs 482
- tabs in conditional action property dialogs 484
- types 116
- types of common actions 117
- types of conditional actions 125
- types of network device actions 118
- unlinking 504
- user permissions for 611
- using the Run Actions feature with specified elements 402
- using the Run Actions feature with specified nodes or node groups 403
- viewing 478

Active Directory nodes

- defined 52

Active Directory rules

- defined 80

Adjust Rule feature

- about 84
- adding a stop point with 400
- adding start points with 398
- deleting stop points with 401
- editing start points with 399

Administration settings

- about 194

administrator account

- about 206

Agent software

- defined 54

alert data

- defined 192

- alert generators
 - clearing alert data in 247
 - defined 192
 - reviewing alert data in 247
 - types 193
- alert widgets
 - changing properties 246
 - clearing alert data from an alert generator 247
 - defined 190
 - reviewing alert data in an alert generator 247
- approval templates
 - defined 273
 - working with 273
- Archive Log Messages Task
 - defined 127
 - running 170
- archiving
 - log messages 170
 - report output 607
- Asset View
 - disabling checks and baselines 387
 - overview 339
 - resolving errors 317
 - restarting Agents 412
 - using 346
- assets
 - applying tags manually 350
 - filtering in the Asset View tab 348
 - overview 339
 - resolving errors 317
 - viewing and selecting 349
- attribute policy tests
 - defined 132
- attributes
 - defined 37
 - defining formats for Active Directory attributes 311
 - defining formats for LDAP directory attributes 311
 - for databases 307

- for UNIX file systems 301
 - for Windows file systems 302
 - for Windows registries 304
 - for Windows RSoP rules 307
 - of directories 93
 - types of directory attributes 97
- audit-event collection
- about 63
 - and the Event Generator 66
 - configuring for multiple Agents 422
 - license requirements 202
 - sources 63
- audit events
- types created by Event Generators on UNIX systems 69
 - types created by Event Generators on Windows systems 68
- authorized composite changes
- defined 174
 - example in a Composite Changes Report 180
- automated remediation
- about 151
 - approving remediation a work order 258
 - assigning a work order 257
 - changing remediation information 536
 - checking the status of a work order 253
 - closing or deleting work orders 260
 - compared to manual remediation 151
 - creating a work order 255
 - creating home pages for 162
 - deferring remediation in a work order 259
 - denying remediation in a work order 258
 - implementing in TE 155
 - licenses 202
 - running remediation in a work order 259
 - user permissions for 159
 - using a failing tests widget 249
 - using a remediation work orders widget 253
 - workflow 151
- automated remediation licenses
- about 202

- applying or removing to/from nodes 418

Automatically Linked node group

- defined 58

availability

- defined 38

Axon Agent

- creating a node with 54

- defined 54

- differences with TE Agent 55

- upgrading 279, 413

B

Baseline Elements Reports

- defined 173

baseline rule tasks

- about 128

- creating 517

- defined 43, 127

- stopping 523

baseline versions

- defined 37

baselines

- promoting a specific element version 393

- promoting all current versions for a node or node group 395

- promoting by match 396

- promoting by reference 397

baselining

- defined 43

- disabling temporarily 387

- initial baselining of monitored objects 382

- re-baselining monitored systems 383

- re-baselining specific monitored objects 384

- Tripwire Enterprise objects used 43

best practices

- for tagging 342

button bar

- about 25

- by-match conditional actions
 - and by-match selection method 74
- by-match selection method
 - about 73
 - discrepancies and promote operations 75
 - supported Tripwire Enterprise features 74
- by-reference selection method
 - about 76
 - process flow 78

C

- categories
 - of TE log messages 167
- certificates
 - changes to keystores in TE 8.4.1 421
- Change Audit Coverage Reports
 - defined 173
- change audit licenses
 - about 202
 - applying or removing to/from nodes 418
- Change Process Compliance Reports
 - defined 173
- Change Rate Reports
 - defined 173
- Change Variance Reports
 - defined 173
- change versions
 - defined 37
- Change Window Reports
 - defined 173
- change windows
 - defined 122
- Changed Elements Reports
 - defined 173

Changes by Node or Group Reports

defined 174

Changes by Rule or Group Reports

defined 174

Changes by Severity Reports

defined 174

changing

access controls for a node or node group 333

access controls for a Policy Manager object 541

access controls for a rule or rule group 443

access controls for a task or task group 515

access controls for an action or action group 489

action group properties 487

action properties 482

Active Directory preferences 311

Agent configuration properties 417

COCR filter criteria 442

COCR search-and-replace criteria 442

COVR filter criteria 442

COVR search-and-replace criteria 442

element properties 326

element version properties 327

file system preferences 310

home page properties 242

home pages in Settings Manager 291

Included Node Properties in multiple policy tests 539

LDAP directory preferences 311

list of monitored objects in a configuration file rule 441

list of monitored objects in a file rule 441

log management settings 268

node group properties 325

node properties 321

post-remediation service commands 283

properties of a criteria set 308

properties of a dashboard 591

properties of a dashboard widget 248

properties of a failing tests widget 249

properties of a log center event widget 251

properties of a policy test 536

- properties of a policy test group 538
- properties of a report 589
- properties of a report group 590
- properties of a report in a report widget 252
- properties of a report widget 251
- properties of a TE policy 534
- properties of a user account 286
- properties of an alert widget 246
- queries in a database query rule 471
- rule group properties 440
- rule properties 437
- scoring thresholds for a TE policy 556
- specifiers in a Windows RSoP rule 472
- start points 466
- stop points 469
- system preferences 266
- task group properties 514
- task properties 512
- the layout of widgets in a home page 242
- the list of excluded nodes in multiple policy tests 540
- the list of user accounts assigned to a home page 243
- the password of a user account 286
- user difference settings 265
- user preference settings 262
- user roles 287
- waivers 566

check rule tasks

- about 129
- creating 518
- creating current baselines for 522
- defined 127
- running actions with 119
- stopping 523

