

HP Server Automation

for the HP-UX, IBM AIX, Red Hat Enterprise Linux, Solaris, SUSE Linux Enterprise Server, VMware, and Windows® operating systems

Software Version: 9.10

User Guide: Audit & Compliance

Document Release Date: June 2011

Software Release Date: June 2011



Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

© Copyright 2001-2011 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Intel® and Itanium® are trademarks of Intel Corporation in the U.S. and other countries.

Microsoft®, Windows®, Windows® XP are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<http://h20230.www2.hp.com/selfsolve/manuals>

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at:

www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

1 Overview of Audit & Remediation	11
Terminology	12
Server Configurations	14
Enforce Security Standards	14
Capture & Replicate Golden Servers	14
2 Audits, Audit Policies, & Audit Results	15
Audits	15
Audit Policies	15
Snapshots	16
Compliance & Remediation	16
Audit Management	16
Audit Comparison Types	16
Audit Process	17
Audit Elements	18
Creating an Audit	19
Creating an Audit from a Server	20
Creating an Audit from a Group of Servers	20
Creating an Audit from the SA Library	20
Creating an Audit from a Snapshot	21
Creating an Audit from an Audit Policy	21
Running an Audit	21
From the SA Library	21
From All Managed Servers	22
From Audit Results	23
Scheduling an Audit	24
Scheduling a Recurring Audit	24
Editing an Audit Schedule	25
Viewing a Completed Audit Job	25
Exporting/Importing an Audit	26
Viewing Audit and Snapshot Usage	26
From All Managed Servers	26
From the Device Explorer	26
Audit Configuration	27
Audit & Snapshot Sources	28
Source: Server	29
Source: Snapshot	30
Source: Snapshot Specification	30
Source: Rules	31
Server Objects	31

Audit & Remediation Rules	33
Configuration Rules	33
Audit and Snapshot Rules	35
Configuring Application Configuration Rule	36
Application Configuration Audit Rule Color Scheme	40
Configuring COM+ Rule	40
Configuring Custom Scripts Rule	41
Custom Scripts Example	43
Configuring the Discovered Software Rule	44
Configuring the File Rule	45
Common Scope Cases with Diagrams	46
Ways to Add a Rule to an Audit	49
Comparing Files in Audits with Configuration Templates	51
Configuring Hardware Rule	52
Configuring IIS Metabase Rule	53
Configuring IIS Rule	54
Configuring IIS 7.0 Rule	55
Configuring Local Security Settings Rule	57
Configuring Registered Software Rule	58
Configuring Storage Rule	59
Configuring Windows .NET Framework Configurations Rule	60
Configuring Windows Registry Rule	61
Configuring Windows Services Rule	62
Configuring Windows/UNIX Users and Groups Rule	63
Configuring Compliance Checks	64
Renaming Compliance Checks	65
Searching for Compliance Checks from the Audit/Snapshot Specification Window	66
Compliance Checks	66
Editing Compliance Check Properties	67
Creating Custom Compliance Check Categories	68
Restoring Compliance Checks to Defaults	68
Showing Deprecated Checks	69
Setting Inclusions & Exclusions for Checks	69
File Inclusion and Exclusion Rules	69
Inclusion and Exclusion Rule Types	70
Example: Including all .txt Files in a Snapshot or Audit	71
Example: Including Only File a in a Snapshot or Audit	72
Example: Including last temp.txt file and exclude all else	72
File Rule Overlap	73
Example A	73
Example B	73
Example C	74
Parameterizing Filenames for SA/Custom Attributes	74
Examples of Parameterizing Filenames	75
Environment Variables in Pathnames	75
Audit Rule Exceptions	76
Rules That Cannot Have Exceptions	76

Considerations When Applying Exceptions to Device Groups	76
Adding a Rule Exception to an Audit	77
Editing or Deleting a Rule Exception	77
Audit Policy Management	78
Linking & Importing an Audit Policy	78
Linking an Audit Policy	78
Importing an Audit Policy	79
Rule Overlap with Multiple Linked Audit Policies	79
Creating an Audit Policy	79
Saving an Audit as an Audit Policy	80
Ways to Link & Import Audit Policies	81
Linking an Audit Policy to an Audit or a Snapshot Specification	81
Linking Audit Policies to a Master Audit Policy	82
Importing Audit Policy Rules	83
Saving an Audit or a Snapshot Specification as an Audit Policy	83
Locating an Audit Policy in the Folder Library	84
Exporting an Audit Policy to HTML or CSV	84
Audit Results	84
Remediating Rules with Inherited Values	85
Viewing Audit Results	86
Audit Results Window	86
Audit Results Summary	87
Remediation Methods: All, By Server, or By Rules	88
Remediating Comparison-Based Audit Results	91
Viewing Value-Based Audit Results–Audit Rule Remediation	92
Viewing and Remediating Audit Results Differences	92
Viewing and Remediating File Differences	93
Viewing and Remediating Object Differences	93
Viewing Audit Results with Exceptions	95
Searching for an Audit	95
Deleting an Audit	96
Deleting Audit Results	96
Archiving Audit Results	97
3 Snapshots, Snapshot Specifications, & Snapshot Jobs	99
Snapshots	99
The Snapshot Process	99
Snapshots & Snapshot Specifications	100
Snapshot Used in an Audit	101
Snapshot Specification Used in an Audit	101
Snapshot Specification Elements	101
Viewing Snapshots	103
In the SA Library	103
In the Device Explorer	103
Searching for Snapshots	103
Viewing Snapshot Results	104
Archiving a Snapshot	106

Deleting a Snapshot	106
Exporting/Importing a Snapshot	106
Copying Objects	107
From a Snapshot to a Server	107
From a Snapshot to a Server	107
Snapshot Specifications	108
Snapshot Specifications & Audit Policies	108
Creating a Snapshot Specification	108
From a Server	109
From the SA Library	109
Deleting a Snapshot Specification	109
Configuring a Snapshot Specification	109
Configuring Snapshot Specification Rules	111
Saving a Snapshot Specification as an Audit Policy	111
Running a Snapshot Specification	112
Snapshot Jobs	113
Scheduling a Recurring Snapshot Job	113
Viewing and Editing a Snapshot Job Schedule	114
Deleting a Snapshot Job Schedule	115
4 Compliance in the SA Client	117
Overview	117
Terminology	119
Compliance Categories	120
Compliance Statuses	120
Compliance Status Definitions	122
Compliance Status Thresholds—Policy, Server, & Server Group	123
Compliance Status Thresholds—Device Group	123
Changing Device Group Compliance Settings	124
The Compliance View	125
Viewing Compliance for a Server	125
Compliance Summary Pie Chart and Details	126
Viewing Compliance for Multiple Servers	128
Device Group Compliance: Status Rollup	128
Device Group Compliance: Aggregate Rollup	129
Viewing Group Compliance	130
Adding and Removing Compliance View Columns	131
Sorting the Compliance Category Display	131
Filtering By Compliance Status	132
Refreshing Compliance Information	132
Setting Automatic Compliance Check Frequency	133
Exporting Compliance View Information	133
Compliance View Remediation	134
Compliance View Remediate—Server Group	134
Compliance View Remediate—Server	135
Compliance Scans	136
Patch Compliance	137

Patch Compliance Status Criteria	137
Remediating Patch Compliance for Servers	138
Remediating Patch Compliance for Groups	139
Audit Compliance	140
Audit Compliance Status Criteria	140
Audit Compliance Remediation	141
Remediating Audits Attached to Servers	141
Audit Policy Compliance	142
Software Compliance	143
Software Compliance Status Criteria	143
Software Compliance Remediation	144
Remediating Software Compliance for Servers	145
Remediating Software Compliance for Groups	146
Configuration Compliance	147
Configuration Compliance Status Criteria	148
Remediating Configuration Compliance—Servers and Groups	149
Index	151

1 Overview of Audit & Remediation

In Server Automation (SA), audit and remediation allows you to identify which objects you want checked, where you want to check for them, and when you want to check them in your IT environment.

- *Audit policies* define what to check—such as files, directories, configuration values, and so on.
- *Audits* define where to check—such as servers and server groups.
- *Audit schedules* define when to check—such as one time or as a recurring job.

These capabilities help you understand how to make your managed server environment compliant and how to keep your servers compliant. In SA, you can define server configuration policies to ensure that servers in your facilities meet policy standards. When servers are found to be *out of compliance*—not configured the way you want them to be—you can remediate them to comply with your organization’s standards.

Using the SA Client, you can audit server configuration values based on a live server or a server snapshot, based on your own custom values, or based on pre-configured audit policies. You can also take server configuration snapshots to capture the current state of a system, so that you can compare other servers against a known baseline.

Audit policies allow you to define company or industry-wide compliance standards, which can then be used inside of audits, snapshot specifications, and other audit policies. Referencing audit policies in your audits or snapshot specifications helps verify that you are up to date with the latest compliance definitions in your organization.



Best Practice: If you have a content subscription to BSA Essentials Subscription Services, you can be kept up to date on the latest industry compliance standard, based on the needs of your data center. For example, Subscription Services give you access to regularly updated security best practices, such as the Center for Internet Security (CIS), Payment Card Industry (PCI), and so on. It also enables access to additional free non-subscription content such as Microsoft Patch Supplement for Server Automation. BSA Essentials Subscription Services enables you to access the most current regulatory compliance policies, such as Federal Information Security Management Act (FISMA, Sarbanes-Oxley, and daily vulnerability alerts. You can also join the content developer communities on the HP Live Network (HPLN) portal to share and access custom-created audit policies and rules. For information about subscribing to BSA Essentials Subscription Services, contact your sales representative.



See the *Server Automation Compatibility Matrix* for detailed information about supported operating systems for audit and remediation. SA does not support auditing or creating snapshots of VMware ESXi servers.

Terminology

The following list defines key terms and concepts used in Server Automation audit and remediation:

- **Archived Audit Result/Snapshot:** Archiving audit results and snapshots allows you to move them from the audit result or snapshot list and keep them available for historical purposes.
- **Audit:** A set of rules (which may contain individual *checks*) that expresses the desired state of a managed server's configuration objects, such as a server's file system directory structure or files, a server's Windows Registry, application configuration, and so on. An audit also contains *sources* (servers, snapshots, or snapshot specifications), *targets* (servers or snapshots), *rule exceptions*, and a schedule.

An audit's rules can be linked to an audit policy—which means the rules of the audit policy are substituted for those in the audit. An audit can be run to baseline compare server configuration object values against a *golden server*, a server snapshot, or user-defined values, to determine how values differ. When an audit reports a difference between servers or user-entered values, you can install software and server objects to remediate the differences so that servers conform to your audit rules.

- **Audit Job:** The process that occurs when you run an audit. An audit job can be run immediately one time or on a recurring basis by scheduling the job. When an audit job is finished, it produces an audit result that reports the differences.
- **Audit Rule Type:** An audit can contain the following types of rules:
 - **Comparison:** A rule that compares a server's or snapshot's configurations of a server with other managed servers or snapshots.
 - **Value-based (user-defined):** A rule that compares one or more set of user-defined values. This type of audit includes an audit that links to an audit policy.
 - **Non-existence:** A rule that checks for the non-existence of an object to determine if it exists on the target server. If the object exists on the target server, the user or group rule is *out of compliance*.
- **Audit Policy:** A collection of rules that defines a desired configuration for a server. A policy can be used by an audit in the following ways:
 - **Link:** A linked policy maintains a persistent connection between the audit and the policy. This means that the rules in the audit are exactly those of the audit policy and if any updates are made to the policy, the latest changes are also reflected in the audit to which the policy is linked. When an audit policy is linked to an audit or snapshot specification, the rules are shown inside the audit or snapshot specification as read-only. The rules inside the audit policy remain editable.
 - **Import (replace, non-linked):** When you import a policy into an audit, the connection between the audit and the audit policy is no longer maintained. You can make changes to the audit without affecting the policy. Conversely, any changes or updates made to the policy will not be reflected in the audit.
 - **Import (merge):** When an audit policy is imported and merged into an audit, the audit policy's rules are added to the rules already present in the audit. No persistent link between the audit and the audit policy is maintained. During the merge, if rules are found to conflict, the newly imported rules from the audit policy will replace the rules in the audit policy.
- **Audit Result:** The results of running an audit. This information shows how a target server or a group of servers' configuration object values match or do not match the values defined in the audit.
- **Exception:** A server and specific rules that has been excepted or disabled, so that when the audit is run, the rule exception is not checked on the selected server. This server is excluded when determining audit compliance.

- **Compliance:** The degree to which a server's configuration conforms to a check or test established in a collection of rules defined in an audit, a snapshot specification, or an audit policy. Compliance in audit and remediation is defined by the audit's or snapshot's rules that specify the values expected of the target servers. If the values on the target server are different than specified in the audit's rules, the server is considered Non-Compliant.
- **Policy Setter:** A user who is responsible for defining server configuration compliance standards (the way a server should be configured) and audit policies in your organization.
- **Rule:** A *check* on a particular server configuration object that includes a desired value and an optional remediation value.

There are two types of rules:

- *server-based rule:* derived directly from a source server
- *user-defined rule:* created by a user

If you are subscribed to BSA Essentials Subscription Services, you can access predefined rules that define a wide range of industry compliance standards, such as the latest patch supplement for Microsoft Windows, current regulatory compliance policies (FISMA, Sarbanes-Oxley), user-created rules from the EP developer community, daily vulnerability content updates, and so on.

- **Server Object:** An object from a server to which an audit or snapshot specification rule can be applied. This can be a value, such as minimum password length, or an object, such as a file or directory, registry entry, Windows Services hardware configuration, and so on.
- **Snapshot:** A representation of the configuration state of a managed server, where the information was captured on a certain date, at a certain time of day. A snapshot is the result of a snapshot specification job that has been run.
- **Snapshot Specification:** An object window that allows you to define and create a snapshot. In other words, you can define the rules and servers to take a snapshot of.
- **Snapshot Specification Job:** The process that occurs when you run a snapshot specification. A snapshot job can be run once or on a recurring basis, by scheduling the job. When a snapshot specification job is completed, it produces a snapshot.
- **Target:** The server or servers that you run an audit against or take a snapshot of. The target for an audit can be a server, multiple servers, a group of servers, or a snapshot. The target for a snapshot can also be other servers.

Server Configurations

The following best practices and examples illustrate ways that SA helps you manage server configurations in your facility:

- [Enforce Security Standards](#)
- [Capture & Replicate Golden Servers](#)

Enforce Security Standards

Your IT organization typically has security policies that you must enforce. These policies verify whether your servers are correctly configured and are protected from security attacks. Your policy setter can create an audit policy to enforce these security standards. A pre-defined audit policy can be linked to multiple audits or snapshot specifications. Administrators who manage live servers can reference the correct audit policy to ensure their servers are being audited correctly.

Example: Your company has Solaris 10 servers that must be kept up to date with the most recent commonly known security vulnerabilities that are specified by Common Vulnerabilities and Exposures (CVE). Your company wants to make sure your servers are not vulnerable to a known threat to Solaris 10, such as CVE-2009-0168 (CVSS 4.9), which checks for an unspecified vulnerability in PPD File Manager (ppdmgr) in Sun Solaris 10 and OpenSolaris snv_61 through snv_106. By subscribing to the BSA Essentials Subscription Services, you have access to an online collection of compliances checks. You can use these checks to audit your Solaris 10 servers and verify whether they are not at risk to this security vulnerability. Your system administrator, who is responsible for defining compliance standards in your organization, can create an audit policy that contains the CVE-2009-0168 compliance check.