Clear Unlinked Groups task

- defined 127

cloning

- element versions 410

clusters

- and equivalent Tripwire Enterprise objects 62

COCRs

see command output capture rules (COCRs) 99

COHRs

see command output hypervisor rules (COHRs) 82

Command Line Interface (CLI)

about 238

command output

as a file server node element 39

as a network device node element 38

as a VI node element 39

command output capture rules (COCRs)

about 99

and regular expressions 107

changing filter criteria 442

changing search-and-replace criteria 442

creating 445

defined 81

examples 100

features 99

regular-expression syntax 108

command output hypervisor rules (COHRs)

creating 446

defined 82

command output validation rules (COVRs)

about 103

and regular expressions 107

changing filter criteria 442

changing search-and-replace criteria 442

creating 446

defined 80

examples 104

features 103

regular-expression syntax 108

common actions

defined 116

Compact Element Versions Task

about 130

defined 127

- comparing
 - a change version with the current baseline 388
 - an element version with the current baseline 389
 - any two versions of different elements 391
 - any two versions of the same element 390

- Compliance History Reports
 - defined 174

- compliance statistics
 - about 137
 - defined 137
 - filtering in the Policy Manager 557
 - how to monitor 137
 - in Compliance tab for a policy test 551
 - in Compliance tab for a policy test group 552
 - in Compliance tab for a TE policy 553

- Composite Changes Reports
 - defined 174
 - example 179

- conditional actions
 - about 125
 - creating 491
 - defined 116
 - example of nested conditional actions 126
 - tabs in conditional action property dialogs 484
 - types 125

- configuration assessment licenses
 - about 202
 - applying or removing to/from nodes 418

- configuration file rules
 - changing list of monitored objects in 441
 - creating 447
 - defined 80

- configuration files
 - as a network device node element 38
 - as a VI node element 39

- Configuration pane
 - tabs 240

- configuration parameters
 - as a database node element 38
 - as a VI node element 39
- Configure Axon Agents task
 - defined 127
- conflicts
 - about 224
- container entries
 - defined 94
- content
 - exporting element version content 408
 - importing element version content 409
- content policy tests
 - defined 132
- COVRs
 - see command output validation rules (COVRs) 103
- creating
 - access controls for a node or node group 333
 - access controls for a Policy Manager object 541
 - access controls for a rule or rule group 443
 - access controls for a task or task group 515
 - access controls for an action or action group 489
 - action groups 491
 - baseline rule tasks 517
 - check rule tasks 518
 - command output capture rules 445
 - command output hypervisor rules 446
 - command output validation rules 446
 - conditional actions 491
 - configuration file rules 447
 - current baselines for a check rule task 522
 - custom nodes 368
 - dashboards 594
 - database metadata rules 448
 - database nodes 370
 - database query rules 449
 - directory rules 450
 - directory server nodes 369

- distributed virtual switch configuration rules 455
- e-mail actions 492
- execution actions 493
- file rules 451
- file system rules 455
- home pages in Home Page Manager 241
- home pages in Settings Manager 290
- launch in context (LIC) URLs 235
- log transfer rules 451
- network device nodes 374
- node groups 368
- policy test groups 547
- policy tests 545
- promote actions 495
- remediation work order 255
- report groups 593
- report tasks 519
- reports 592
- restore actions 496
- rule groups 445
- run command actions 497
- run report actions 497
- run rule actions 498
- run task actions 498
- saved searches 234
- scoring thresholds for a TE policy 555
- set custom value actions 499
- severity override actions 499
- SNMP actions 500
- start points 462
- status check rules 452
- stop points 467
- syslog actions 500
- task groups 519
- TE policies 543
- user accounts 285
- VI hypervisor rules 453
- VI nodes 375
- virtual machine configuration rules 453
- virtual switch configuration rules 454

- waivers 564
- Windows registry rules 457
- Windows RSoP rules 458
- criteria sets
 - and database metadata rules 89
 - and directory rules 96
 - and file system rules 83
 - and Windows registry rules 87
 - changing 308
 - creating for database metadata rules 307
 - creating for database rules 307
 - creating for file system rules 300
 - creating for Windows registry rules 304
 - creating for Windows RSoP rules 306
 - deleting 309
 - duplicating in Settings Manager 309
 - user permissions for 611
- current baselines
 - creating for a check rule task 522
- custom file rules
 - defined 80
- custom nodes
 - creating 368
 - creation of 56
 - defined 52
 - user permissions for 612
 - working with 299
- custom properties
 - about 197
 - and set custom value actions 124
 - changing in policy test properties 539
 - defined 197
 - defining values for a node 328
 - defining values for an element 330
 - defining values for an element version 331
 - example 199
 - settings 195
 - types 197
 - working with 298

Customer Center widgets
defined 190

D

Dashboard Viewer
defined 182

dashboard widgets
changing properties 248
defined 190
running reports in 248

dashboards
about 182
changing properties of 591
changing the properties of a dashboard widget 248
creating 594
defined 182
deleting 596
duplicating 595
exporting 599
import from XML files 230
importing 600
linking 597
moving 597
running 607
running a report in a dashboard widget 248
tabs in dashboard property dialogs 591
unlinking 598
viewing 585

database definition language
see DDL 38

database index statistics
recalculating 269

database indices
recalculating statistics for 269

database metadata rules
about 89
changing start points 466

- changing stop points 469
- components 89
- creating 448
- creating criteria sets for 307
- creating start points 462
- creating stop points 467
- defined 79
- deleting start points 466
- deleting stop points 469
- objects monitored by 89

database nodes

- configuring SSL 419
- creating 370
- defined 52
- how to create 56
- types of elements 38

database objects

- defined 38

database queries

- managing with whitelists 429

database query rules

- about 92
- adding a query to 470
- changing a query in 471
- creating 449
- creating criteria sets for 307
- defined 79
- deleting a query from 471

database rules

- attributes for 307
- types 79

database servers

- defined 52

datacenters

- and equivalent Tripwire Enterprise objects 62

datastores

- and equivalent Tripwire Enterprise objects 62

DDL

- and database objects 38

defining

- custom property values for a node 328
- custom property values for an element 330
- custom property values for an element version 331