Best Practice: System administrators who are responsible for managing Solaris servers can create audits for their servers and then link their audit's rules to this audit policy. When an audit links to an audit policy, any changes made to the policy are immediately reflected in the audit. Therefore, the person who runs the audits on the servers knows that the audit rules are always up to date. For example, if a new CVE update came out for Solaris 10 servers, the policy setter would update the policy and all audits that link to that policy will have the latest compliance checks. Knowing that her audit will always contain the latest vulnerabilities checks, the policy setter can schedule the audit to run regularly to check all of the Solaris 10 servers that she manages. If the audit results show that any of the target servers do not contain the new CVE security check, those servers can be remediated to fix the problem.

Capture & Replicate Golden Servers

Sometimes a server becomes configured in such a way that it represents the ideal state of server configuration for a certain purpose in your facility. For example, if you want to set up a collection of servers that handle Web traffic, you might configure a single server that represents an ideal configuration—a *golden server* configuration—for a group of Web servers. After you configure this golden server, you can duplicate its configuration across a group of SA managed servers.

Example: You have a Red Hat Linux server that has a unique configuration of Apache Web Servers, and you want to duplicate this exact configuration across several other managed servers. Using audit and remediation, you can create an audit that uses the golden server as the source configuration. In the audit, you select those configurations to use to audit other servers, such as an application policy and specific application configuration rules. Select those servers as the target of the audit to be configured like the golden server. After you run the audit, you can remediate any target server's configurations that do not match the golden server. You can schedule the audit to run on a regular basis. If any server becomes non-compliant, you remediate it when it deviates from the golden server.

2 Audits, Audit Policies, & Audit Results

Audits

An *audit* defines a set of rules or configuration values that determine whether the configuration of a managed server or group of managed servers match your organization's compliance standards. Audit rules can be configured in an ad-hoc manner or, more effectively, reference a predefined audit policy that specifically defines the required configuration for a managed server in Server Automation.

An audit can:

- Compare a server's configuration against the rules defined in the audit policy.
- Check that a configuration value meets the criteria specified in the audit rule.
- Check to ensure that a specific value does or does not exist.

Some audit rules also allow you to run scripts that capture more detailed configuration information.



Best Practice: You can define the audit policy to:

- Identify whether an IIS Metabase value exists, especially when you do not want it to.
- Make sure a specific Linux service is set to always be running, especially if it's a critical service that must always be running for security reasons.
- Determine if a certain file system directory does not exceed a certain size limit.
- Make sure that the maximum length setting for user passwords has not been exceeded.

You can define what the audit should look for, what values you expect to find on the server, and what replacement values to use that will fix them when differences are found.

After it is configured, an audit can be run once, scheduled for a future run, or be scheduled to run a regular basis. After an audit is run, its results indicate the extent to which those servers meet the definitions set in the audit rules. In cases where discrepancies are found, you can remediate those servers to bring them into compliance.

Audit Policies

An *audit policy* is a collection of reusable rules that define the desired state of server configuration, based on industry standards and the compliance goals set by your organization. An audit policy can be linked to audits, snapshot specifications, and other audit policies. When changes are made to an audit policy, all references to that audit policy are also updated.

An audit policy is typically created by a policy setter who understands the compliance standards that a company requires its servers to meet for a specific configuration domain and operating system. Administrators who manage servers can use predefined audit policies by linking them to their audits or snapshot specifications. If any changes are made to an audit policy, the audit that links to it also contains the updated rules. Administrators who audit SA managed servers can be sure their audits always reflect the latest policy standards in their organization.

Snapshots

A *snapshot* is a representation of the configuration state of a managed server, where the information was captured on a certain date, at a certain time of day. A snapshot is useful for capturing the configuration of a *golden server* that you would like to baseline compare against other servers in your facility. You can use the snapshot as the source of an audit. If a server does not match the configuration captured in the snapshot, you can remediate those servers after the audit has run.

Compliance & Remediation

The Compliance view in the SA Client allows you to view the overall compliance levels for SA managed servers in your facility. The Compliance view is also known as the *compliance dashboard*. From the compliance dashboard, you can identify and then, subsequently, remediate compliance problems.

Audit Management

An *audit* is a collection of rules that enable you to define what should be or what should not be in a server's configuration. An audit contains rules, a source, target servers, and a schedule that defines when and how often the audit will run.

Audit rules allow you to define and check the state of various configurations or objects and files on a managed server, such as the state of server's file system, registry settings, installed and registered software (patches and packages), events, software, application configurations, operating system settings, and so on.

If the configuration or object on the target server is different than the state you defined in the audit rules, the rule is considered Non-Compliant. When you view an audit's results, you can remediate the object configuration to make sure the target server's configuration is in compliance with the desired configuration.

You can audit server configuration values for a single server, multiple servers, or another server snapshot. You can also schedule audits to run immediately or on a recurring schedule, and send email notifications when the audit has completed.

Audit Comparison Types

In general, an audit can contain the following types of comparisons, based on the source of the audit:

- **Comparison:** An audit based on configuration values from a source server or source snapshot specified at the time the audit is created. The source server or server snapshot is also known as a *golden server*. For example, you might want to compare file directories or file contents, registry structures, IIS Metabase entries, or user group settings among managed servers. Using a snapshot as the source of an audit, you can compare the snapshot with other servers in your facility.

Comparison audits can perform the following types of comparisons:

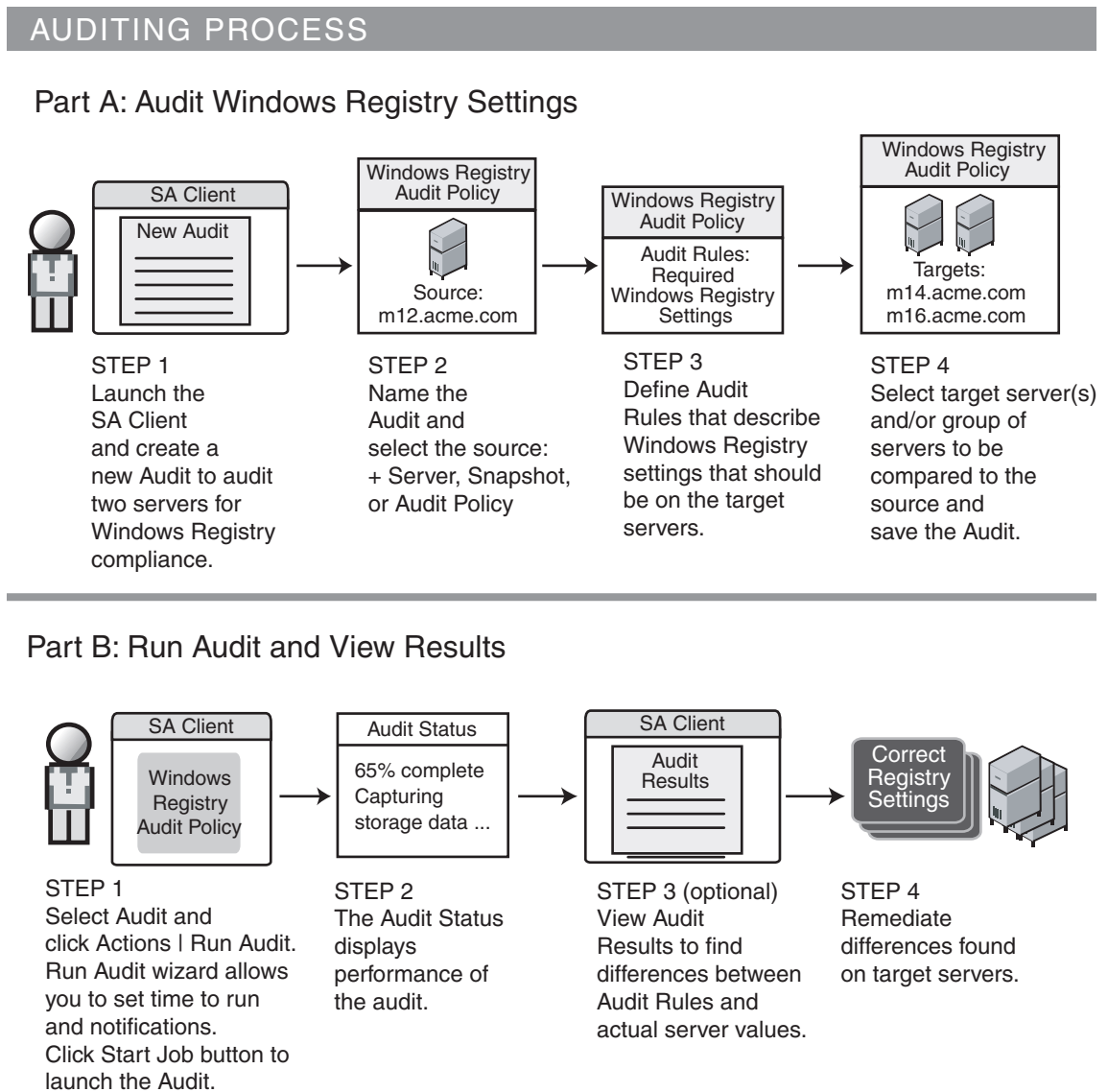
- **Property:** Checks the property of a selected object or object configuration. For example, you could check the release version of a patch on a target server or group of servers, to make sure it matches what you expect to be installed on the targets. You can select this version number based on a source server or snapshot or add your own value.
- **Equivalence:** Checks to determine that a target server configuration is the same between the source server or snapshot of the audit. For example, you could check to see if the target of the audit has the same user group as a group you selected from a source server.

- **Non-existence:** Checks the target server to determine the non-existence of a server object or configuration. For example, you could check a server to make sure it does not contain a specific COM+ object.
- **Value-based (user-defined):** An audit based on custom, user-defined values for each server object (file system, windows services, IIS Metabase, users and groups, and so on). These values can be derived from a source server, SA attributes, or custom attributes. This type of audit includes those based on an audit policy. In an audit policy, a policy setter pre-defines values for each configuration object, based on company or industry compliance standards.

Audit Process

The following diagram illustrates a basic example of creating and running an audit on Windows servers.

Figure 1 The Auditing Process



Audit Elements

An audit consists of the following elements:

- **Properties:** The name and description of the audit.
- **Source:** The source of an audit can be a server, a snapshot, or no source at all. However, some rules require a source.
 - Choosing a server as the source for an audit allows you to select server objects from that server as the basis of your audit.
 - Choosing a snapshot as the source of an audit allows you to use the configuration values of the snapshot.
 - Choosing a snapshot specification as the source allows you to audit a server against itself over time. For example, if you took a snapshot of a server, then used that snapshot specification as the source of the audit, every time you run the audit, you can compare the original state of the server against the server's actual configuration over time, using a recurring audit schedule. If you choose no source, you can only define your own custom values for the audit or snapshot.
- **Rules:** A check on a particular server object with a desired value and an optional remediation value. For example, you might check to see if this server contains a specific Windows Service, and if found, determine if the service is turned off. See [Server Objects](#) on page 31.
- **Targets:** The servers that the audit will check for compliance. You can choose as many servers and groups of servers as needed for an audit or snapshot.

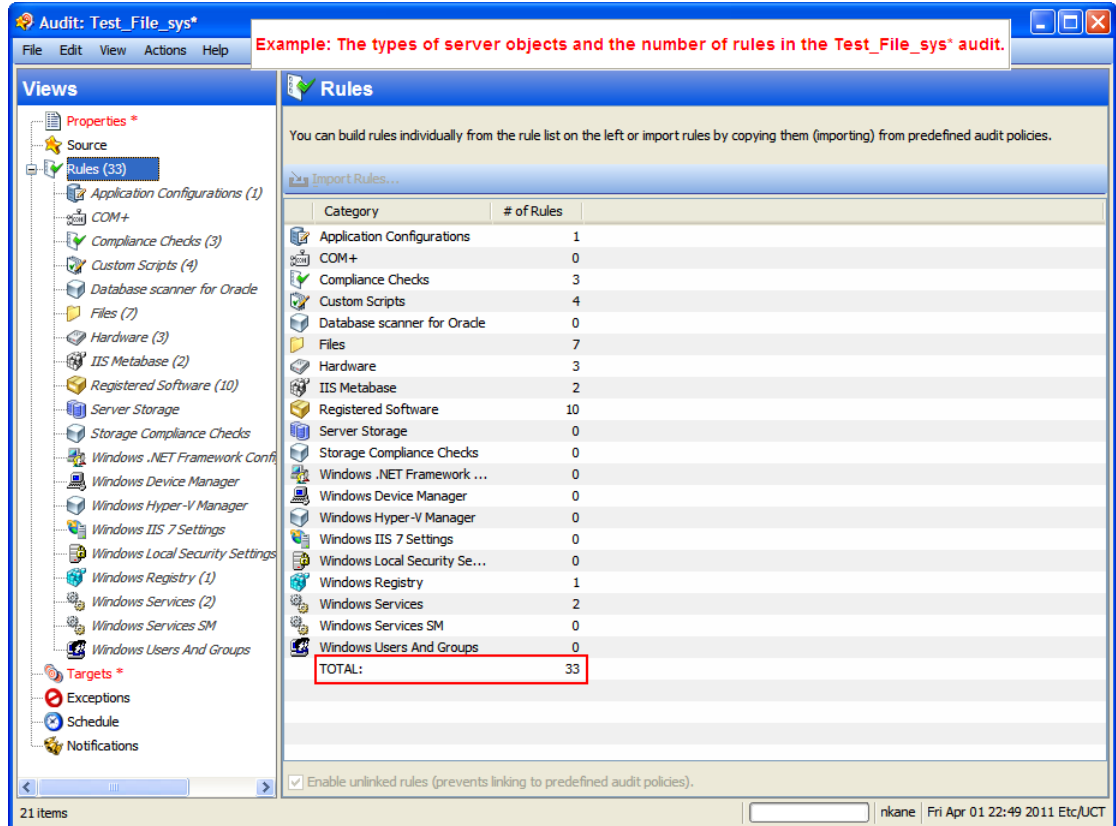


VMware ESXi servers cannot be the target of an audit or snapshot.

- **Exceptions:** Servers and specific rules that will not be checked for compliance when the audit is run.
- **Schedule:** You can run an audit on a one-time basis or on a recurring schedule. Audits that run on a recurring schedule appear as a single compliance column in the compliance dashboard.
- **Notifications:** You can send emails when the audit has finished running, and base the notification on the success, failure, or the completion of an audit job.

To configure an audit, select server configuration objects and then apply rules to those objects in order to define their desired configuration state. For example, [Figure 2](#) shows an audit that includes 33 defined rules. These rules are used to determine whether target server configurations match the rules in the audit.

Figure 2 Audit Browser Showing Objects in an Audit



Creating an Audit

In the SA Client, there are several ways to create an audit.