delegated Agents

- assigning to a node 411
- defined 56, 411

deleting

- access controls for a node or node group 334
- access controls for a Policy Manager object 542
- access controls for a rule or rule group 444
- access controls for a task or task group 516
- access controls for an action or action group 490
- action groups 502
- actions 502
- archived report output 609
- criteria sets 309
- dashboards 596
- elements 378
- home pages in Home Page Manager 244
- home pages in Settings Manager 291
- license files 297
- nodes and node groups 377
- Policy Manager objects 549
- post-remediation service commands 284
- queries from a database query rule 471
- remediation work orders 260
- reports and report groups 596
- rule groups 459
- rules 459
- saved searches 235
- scoring thresholds for a TE policy 556
- specifiers from a Windows RSoP rule 472
- start points 466
- stop points 469
- task groups 521
- tasks 521

- TE log messages 583
- user accounts 288
- waivers 569
- widgets 254
- Detailed Changes Reports
 - defined 175
- Detailed Node View
 - defined 313
- Detailed Test Inventory Reports
 - defined 175
- Detailed Test Results Reports
 - defined 175
- Detailed Waivers Reports
 - defined 175
- Device Inventory Reports
 - defined 175
- Difference Viewer
 - about 46
 - clearing Mark for Compare selections 392
 - license requirements 202
- directories
 - about 93
 - about object classes and schemas 94
 - and distinguished names 95
 - attributes of 93
 - common attribute names 93
 - defined 52
 - directory protocol 52
 - entries 93
 - example hierarchy 95
 - organization of 94
- directory rules
 - about 96
 - changing start points 466
 - changing stop points 469
 - components 96
 - creating 450
 - creating start points 462

- creating stop points 467
- deleting start points 466
- deleting stop points 469
- types 80

directory server nodes

- configuring SSL 419
- creating 369
- defined 52
- how to create 56
- types of elements 38

directory servers

- binary attributes 97
- defined 52
- defining formats for Active Directory attributes 311
- defining formats for LDAP directory attributes 311
- security attributes 97

disabling

- checks and baselines on a node temporarily 387
- tasks 524

Discovered node group

- defined 58

discovered nodes alert generators

- defined 193

discovery

- see VI node discovery 56

distributed virtual port groups

- and equivalent Tripwire Enterprise objects 62

distributed virtual switch configuration rules

- creating 455
- defined 82

distributed virtual switch nodes

- defined 53

distributed virtual switches

- and equivalent Tripwire Enterprise objects 62

downloading

- Agent log files 423

- duplicating
 - a task 520
 - an action 501
 - criteria sets in Settings Manager 309
 - dashboards 595
 - home pages in Home Page Manager 244
 - home pages in Settings Manager 290
 - nodes 376
 - policy tests 548
 - reports 595
 - rules 459
- dynamic policy scoping
 - setting 266

E

- e-mail actions
 - about 120
 - creating 492
 - defined 117
- e-mail servers
 - about 196
 - defined 196
 - user permissions for 612
 - working with 272
- effective scopes
 - about 133
 - defined 131
 - factors determining 134
- effective user roles
 - about 207
 - defined 204
- Element Content Reports
 - defined 175
- element custom properties
 - defined 197
- element versions
 - changing properties 327

- clearing Mark for Compare selections 392
- cloning an element version 410
- Compact Element Versions Task 130
- comparing a change version with the current baseline 388
- comparing an element version with the current baseline 389
- comparing any two versions of different elements 391
- comparing any two versions of the same element 390
- custom properties for 298
 - defined 36
 - defining custom property values for 331
- exporting content of 408
- importing element version content 409
- promoting a specific element version 393
- promoting all current versions for a node or node group 395
- promoting by match 396
- promoting by reference 397
- search criteria 365
- searching for 364
- tabs in element version property dialogs 328
- using the Difference Viewer 46

elements

- changing properties 326
- custom properties for 298
- defined 36
- defining custom property values for 330
- deleting 378
- differences between TE Agent and Axon Agent 40
- filtering in the Node Manager 320
- for database nodes 38
- for directory server nodes 38
- for file server nodes 39
- for network device nodes 38
- for virtual infrastructure nodes 39
- search criteria 362
- searching for 361
- tabs in element property dialogs 327
- user permissions for 612
- using the Difference Viewer 46
- viewing 313

Elements Reports

- defined 175

enabling

- checks and baselines on a node temporarily 387
- tasks 523

entries

- about directory entries 93
- container entries in directories 94
- directory entries defined 38
- leaf entries in directories 94
- Windows registry entries defined 85

errors

- resolving for nodes 317

Event Generators

- and collection of audit events 66
- and real-time monitoring 70
- defined 66
- guidelines for AIX systems 72
- guidelines for Linux systems 72
- types of audit events created on UNIX systems 69
- types of audit events created on Windows systems 68

execution actions

- about 121
- and restoration 50
- command line variables 494
- creating 493
- defined 117

exporting

- about export of TE objects 217
- actions and action groups 505
- dashboards 599
- element version content 408
- home pages 292
- log messages 582
- nodes and node groups 406
- Policy Manager objects 573
- post-remediation service commands 284
- reports and report groups 599

- rules and rule groups 475
- saved searches 235
- settings 277
- tasks and task groups 527

F

failing tests widgets

- changing properties 249
- defined 191

Fast Track

- using Fast Track to configure TE 32
- what to do after Fast Track 34

file rules

- changing list of monitored objects in 441
- creating 451
- defined 80

file server nodes

- creating 54
- defined 52
- types of elements 39

file server rules

- types 81

file servers

- defined 52

file system preferences

- descriptions 310

file system rules

- about 83
- changing start points 466
- changing stop points 469
- components of 83
- creating 455
- creating criteria sets for 300
- creating start points 462
- creating stop points 467
- deleting start points 466
- deleting stop points 469

file systems

- attributes for UNIX systems 301
- attributes for Windows systems 302
- defined 52
- preferences 310

filtering

- in the Log Manager 578
- in the Node Manager 320
- in the Policy Manager 557

FIPS mode

See *the Tripwire Enterprise Hardening Guide*

folders

- and equivalent Tripwire Enterprise objects 62

Frequently Changed Elements Reports

- defined 175

Frequently Changed Nodes Reports

- defined 175

G

getting started

- using Fast Track 32

global variables

- about 196
- defined 196
- working with 271

Group Policy Objects

- defined 88

groups

- about 29
- about action groups 120
- default groups 30
- default Node Manager groups 58
- import from XML files 226
- smart node groups 57