You can:

- Select a managed server as the source of the audit, to run the audit on a single server.
See [Creating an Audit from a Server](#) on page 20.
- Select a group of managed servers as the source of the audit, to run the audit on all servers in that group.
See [Creating an Audit from a Group of Servers](#) on page 20.
- Create a new audit from the SA Library.
See [Creating an Audit from the SA Library](#) on page 20.
- Create an audit that is based on the server configuration captured in a snapshot.
See [Creating an Audit from a Snapshot](#) on page 21.
- Create an audit that is based on the audit policy.
See [Creating an Audit from an Audit Policy](#) on page 21.

Creating an Audit from a Server

When you create a new audit from a managed server, the audit uses the selected server as the source of the audit. You can choose another server or snapshot for the audit source, or even not choose a source and define your own custom rules.



To audit a managed server, the server must be reachable and you must have access to the server.

To create an audit from a server:

- 1 In the navigation pane, select **Devices** ► **Servers** ► **All Managed Servers**.
- 2 Select a server.
- 3 From the **Actions** menu, select **Create** ► **Audit** to open the Audit window.
See [Audit Configuration](#) on page 27.

Creating an Audit from a Group of Servers

When you create an audit from a group of servers, the audit will evaluate all accessible servers in that group. However, the audit will evaluate only those servers in a group for which your user has access.

To audit a group of servers:

- 1 In the navigation pane, select **Devices** ► **Device Groups**.
- 2 In the content pane, select Public or private.
- 3 Select the server group that you want to audit.
- 4 In the content pane, select a server group.
- 5 From the **Actions** menu, select **Create** ► **Audit** to open the Audit window.

When you perform an audit by selecting a group of servers, the group of servers becomes the target. If the audit rule requires a source, you must specify one. See [Audit Configuration](#) on page 27.

Creating an Audit from the SA Library

To create an audit from the SA Library:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Audit and Remediation**.
- 2 In the navigation pane, expand **Audits**.
- 3 Select an operating system: Windows or Unix.
- 4 From the **Actions** menu, select **New** to open the Audit window.
See [Audit Configuration](#) on page 27.

Creating an Audit from a Snapshot

You can select any snapshot in the SA Library and create an audit that is based on the server configuration captured in the snapshot. The snapshot will serve as the source of the audit; however, after you create the new audit from the snapshot, you can also select a different snapshot or server as the source.

To create an audit from a snapshot:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Audit and Remediation**.
- 2 In the navigation pane, expand **Snapshot Specifications**.
- 3 Select an operating system: Windows or Unix.
- 4 From the **Actions** menu, select **New** to open the Snapshot Specification window.
See [Audit Configuration](#) on page 27.

Creating an Audit from an Audit Policy

Audit policies are designed to be used by audits. When you create an audit from an audit policy, the audit policy is linked to the audit. When updates are made to that audit policy, all changes are reflected in the audit.

To create an audit from an audit policy:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Audit and Remediation**.
- 2 In the navigation pane, expand **Audit Policies**.
- 3 Select an operating system: Windows or Unix.
- 4 From the **Actions** menu, select **New** to open the Audit Policy window.
See [Audit Configuration](#) on page 27.

Running an Audit

Running an audit will execute the selected audit on the target server, servers, or snapshot of the audit. The audit evaluates the targets according to the rules defined in the audit. You can run an audit from the following locations in the SA Client:

- [From the SA Library](#) on page 21
- [From All Managed Servers](#) on page 22
- [From Audit Results](#) on page 23

From the SA Library

The SA Library contains all available audits that you can run, organized by operating system: Windows or Unix. The list of audits in the Library can be sorted by any of the columns, such as Name, Last Modified Date, and so on. The search tool can also be used to search the audit list by entering a name, ID, person who created the audit, and so on.

To run an audit from the SA Library:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Audit and Remediation**.
- 2 Select Audits, and then select either Windows or Unix.
- 3 Select the audit you want to run, right-click, and select **Run Audit**.

- 4 In the Run Audit window, step one shows you the name of the audit, the source server, or snapshot being used in the audit, the total number of rules defined in the audit, and all targets of the audit (servers and snapshot). Click **View Rule Details** to view the rule definitions.
(Optional) If you want to immediately run the audit, click **Start Job** at any point in the process.
- 5 Click **Next**.
- 6 In the Scheduling page, choose whether you want the audit to run immediately or at a later date and time. To run the audit at a later time, select **Run Task At** and then choose a day and time.
- 7 Click **Next**.
- 8 In the Notifications window, by default your user will have a notification email sent when the audit finishes, whether or not the audit job is successful. To add an email notifier, click **Add Notifier** and enter an email address.
- 9 *(Optional)* You can specify if you want the email to be sent on success or failure of the audit job.
- 10 *(Optional)* You can specify a Ticket Tracking ID in the Ticket ID field. The ticket ID field is only used when SA Professional Services has integrated SA with your change control systems. Otherwise, it should be left blank.
- 11 Click **Next**.
- 12 In the Job Status page, click **Start Job** to run the audit. When the audit has run, click **View Results** to view the results of the audit.

From All Managed Servers

You can run an audit from this location, if the server is being used as a target for an audit.

To run an audit from the All Managed Servers list:

- 1 In the navigation pane, select **Devices > Servers > All Managed Servers**.
- 2 Select a server. In the View drop-down list, select Audit and Remediation. The details pane displays below the content pane.
- 3 In the details pane Show drop-down list, select Audit - Server is Target.
- 4 Select an audit from the list, right-click, and select **Run Audit**.
- 5 In the Run Audit window, step one shows you the name of the audit, the source server, or snapshot being used in the audit, the total number of rules defined in the audit, and all targets of the audit (servers and snapshot). Click **View Rule Details** to view the rule definitions.
(Optional) If you want to immediately run the audit, click **Start Job** at any point in the process.
- 6 Click **Next**.
- 7 In the Scheduling page, choose whether you want the audit to run immediately or at a later date and time. To run the audit at a later time, select **Run Task At** and then choose a day and time.
- 8 Click **Next**.
- 9 In the Notifications window, by default your user will have a notification email sent when the audit finishes, whether or not the audit job is successful. To add an email notifier, click **Add Notifier** and enter an email address.
- 10 *(Optional)* You can specify if you want the email to be sent on success or failure of the audit job.

- 11 *(Optional)* You can specify a Ticket Tracking ID in the Ticket ID field. The ticket ID field is only used when SA Professional Services has integrated SA with your change control systems. Otherwise, it should be left blank.
- 12 Click **Next**.
- 13 In the Job Status page, click **Start Job** to run the audit. When the audit has run, click **View Results** to view the results of the audit.

From Audit Results

You can rerun an audit from an audit results if you would like to run the same audit another time.

Note that when you are viewing the results of an Audit or a Snapshot and re-run the audit from those results, the rules in the original audit may have changed after the results have been capture. Thus it is possible that you will be running the updated audit, and not necessarily the exact audit from which produced these results.

To rerun an audit:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Audit and Remediation**.
- 2 Select Audits, and then select either Windows or Unix.
- 3 Select an audit, and in the details pane, select an audit result for the audit. Each time the audit is run, its results are accumulated in the details pane.
- 4 Double-click the audit result to open it.
- 5 From the **Actions** menu, select **Re-Run audit**.
- 6 In the Run Audit window, step one shows you the name of the audit, the source server, or snapshot being used in the audit, the total number of rules defined in the audit, and all targets of the audit (servers and snapshot). Click **View Rule Details** to view the rule definitions.
(Optional) If you want to immediately run the audit, click **Start Job** at any point in the process.
- 7 Click **Next**.
- 8 In the Scheduling page, choose whether you want the audit to run immediately or at a later date and time. To run the audit at a later time, select **Run Task At** and then choose a day and time.
- 9 Click **Next**.
- 10 In the Notifications window, by default your user will have a notification email sent when the audit finishes, whether or not the audit job is successful. To add an email notifier, click **Add Notifier** and enter an email address.
- 11 *(Optional)* You can specify if you want the email to be sent on success or failure of the audit job.
- 12 *(Optional)* You can specify a Ticket Tracking ID in the Ticket ID field. The ticket ID field is only used when SA Professional Services has integrated SA with your change control systems. Otherwise, it should be left blank.
- 13 Click **Next**.
- 14 In the Job Status page, click **Start Job** to run the audit. When the audit has run, click **View Results** to view the results of the audit.