H

health

- resolving node errors 317

help

- launching online help 25

Home Page Manager

- defined 27
- diagram 190
- tabs in the Configuration pane 240

home pages

- about 189
- adding a widget 245
- changing layout of widgets 242
- changing properties 242
- changing properties in Settings Manager 291
- changing properties of a dashboard widget 248
- changing properties of a failing tests widget 249
- changing properties of a log center event widget 251
- changing properties of a report widget 251
- changing properties of an alert widget 246
- changing the list of assigned user accounts 243
- creating in Home Page Manager 241
- creating in Settings Manager 290
- defined 189
- deleting in Home Page Manager 244
- deleting in Settings Manager 291
- duplicating in Home Page Manager 244
- duplicating in Settings Manager 290
- exporting 292
- import from XML files 226
- importing 292
- viewing 240
- who can view and configure 192

Home Pages tab

- defined 240

hypervisors

- defined 59

I

import timestamps

- defined 222

importing

- about conflicts 224
- about import of TE objects 217
- about import of XML files 222
- actions and action groups 506
- actions in XML files 230
- dashboards 600
- dashboards in XML files 230
- element version content 409
- groups in XML files 226
- home pages 292
- home pages in XML files 226
- nodes and node groups 407
- nodes in XML files 227
- order of import for multiple XML files 219
- Policy Manager objects 574
- policy tests in XML files 230
- post-remediation service commands 283
- reports and report groups 600
- rules and rule groups 476
- rules in XML files 230
- saved searches 235
- settings 276
- settings in XML files 225
- tasks and task groups 528
- tasks in XML files 230
- TE policies in XML files 229
- VI nodes in XML files 228

initial baselining

- of monitored objects 382

interface toolbar

- about 25

Inventory Changes Reports

- defined 176

- inventory objects
 - and equivalent TE objects 62
 - defined 60
- inventory views
 - defined 60

K

- keys
 - see Windows registry keys 85

L

- Last Node Check Status Reports
 - defined 176
- launch in context (LIC) URLs
 - creating 235
 - using 236
- LDAP directory nodes
 - defined 52
- LDAP rules
 - defined 80
- LDAP/Active Directory login method
 - configuring 294
- leaf entries
 - defined 94
- license files
 - about 202
 - adding 297
 - deleting 297
 - licensing and unlicensing nodes 418
 - user permissions for 612
- linked objects
 - defined 213
- linking
 - about 214
 - actions and action groups 503
 - dashboards 597

- defined 213
- example 215
- link emblem 214
- nodes and node groups 380
- Policy Manager objects 571
- reports and report groups 597
- rules and rule groups 473
- tasks and task groups 525

loading

- a saved search 234

local variables

- about 196
- defined 196

log center event widgets

- changing properties 251
- defined 191

log files

- downloading Agent log files 423

log management settings

- changing 268
- descriptions 268

Log Manager

- about 166
- columns in Log Manager table 577
- defined 27
- filters 578

log messages

- about 166
- and the Archive Log Messages Task 170
- defined 166
- exporting 582
- filtering in the Log Manager 578
- forwarding to a syslog server 268
- types 166
- user permissions for 613
- viewing properties 577

log transfer rules

- about 55, 98

- creating 451
- defined 81
- logging out
 - of Tripwire Enterprise Console 25
- login methods
 - about 207
 - configuring 294

M

- main pane
 - about 26
- Manager bar
 - about 24
- Managers
 - defined 27
 - in the Tripwire Enterprise interface 27
- manual remediation
 - about 165
 - compared to automated remediation 151
 - viewing manual remediation instructions 165
- match files
 - contents and matching strategies 73
 - defined 73
- matching objects
 - and import of XML files 222
- matching strategies
 - and match file contents 73
 - defined 73
- metadata rules
 - see database metadata rules 79
- Missing Elements Reports
 - defined 176
- modification timestamps
 - defined 222
- monitored objects
 - defined 37

- identified by start points and stop points 461
- initial baselining of 382
- re-baselining of 384
- restoring manually vs. automatically 50
- version checking 386

monitored systems

- defined 51
- re-baselining 383
- version checking 385

monitoring

- compliance statistics 137

Monitoring Preferences

- about 195

moving

- actions and action groups 503
- dashboards 597
- nodes and node groups 379
- Policy Manager objects 570
- reports and report groups 597
- rules and rule groups 473
- tasks and task groups 525

N

network device actions

- defined 116, 118

network device nodes

- creating 374
- defined 52
- how to create 56
- types of elements 38

network device rules

- types 80

networks (virtual)

- and equivalent Tripwire Enterprise objects 62

node custom properties

- defined 197

node errors alert generators
defined 193

node groups
changing properties 325
creating 368
default node groups 57
deleting 377
exporting 406
importing 407
linking 380
moving 379
smart node groups 57
tabs in node group property dialogs 325
unlinking 381
viewing 313
viewing in Asset View 351

Node Manager
about 51
columns with a node group selected 315
columns with elements displayed 316
columns with rules displayed 316
defined 27
filters 320
viewing nodes and groups in Asset View 351
viewing nodes, node groups, and elements 313

Node Manager baseline operations
defined 43

node types
defined 52

node/rule pairs
and baseline rule tasks 128
and check rule tasks 129
defined 128

nodes
about delegated Agents 56
about smart node groups 57
adding waivers for a single node 336
assigning a delegated Agent to a node 411