Scheduling an Audit

Scheduling an audit requires specifying when you want an audit to be run (either once or as a recurring job) and who you want to receive email notification about the status of the job. You can also view, edit, and delete or cancel existing scheduled audits. When you delete a scheduled audit, all schedules that you have created associated with that audit will also be deleted.



You must have permissions to create, view, edit, and delete audit schedules. To obtain these permissions, contact your SA administrator. See the *SA Administration Guide* for more information on permissions.

Scheduling a Recurring Audit

After you have created, configured, and saved an audit, you can set up a schedule that specifies when you want the audit to run on a recurring basis. When you specify a recurring schedule, the end date must allow for the audit job to run at least once. After the schedule is set, you can edit the schedule according to your needs.

To schedule a recurring audit:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Audit and Remediation**, and then select Audits.
- 2 Select an OS (Windows or UNIX) and then double-click an audit to open it.
- 3 In the Views pane of the Audit window, select Schedule.
- 4 In the Schedule section, choose to run the audit once, daily, weekly, monthly, or on a custom schedule. Parameters include:
 - **None**: No schedule will be set. To run the audit, select the audit, right-click, and select **Run Audit**.
 - **Daily**: Choose this option to run the audit on a daily basis.
 - **Weekly**: Choose the day or days of the week to run the audit.
 - **Monthly**: Choose the months to run the audit run, and the days of the month.
 - **Custom**: In the Custom Crontab string field, enter a string that indicates a time schedule. The crontab string can include serial (1,2,3,4) and range (1-5) values. For example, the following crontab string will create the audit at 1:00 a.m. every weekday:

```
0 1 * * 1-5
```

An asterisk (*) in any of these fields represents all days of the month, all months of the year, all days of the week, and so on. For more information about crontab entry formats, consult the Unix man pages.
- 5 In the Time and Duration section, for each type of schedule, specify the hour and minute you want the daily schedule to start. Unless you specify an end time, the audit will keep running indefinitely. To choose a date to end the audit schedule, select End and then choose a date. The Time Zone is set according to the time zone set in your user profile.
- 6 (Optional) Deselect the End option, if you want the audit schedule to run indefinitely.
- 7 To save the audit schedule, from the **File** menu, select **Save**. The audit will now run according to the defined schedule.

Editing an Audit Schedule

You can edit an audit schedule after you have created (or edited) and saved it.

To edit a scheduled audit:

- 1 In the navigation pane, select Jobs and Sessions.
- 2 Select Recurring Schedules.
- 3 In the drop-down list at the top of the content pane, select Audit Servers.
- 4 Select a scheduled audit job, right-click, and select **Open**.
- 5 In the Audit window, select Schedule in the Views pane to view the audit schedule.
- 6 To edit the audit Schedule, modify the following parameters:
 - **None**: No schedule will be set. To run the audit, select the audit, right-click, and select **Run Audit**.
 - **Daily**: Choose this option to run the audit on a daily basis.
 - **Weekly**: Choose the day or days of the week to run the audit.
 - **Monthly**: Choose the months to run the audit run, and the days of the month.
 - **Custom**: In the Custom Crontab string field, enter a string that indicates a time schedule. The crontab string can include serial (1,2,3,4) and range (1-5) values. For example, the following crontab string will create the audit at 1:00 a.m. every weekday:

```
0 1 * * 1-5
```

An asterisk (*) in any of these fields represents all days of the month, all months of the year, all days of the week, and so on. For more information about crontab entry formats, consult the Unix man pages.
- 7 In the Time and Duration section, for each type of schedule, specify the hour and minute you want the daily schedule to start. Unless you specify an end time, the audit will keep running indefinitely. To choose a date to end the audit schedule, select End and then choose a date. The Time Zone is set according to the time zone set in your user profile.
- 8 (Optional) Deselect the End option, if you want the audit schedule to run indefinitely.
- 9 To save the audit schedule, from the **File** menu, select **Save**. The audit will now run according to the defined schedule.

Viewing a Completed Audit Job

To view information about a completed audit job:

- 1 In the navigation pane, select Jobs and Sessions.
- 2 Select Job Logs.
- 3 The content pane displays all jobs run in this SA core. To display only audit jobs, from the drop-down list at the top of the content pane, select Run Audit Task. If you want to see only your scheduled audits, enter your user ID in the User ID field at the top of the content pane.
- 4 Open an audit job to view the audit results, and then click **View Results**.

Exporting/Importing an Audit

Use the audit filter to tell DET which audit to export from an SA core/mesh so that you can then import it into another SA core/mesh. See the *SA Content Utilities Guide*.

Viewing Audit and Snapshot Usage

After you create and run an audit, you can view it from the All Managed Servers list or from the Device Explorer, and see all audits that are associated with a certain server.

From All Managed Servers

To view a server's audit usage from the All Managed Servers list:

- 1 In the navigation pane, select **Devices** ► **Servers** ► **All Managed Servers**.
 - 2 In the content pane, select a server.
 - 3 In the View drop-down list, select Audits or Snapshot Specifications. The details pane shows information about audit and snapshot usage.
 - 4 If you selected Audits, in the details pane you can choose one of the following options:
 - **Audit - Server is Target:** Shows all audits where the selected server is the target of the audit.
 - **Audit - Server is Source:** Shows all audits where the selected server is used as the source of the audit.
- Or
- 5 If you selected Snapshot Specifications, the details pane shows all snapshot specifications that target the selected server.
 - 6 *(Optional)* In any either of these views, you can select an audit or audit results, and perform actions from the Actions menu. For example, you can open an audit, create an audit, re-run an audit, or delete an audit.

From the Device Explorer

To view a server's audit usage from the Device Explorer:

- 1 In the navigation pane, select **Devices** ► **All Managed Servers**.
- 2 In the content pane, select a server, right-click, and then select **Open**.
- 3 In the Device Explorer, from the Views pane, select **Management Policies** ► **Audits**.
- 4 In the content pane, from the Show drop-down list, select one of the following options:
 - **Audit - Server is Target:** Shows all audits where the selected server is the target of the audit.
 - **Audit - Server is Source:** Shows all audits where the selected server is used as the source of the audit.
- 5 *(Optional)* In this view, you can select an audit and perform actions from the Actions menu. For example, you can open an audit, create an audit, re-run an audit, or delete an audit.
- 6 Next, from the Views pane you can select Archived Audit Results to see all audit results associated with this server that have been archived.

Audit Configuration

The following tasks are required to configure an audit or an audit policy:

- Name and describe the audit or audit policy
- Select a source for the audit or audit policy: a server, a snapshot, snapshot specification, or none.
- Configure the audit rules—you have the option of linking to an audit policy. This specifies that you want to use the rules from an audit policy in your audit. This also disables the ability to configure individual rules. You can also import all rules of an audit policy into the audit.
- Choose a target server, group of servers, or snapshot to audit
- Add audit rule exceptions (optional)
- Schedule the audit
- Set the Email Notification (*optional*)
- Save the audit



VMware ESXi servers cannot be the source or the target of an audit or snapshot.

To configure an audit:

- 1 Create the new audit from one of the methods described in [Creating an Audit](#) on page 19. The Audit window opens.
- 2 Enter the following information for the audit:
 - **Properties:** Enter a name and description for the audit.
 - **Source:** Every audit can use a server, snapshot, or snapshot specification as its source. (Or, you can choose no source and define your own rules.) If you use a server as the source, you can browse the server for values to define the audit's rules. If you choose a snapshot, you will be limited to the rules in the snapshot and the snapshot results when you define the audit rules. If you choose a snapshot specification, then the audit will compare the snapshot taken of the targets of the snapshot specification, and compare those against the targets of the audit. When you choose snapshot specification as the source, the rules in the snapshot are not editable. If you choose no source, you must define your own rules, or choose to link to an audit policy in the rules section. Some rules, however, require a source in order to be defined.
 - **Rules:** Choose a rule category from the list to begin configuring your audit's rules. Each audit rule is unique and requires its own instructions. For information on how to configure individual audit rules, see [Audit & Remediation Rules](#) on page 33.

If you want to use an audit policy to define the rules of your audit, click either [Link Policy](#) or [Import Policy](#). When you link an audit policy, the audit maintains a direct connection with the audit policy, and disables the ability to create rules. After you link a policy, the audit will use only the rules configured in the audit policy. So if any changes are made to the policy, the audit will update with the new changes. If you import an audit policy, the audit will use all the rules defined in the policy but will not maintain a link to the audit policy. For information about audit policies, see [Audit Policy Management](#) on page 78.

- **Targets:** Choose the Targets of the audit. These are servers, groups of servers, or snapshots that you want the configured audit rules to evaluate and compare. To add a server or group of servers, click **Add**. To add a snapshot target, in the Snapshot Targets section, click **Add**.

- **Exceptions:** Click **Add** to add exceptions to the rules in your audit. In the Add Exception window, select a server or multiple servers (or device groups), and then select one or more rules you want to except from the chosen servers. You can except any of the rules in the audit from any of the target servers or snapshots. You can optionally add an explanation, a ticket ID, and an expiration date for the exception.
- **Schedule (Optional):** Choose whether you want to run the audit once, daily, weekly, monthly, or on a custom schedule. Parameters include:
 - **None:** No schedule will be set. If you want to run the audit immediately, or on a onetime basis, you have to select the audit, right-click, and select **Run Audit**.
 - **Daily:** Choose this option to run the audit on a daily basis.
 - **Weekly:** Choose the day of the week that you want the audit to run.
 - **Monthly:** Choose the months that you want the audit run.
 - **Custom:** In the Custom Crontab string field, enter a string that indicates a time schedule. The crontab string can include serial (1,2,3,4) and range (1-5) values. For example, the following crontab string will create the snapshot at midnight every weekday:

```
0 0 * * 1-5
```

An asterisk (*) in any of these fields represent all days of the month, all months of the year, all days of the week, and so on. For more information about crontab entry formats, consult the Unix man pages.
 - **Time and Duration:** For each type of schedule, specify the hour, minute, day of the week, and month for the schedule to start. Unless you specify an end time, the audit will keep running indefinitely. To choose an end date, select End. In the calendar selector, choose an end date. The Time Zone is set according to the time zone set in your user profile.
 - **Notifications:** Enter email addresses to notify people when the audit job finishes running. You can choose to send the email on both the success and the failure of the audit job (not the success of the audit rules). To add an email address, click Add Notification rule. (This is only relevant if the audit is set to run on a recurring schedule.)

3 When you have finished configuring the audit, from the **File** menu, select **Save**.

Audit & Snapshot Sources

There are several options for choosing a source for an audit or a snapshot specification:

- Source: [Server](#) on page 29
- Source: [Snapshot](#) on page 30
- Source: [Snapshot Specification](#) on page 30
- Source: [Rules](#) on page 31

The source of an audit determines the rules you are able to select from and configure in your audit or snapshot specification. Choosing a source depends on the purpose of your audit or snapshot specification.

Source: Server

A managed server can be a source for an audit or a snapshot specification.

If you know that a certain server contains the desired server objects that you want to add to the audit or snapshot specification, choose that server as the source of an audit. For example, if you are interested in auditing or taking a snapshot of application configuration files for an Apache Web Server (such as `httpd.conf`) on certain target servers, choose a server that you know has Apache installed on it and that is configured correctly—as the source of your audit.

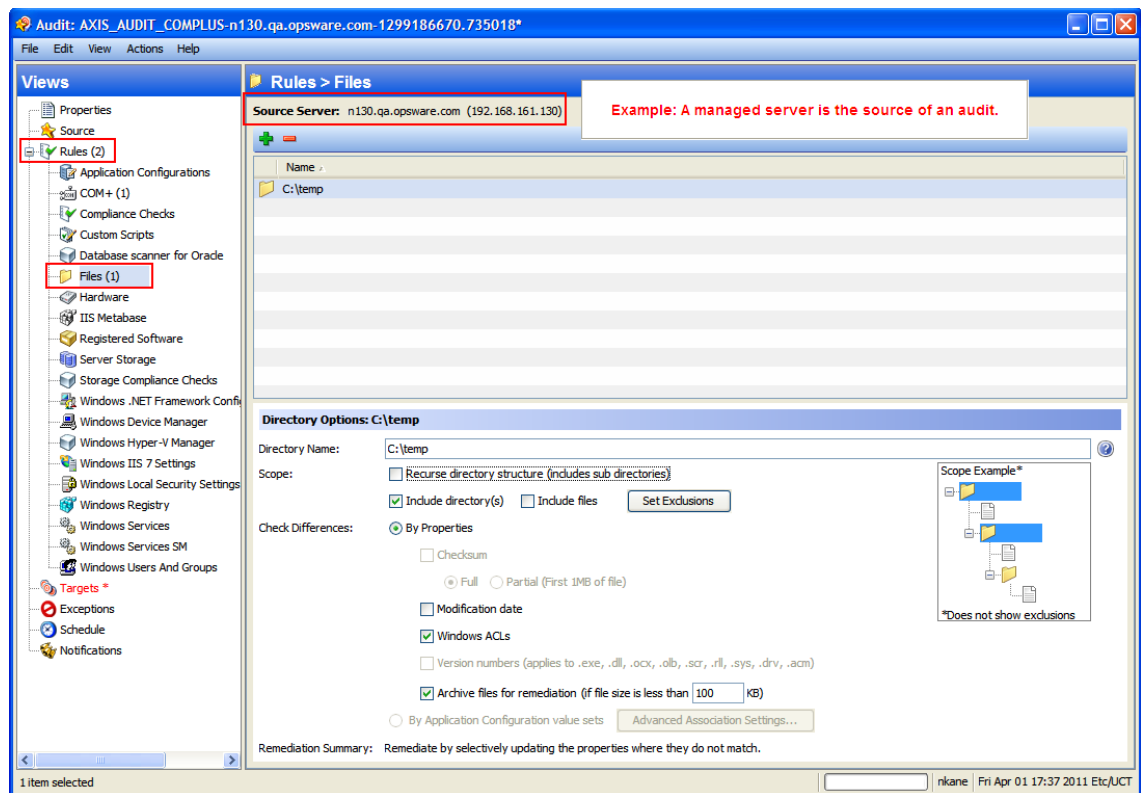
You can choose several different source servers when you create your audit or snapshot specification rules. You can also choose a different source for each server object rule.



VMware ESXi servers cannot be the source of an audit or snapshot.

Figure 3 shows the content pane that displays in an Audit window or in a Snapshot Specification window, when you choose a server as the source for an audit.

Figure 3 Server as Source of Audit: Creating Audit Rules



See [Common Scope Cases with Diagrams](#) on page 46 for more information about Directory Options.