- changing properties 321
- changing the list of excluded nodes in policy test properties 540
- creating a custom node type 299
- creating file system nodes by installing Agent software 54
- creating nodes manually with the New Node Wizard 56
- custom properties for 298
- defined 51
- defining custom property values for 328
- deleting 377
- differences between Axon Agent and TE Agent 55
- disabling checks and baselines 387
- duplicating 376
- errors 317
- exporting 406
- import from XML files 227
- importing 407
- licensing and unlicensing 418
- linking 380
- moving 379
- promoting policy test results for 337
- re-running policy tests for a single node 335
- resolving errors 317
- restricting visibility with access controls 212
- search criteria 356
- searching for 355
- tabs in node property dialogs 321
- types 51
- unlinking 381
- user permissions for 613
- viewing 313
- viewing changed nodes 320
- viewing in Asset View 351

Nodes with Changes Reports

- defined 176

O

- online help
 - launching 25

- operational tag sets
 - defined 352
- ordering
 - actions in an action group 488
- Outside Change Window Action
 - about 122
 - defined 117

P

- package objects
 - defined 49
- parent policies
 - defined 131
- pass/fail criteria
 - defined 131
- pass/fail scores
 - defined 139
- password
 - changing for a user account 286
 - controlling login method 294
- password variables
 - defined 196
- permissions
 - see user permissions 204
- policies
 - dynamic policy scoping 266
 - user permissions for 614
- Policy Manager
 - columns in the Tests tab 531
 - Compliance tab for a policy test 551
 - Compliance tab for a policy test group 552
 - Compliance tab for a TE policy 553
 - defined 27
 - filters 557
- Policy Manager objects
 - about 131

- changing access controls for 541
- creating access controls for 541
- defined 131
- deleting 549
- deleting access controls for 542
- example 148
- exporting 573
- importing 574
- linking 571
- moving 570
- types 131
- unlinking 572

policy score change alert generators

- defined 193

policy scores

- about 138
- defined 138
- example 140
- how Tripwire Enterprise calculates 139
- purging 145

policy test groups

- about 131
- and compliance statistics 552
- and weights 138
- changing properties of 538
- creating 547
- tabs in policy test group property dialogs 538
- viewing in the Compliance tab 550
- viewing in the Tests tab 530

policy test results

- defined 135
- promoting 562
- promoting results generated for a node 337
- purging 145
- reviewing in the Policy Manager 144
- search criteria 560
- searching for 559
- tabs in TE policy property dialogs 555
- viewing in a failing tests widget 249

viewing in the Compliance tab 554

policy tests

- about 131
- about pre-configured policy tests from Tripwire 219
- about scopes 133
- and compliance statistics 551
- and parent policies 131
- and severity levels 132
- changing Included Node Properties in 539
- changing properties of 536
- changing the list of excluded nodes in 540
- creating 545
- defined 131
- duplicating 548
- how a policy test works 135
- import from XML files 230
- managing user access for pre-configured policy tests 220
- manual remediation 165
- process flow 136
- promotion options defined 564
- properties defining the scope of 134
- re-running for a single node 335
- running manually 561
- search criteria 532
- searching for 532
- tabs in policy test property dialogs 537
- types 132
- viewing in the Compliance tab 550
- viewing in the Tests tab 530

post-remediation service commands

- about 164
- changing 283
- deleting 284
- exporting 284
- importing 283
- logging 164
- requirements 164
- user permissions for 614

- promote-by-match
 - promoting element versions 396
- promote-by-match actions
 - defined 117
- promote-by-reference actions
 - defined 117
- promote actions
 - and automatic promotion 47
 - and by-match selection method 74
 - creating 495
 - using the by-reference selection method 77
- promote specific versions actions
 - defined 117
- Promote to Baseline Action
 - and automatic promotion 47
 - defined 117
- promoting
 - a specific element version 393
 - all current versions for a node or node group 395
 - policy test results 562
 - promoting by match 396
 - promoting by reference 397
- promotion
 - about 47
 - and by-match selection method 74
 - and software-installation packages 48
 - defined 47
 - discrepancies and by-match selection method 75
 - promotion types for policy test results 564
 - using the by-reference selection method 77
- purging
 - policy scores 145
 - policy test results 145
 - waivers 145

Q

queries

- adding to a database query rule 470
- changing in a database query rule 471
- deleting from a database query rule 471
- query results defined 38

query rules

- see database query rules 79

query whitelists

- about 429

R

re-baselining

- monitored systems 383
- specific monitored objects 384

real-time monitoring

- about 70
- configuring for multiple Agents 422
- license requirements 202

Reference Node Variance Reports

- defined 176

reference nodes

- and conditional by-reference selection method 76

refreshing

- the TE interface 25

registry

- see Windows registry 85

registry entries

- as a file server node element 39

registry keys

- as a file server node element 39

regular expressions

- about 107
- examples 109
- syntax 108

- using with tagging profiles 354
- remediation
 - see automated remediation or manual remediation 151
- Remediation Assessment Reports
 - defined 176
- remediation messages alert generators
 - defined 193
- remediation work orders
 - approving remediation 258
 - assigning 257
 - closing 260
 - creating 255
 - creating from a failing tests widget 249
 - deferring remediation 259
 - deleting 260
 - denying remediation 258
 - running remediation 259
 - user permissions for 614
 - viewing in a remediation work orders widget 253
- Remediation Work Orders Details Reports
 - defined 176
- Remediation Work Orders Summary Reports
 - defined 176
- remediation work orders widgets
 - defined 191
 - using 253
- report criteria
 - defined 172
- report groups
 - changing properties of 590
 - creating 593
 - deleting 596
 - exporting 599
 - importing 600
 - linking 597
 - moving 597
 - tabs in report group property dialogs 590
 - unlinking 598

viewing 585

Report Manager

about 172

columns in Report Manager table 586

defined 28

report output

archiving 607

defined 172

deleting archived output 609

embedded links in 182

managing 181

Report Viewer buttons for archived output 608

Report Viewer buttons in Elements View 605

Report Viewer buttons in Nodes View 604

Report Viewer buttons in standard Report View 602

Report Viewer buttons in Test Results View 606

Report Viewer buttons in Versions View 606

working with archived output 608

report tasks

about 186

components 186

creating 519

defined 127

process flow 187

Report Viewer

buttons for archived report output 608

buttons in Elements View 605

buttons in Nodes View 604

buttons in standard Report View 602

buttons in Test Results View 606

buttons in Versions View 606

report widgets

changing properties 251

changing properties of a report in a report widget 252

defined 191

running reports in 252

reports

about 172

- and embedded links in output 182
- and report tasks 186
- archiving output 607
- changing properties in a report widget 252
- changing properties of 589
- changing the properties of a report widget 251
- changing the properties of a TLC event widget 251
- creating 592
- defined 172
- deleting 596
- deleting archived output 609
- duplicating 595
- example of embedded links in output 183
- exporting 599
- importing 600
- linking 597
- Manage System Reports permission 185
- managing report output 181
- moving 597
- process flow 181
- running in a dashboard widget 248
- running in a report widget 252
- running manually 601
- search criteria 588
- searching for 587
- system reports vs. user reports 184
- tabs in report property dialogs 589
- types of 173
- unlinking 598
- user permissions for 614
- viewing 585
- working with archived output 608

resource pools

- and equivalent Tripwire Enterprise objects 62

restarting

- Tripwire Enterprise Agents 412

restoration

- about 50
- manual vs. automatic 50

- restore actions
 - about 123
 - and restoration 50
 - creating 496
 - defined 118
- restoring
 - a changed file with the Run Actions feature 404
 - multiple files with the Run Actions feature 405
- Resultant Set of Policy
 - see RSoP 88
- reviewing
 - alert data in an alert generator 247
 - policy test results 144
- roles
 - see user roles 287
- root DSE
 - defined 94
- Root Group
 - defined 30
- root keys
 - common 85
- RSoP
 - defined 88
- rule groups
 - changing properties 440
 - creating 445
 - deleting 459
 - exporting 475
 - importing 476
 - linking 473
 - moving 473
 - tabs in rule group property dialogs 440
 - unlinking 474
 - viewing 432
- Rule Manager
 - about 79
 - columns in Rule Manager table 433

defined 27

rules

about 79

about pre-configured rules from Tripwire 219

about the Adjust Rule feature 84

and severity levels 112

changing COCR filter criteria 442

changing COCR search-and-replace criteria 442

changing COVR filter criteria 442

changing COVR search-and-replace criteria 442

changing list of monitored objects in a configuration file rule 441

changing list of monitored objects in a file rule 441

changing properties 437

changing start points 466

changing stop points 469

creating a configuration file rule 447

creating a database metadata rule 448

creating a database query rule 449

creating a directory rule 450

creating a distributed virtual switch configuration rule 455

creating a file system rule 455

creating a status check rule 452

creating a VI hypervisor rule 453

creating a virtual machine configuration rule 453

creating a virtual switch configuration rule 454

creating a Windows registry rule 457

creating a Windows RSoP rule 458

creating command output capture rules (COCRs) 445

creating command output hypervisor rules (COHRs) 446

creating command output validation rules (COVRs) 446

creating file rules 451

creating log transfer rules 451

creating start points 462

creating stop points 467

deleting 459

deleting start points 466

deleting stop points 469

duplicating 459

exporting 475

import from XML files 230

- importing 476
- linking 473
- managing user access for pre-configured rules 220
- moving 473
- search criteria 435
- searching for 434
- tabs in rule property dialogs 438
- types 79
- types of database rules 79
- types of directory rules 80
- types of file server rules 81
- types of network device rules 80
- types of VI rules 82
- unlinking 474
- user permissions for 615
- viewing 432

Run Actions feature

- restoring a changed file 404
- restoring multiple files 405
- running actions for nodes or node groups 403
- running actions for specific elements 402

run command actions

- creating 497
- defined 118

run report actions

- about 188
- creating 497
- defined 117
- optional scope criteria 188

run rule actions

- about 123
- creating 498
- defined 118

run task actions

- creating 498
- defined 118

running

- a dashboard 607

- a report manually 601
- policy tests manually 561
- reports in a dashboard widget 248
- reports in a report widget 252
- tasks and task groups manually 523

S

saved filters

- defined 353
- working with 353

saved searches

- about 233

scopes

- about scopes and Policy Manager objects 133
- defined for TE policies and policy tests 133
- for alert generators 192

Scoring History Reports

- defined 177

Scoring Reports

- defined 176

scoring thresholds

- about 142
- changing for a TE policy 556
- creating for a TE policy 555
- defined 142
- deleting for a TE policy 556
- example 142

searches

- about 232
- action search criteria 481
- creating a saved search 234
- deleting saved searches 235
- element search criteria 362
- element version search criteria 365
- exporting saved searches 235
- features 233
- importing saved searches 235

- loading a saved search 234
- node search criteria 356
- policy test result search criteria 560
- policy test search criteria 532
- report search criteria 588
- rule search criteria 435
- task search criteria 511
- TE log message search criteria 580
- TLC log message search criteria 581
- waiver search criteria 568
- wildcards 233

searching

- for actions 480
- for element versions 364
- for elements 361
- for nodes 355
- for policy test results 559
- for policy tests 532
- for reports 587
- for rules 434
- for tasks 510
- for TE log messages 579
- for TLC log messages 581
- for waivers 567

selection methods

- about 73
- and promotion 47
- by-match method 73
- by-reference method 76

set custom value actions

- about 124
- creating 499
- defined 118

settings

- Administration settings 194
- Custom Property settings 195
- exporting 277
- import from XML files 225
- importing 276

- Monitoring Preferences 195
- System settings 194
- User settings 194
- Settings Manager
 - about 194
 - categories 194
 - defined 28
- severity indicators 202
 - defined 114
- severity levels
 - about 112
 - and policy tests 132
 - example 115
 - license requirements 112
 - user permissions for 615
- severity override actions
 - creating 499
 - defined 118
- severity ranges
 - about 114
 - default severity ranges 114
 - defined 114
 - example 115
 - working with 270
- smart node groups
 - defined 57
 - enabling 57
- SNMP actions
 - about 124
 - creating 500
 - defined 118
- software-installation packages
 - and promotion 48
 - how package data is used in Tripwire Enterprise 49
- specifiers
 - adding to a Windows RSoP rule 472
 - changing in a Windows RSoP rule 472
 - deleting from a Windows RSoP rule 472

SSL

- configuring SSL for database and directory server nodes 419
- keystore changes in TE 8.4.1 421

Standard Node View

- defined 313

start points

- about 461
- adding to a rule 462
- and database metadata rules 89
- and directory rules 96
- and file system rules 83
- and Windows registry rules 87
- changing 466
- creating with the Adjust Rule feature 398
- deleting 466
- editing with the Adjust Rule feature 399
- monitored objects identified by 461

status bar

- about 26

status check rules

- creating 452
- defined 80

stop points

- about 461
- adding to a rule 467
- and database metadata rules 89
- and directory rules 96
- and file system rules 83
- and Windows registry rules 87
- changing 469
- creating with the Adjust Rule feature 400
- deleting 469
- deleting with the Adjust Rule feature 401
- monitored objects identified by 461

stopping

- baseline rule tasks and check rule tasks manually 523

support data

- creating diagnostic files for Tripwire Support 278

- syslog actions
 - creating 500
 - defined 118
- System Access Control Reports
 - defined 177
- System Log Reports
 - defined 177
- system preferences
 - changing 266
 - descriptions 266
- system reports
 - defined 184
- System settings
 - about 194
- system tag sets
 - defined 352

T

- tabs
 - about 24
 - in action group property dialogs 487
 - in common action property dialogs 482
 - in conditional action property dialogs 484
 - in dashboard property dialogs 591
 - in element property dialogs 327
 - in element version property dialogs 328
 - in network-device action property dialogs 482
 - in node group property dialogs 325
 - in node property dialogs 321
 - in Policy Result Properties dialogs 555
 - in policy test group property dialogs 538
 - in policy test property dialogs 537
 - in report group property dialogs 590
 - in report property dialogs 589
 - in rule group property dialogs 440
 - in rule property dialogs 438
 - in task group property dialogs 514

- in task property dialogs 513
 - in TE log message dialogs 577
 - in TE policy property dialogs 535
- tag actions
 - defined 118
- tag sets
 - defined 352
 - working with 352
- tagging profiles
 - defined 354
 - working with 354
- tags
 - applying manually 350
 - applying or unapplying with an action 118
 - best practices 342
 - defined 352
 - overview 339
 - using the Asset View tab 346
 - working with 352
- target nodes
 - and the by-reference selection method 76
- task groups
 - changing properties 514
 - creating 519
 - deleting 521
 - exporting 527
 - importing 528
 - linking 525
 - moving 525
 - running manually 523
 - tabs in task group property dialogs 514
 - unlinking 526
 - viewing 508
- Task Manager
 - about 127
 - columns in Task Manager table 509
 - defined 27

Task Reports

defined 177

tasks

about 127

about baseline rule tasks 128

about check rule tasks 129

about the Archive Log Messages Task 170

about the Compact Element Versions Task 130

changing properties 512

creating baseline rule tasks 517

creating check rule tasks 518

creating current baselines for a check rule task 522

creating report tasks 519

deleting 521

disabling 524

duplicating 520

enabling 523

exporting 527

how a report task works 186

import from XML files 230

importing 528

linking 525

moving 525

running manually 523

search criteria 511

searching for 510

stopping manually 523

tabs in task property dialogs 513

types of tasks 127

unlinking 526

user permissions for 615

viewing 508

TE Announcements widget

defined 190

TE Developer Blog widget

defined 190

TE Forums widget

defined 190

TE Knowledge Base widget

defined 190

TE log messages

categories 167

defined 166

deleting 583

search criteria 580

searching for 579

tabs in TE log message dialogs 577

viewing 576

TE policies

about 131

about pre-configured TE policies from Tripwire 219

about scopes 133

adding waivers for a single node 336

and compliance statistics 553

and policy scores 138

and waivers 138

and weights 138

changing properties of 534

changing scoring thresholds for 556

creating 543

creating scoring thresholds for 555

defined 131

deleting scoring thresholds for 556

example 148

import from XML files 229

properties defining the scope of 133

tabs in TE policy property dialogs 535

viewing in the Compliance tab 550

viewing in the Tests tab 530

templates

and equivalent Tripwire Enterprise objects 62

test result indicators

defined 144

Test Result Summary Reports

defined 177

- Test Results By Node Reports
 - defined 177
- test/node pairs
 - and waivers 138
 - defined 138
- text-field qualifiers
 - about 233
- text variables
 - defined 196
- TID
 - see Tracking Identifiers 223
- Time to Reconcile Reports
 - defined 177
- timestamps
 - import timestamps defined 222
 - modification timestamps defined 222
- TLC log messages
 - and log transfer rules 98
 - defined 166
 - search criteria 581
 - searching for 581
- Tracking Identifiers
 - about 223
- tree pane
 - about 26
- Tripwire Enterprise Agent
 - assigning to a node 411
 - changing configuration properties of 417
 - creating a node with 54
 - defined 54
 - differences with Axon Agent 55
 - downloading Agent log files 423
 - restarting 412
 - upgrading 279, 413
- Tripwire Enterprise Console
 - configuring 274
 - logging out 25

- Tripwire Enterprise Console database
 - recalculating database index statistics 269
- Tripwire Enterprise objects
 - defined 27
 - for clusters 62
 - for datacenters 62
 - for datastores 62
 - for distributed virtual port groups 62
 - for distributed virtual switches 62
 - for folders 62
 - for resource pools 62
 - for VI host machines 62
 - for virtual applications 62
 - for virtual machine templates 62
 - for virtual machines 62
 - for virtual networks 62
 - for virtual switches 62
 - links between 213
 - node, element, and element version diagram 36
 - types 27
 - used in a version check 44
- Tripwire Enterprise User Guide
 - chapters in 19
- Tripwire Support
 - creating diagnostic files for 278

U

- unauthorized composite change
 - defined 174
- unauthorized composite changes
 - example in a Composite Changes Report 180
- Unchanged Elements Reports
 - defined 178
- unique identifiers
 - defined 49
- UNIX file system rules
 - defined 81

Unlinked Group

- clearing 127
- defined 30

unlinking

- about 214
- actions and action groups 504
- dashboards 598
- example 215
- nodes and node groups 381
- Policy Manager objects 572
- reports and report groups 598
- rules and rule groups 474
- tasks and task groups 526

Unmonitored Nodes Reports

- defined 178

upgrading

- Agent software 279, 413

user accounts

- about 206
- changing assigned user role 287
- changing list of accounts assigned to a home page 243
- changing passwords of 286
- changing properties of 286
- changing user groups 287
- creating 285
- default administrator account 206
- defined 206
- deleting 288
- unlocking 288
- user permissions for 616

user differences

- changing 265
- descriptions 265

user groups

- about 206
- associating user accounts with 287
- defined 206
- working with 289

- user permissions
 - about 204
 - about the Manage System Reports permission 185
 - common types 205
 - defined 204, 611
 - for actions 611
 - for criteria sets 611
 - for custom nodes 612
 - for e-mail servers 612
 - for elements 612
 - for license files 612
 - for log messages 613
 - for nodes 613
 - for policies 614
 - for post-remediation service commands 614
 - for remediation work orders 614
 - for reports 614
 - for rules 615
 - for severity levels 615
 - for tasks 615
 - for user accounts 616
 - for variables 616
 - miscellaneous 613
- user preferences
 - changing 262
 - descriptions 262
- user reports
 - defined 184
- user roles
 - about 204
 - and access controls 208
 - changing for a user account 287
 - customized 204
 - default user roles 205
 - defined 204
 - working with 293
- User Roles All Object Types Reports
 - defined 178

User Roles Reports

defined 178

User settings

about 194

users

about licenses 202

Users tab

defined 240

V

variables

about 196

user permissions for 616

working with global variables 271

version checking

about 44, 55

about run rule actions 123

disabling temporarily 387

monitored objects 386

monitored systems 385

overview 37

Tripwire Enterprise objects used 44

version custom properties

defined 197

VI host machines

and equivalent Tripwire Enterprise objects 62

defined 59

VI hypervisor nodes

defined 53

VI hypervisor rules

creating 453

defined 82

VI management nodes

creating 375

defined 53

VI node change alert generators

defined 193

VI node discovery

about 59

and VMware virtual infrastructures 60

defined 56

VI nodes

configuring SSL 419

creating 375

defined 53

how to create 56

import from XML files 228

types of elements 39

VI rules

types 82

viewing

actions and action groups 478

changed nodes 320

changes with the Difference Viewer 46

home pages and widgets 240

nodes, node groups, and elements 313

policy test results in the Compliance tab 554

reports, report groups, and dashboards 585

rules and rule groups 432

tasks and task groups 508

TE log messages 576

TE policies, policy tests, and policy test groups in the Compliance tab 550

TE policies, policy tests, and policy test groups in the Tests tab 530

the properties of a log message 577

virtual applications

and equivalent Tripwire Enterprise objects 62

virtual infrastructure

see VI 53, 59

virtual machine configuration rules

creating 453

defined 82

virtual machine nodes

defined 53

- virtual machine template nodes
 - defined 53
- virtual machines
 - and equivalent Tripwire Enterprise objects 62
- virtual switch configuration rules
 - creating 454
 - defined 82
- virtual switch nodes
 - defined 53
- virtual switches
 - and equivalent Tripwire Enterprise objects 62
- virtual systems
 - defined 59
- virtualization
 - defined 59
- VMs
 - components of 59
 - defined 59
- VMware ESXi rules
 - see VI hypervisor rules 82
- VMware ESXi Service Console rules
 - see command output hypervisor rules (COHRs) 82
- VMware vCenter nodes
 - defined 60
 - example in Node Manager 61
- VMware virtual infrastructures
 - and VI node discovery 60
- VMware VM rules
 - see virtual machine configuration rules 82
- VMware vNetwork Distributed Switch rules
 - see virtual switch configuration rules 82
- VMware vSwitch rules
 - see virtual switch configuration rules 82
- vSphere
 - defined 60

vSwitch
see virtual switch 53

W

waiver expiration alert generators
defined 193

waivers
adding for a single node 336
changing 566
closing 569
creating 564
defined 138
deleting 569
purging 145
search criteria 568
searching for 567

weighted scores
defined 139

weights
defined 138

whitelists
about 424
using to manage database queries 429
using to restrict commands on Agents 424

widgets
about 189
adding to a home page 245
changing layout in a home page 242
defined 189
deleting 254
types of 190
viewing 240

Widgets tab
defined 240

wildcards
using in searches 233

Windows ACL policy tests

- defined 132

Windows file system rules

- defined 81

Windows registry

- about 85

- attributes of 304

- common root keys 85

- data types 306

- example of a Windows Registry Browser 86

Windows registry keys

- defined 85

Windows registry rules

- about 85-86

- changing start points 466

- changing stop points 469

- components 87

- creating 457

- creating criteria sets for 304

- creating start points 462

- creating stop points 467

- defined 81

- deleting start points 466

- deleting stop points 469

- naming requirements for registry keys and entries 87

Windows RSoP rules

- about 88

- adding a specifier to 472

- attributes for 307

- changing a specifier in 472

- creating 458

- creating criteria sets for 306

- defined 81

- deleting a specifier from 472

work order

- see remediation work order 255

working

- with archived report output 608

X

XML files

about import of 222

defined 217

how pre-configured XML files changed in Tripwire Enterprise 7.1 221

order of import 219