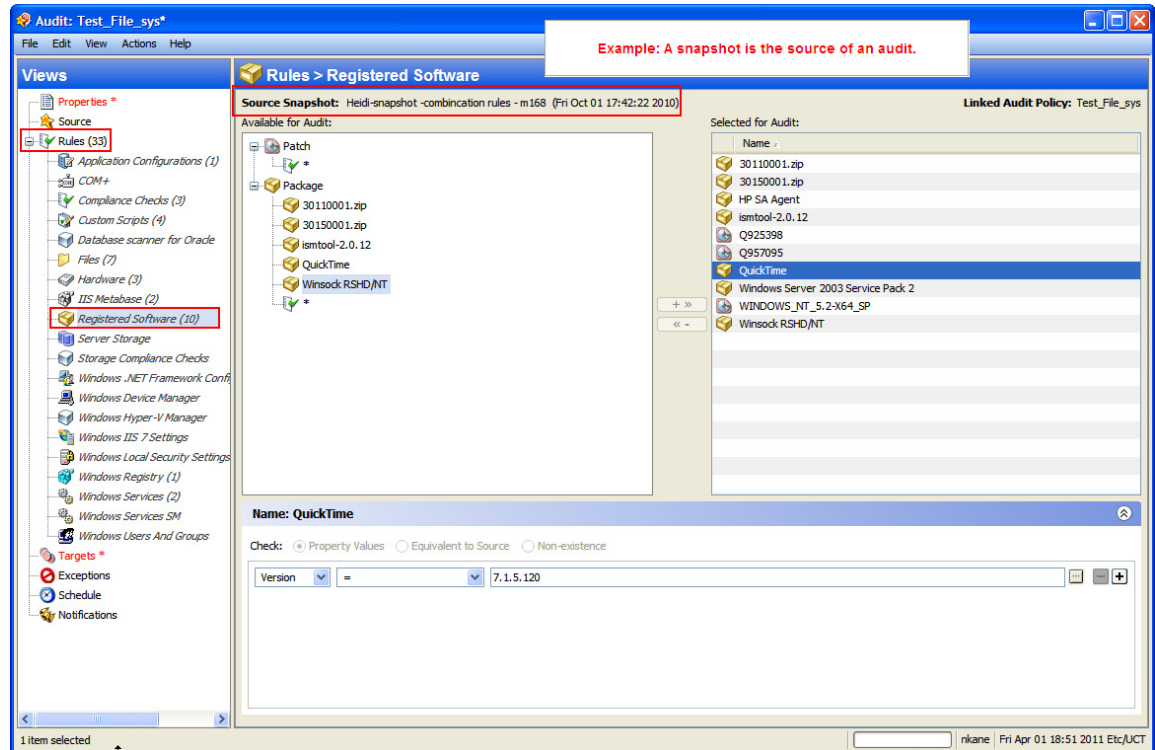
Source: Snapshot

A snapshot can be a source for an audit or a snapshot specification.

If you have a snapshot of a managed server that is in a known good state (a *golden server* configuration) and you would like to compare that snapshot with other servers in an audit, choose that snapshot as the source for an audit or a snapshot specification. Or, choose this option to use the captured server values to take a snapshot of another server. Using a snapshot as the source for an audit or snapshot specification allows you to choose both the results and the rules of the original snapshot specification that the snapshot was based on.

Figure 4 shows the options for creating audit or snapshot specification rules when you use a snapshot as the source. You can choose from the snapshot's results and the snapshot's rules.

Figure 4 Snapshot as Source of Audit: Available Server Objects to Create Audit Rules



Source: Snapshot Specification

A snapshot specification can be a source for an audit. This is commonly known as *reflexive auditing*.

Choose this option if you want to keep track of a server's configuration over time and monitor any changes that occur. For example, you might want to keep track of an application to make sure that its configuration remains correct over a period of time. If this application runs on several servers, you can create a snapshot specification that defines a desired state of server configuration and then run the snapshot.

Next, you can create an audit and use the snapshot specification as the source for your audit. Each server that was targeted by the snapshot is now also included as a target of the audit. When you run the audit, either on-demand or on a scheduled basis, each server's current configuration will be compared with the state originally captured from the snapshot. If the snapshot specification that serves as the source of the audit is set to run on a recurring basis, the audit will compare against the most recently run snapshot. Any changes are displayed in the audit results window.

Source: Rules

Rules that use a source value from a source server can be used as a source for an audit.

Most rules require a source in order to define them, except the following rules:

- Any of the pre-configured rules that you do not set the value to derive from a source (server or snapshot or snapshot specification)
- Custom Scripts rules that you do not set the compare value to derive from a source (server or snapshot or snapshot specification)

You cannot save an audit that contains rules that require a source and no source has been specified. You must select a source for all comparison checks and for rules that compare against a source value.

Server Objects

Table 1 lists all server objects that you can create rules for in an audit or in a snapshot specification. Some server object values are captured and audited live and some objects are captured from the Model Repository.

Table 1 Server Objects Used in Audits & Snapshots

Server Object	Description	Captured Live and/or from Model Repository
Application Configurations	Contents of application configuration files and their values.	Live
Windows COM+ (See note below table.)	COM+ objects and component categories.	Live
Custom Scripts	Write your own custom scripts to retrieve information from a server and compare contents. For example, you can run a script to gather output from a custom application and evaluate returned output against values set in the audit. (Python 1.5.2 only for python scripts.)	Live
Discovered Software	Discovered Software provides a signature-based software discovery mechanism for Windows and UNIX managed servers to help you manage applications and software that are not managed by SA.	Live
Files	Contents of files and directories (and subdirectories), user and group access, checksum for files, file modification date, and Windows ACLs (Windows only).	Live
Hardware	CPU, storage devices, and memory.	Model Repository
IIS Metabase	Microsoft IIS Metabase objects and configuration values to snapshot or audit.	Live
IIS 7.0	Microsoft IIS 7.0	Live
Internet Information Server	Real time information about IIS for a Windows server, such as server name, server type, server state, log file path, document file path, and so on.	Live

Table 1 Server Objects Used in Audits & Snapshots (cont'd)

Server Object	Description	Captured Live and/or from Model Repository
Local Security Settings	Real time information about security settings, including security settings such as password policy, audit policy, user rights, and security options.	Live
Registered Software	All installed packages or patches actually installed on a source server, whether or not they have been registered by the model repository.	Live
Storage	<p>Information related to storage devices and SAN devices and connections in your data center (if your core is storage-enabled).</p> <p>In order to audit and snapshot SAN objects, Storage Essentials (SE) version 6.1.1 or later is required and the Server Automation SE Connector component must be installed and configured on your SA core.</p>	Live
BSA Essentials Subscription Services “compliance checks”	If you are subscribed to BSA Essentials Subscription Services, you have access to many different types of audit rules and their constituent components (also known as “compliance checks”. The exact kind of checks you have access to depend on your subscription, but can include such rules as the latest patch supplements for Microsoft Windows, current regulatory compliance policies (for example, FISMA, Sarbanes-Oxley), user-created rules from the BSA Essentials Subscription Services developer community, daily updated vulnerability content, and so on.	Live
Users and Groups	Compare information about users and groups on servers, such as user name for last login, whether or not CTRL + ALT + DELETE is enabled, and so on.	Live
Windows .NET Framework Configuration	<p>Real time information about Assembly Cache and Configured Assembly List, such as assembly name, version, locale, public key token, cache file (GAC or ZAP), processor architecture, custom, and file name.</p> <p>For every Configured Assembly List, you can use information such as assembly name, public key token, codebases, binding policy, file name, file data.</p>	Live

Table 1 Server Objects Used in Audits & Snapshots (cont'd)

Server Object	Description	Captured Live and/or from Model Repository
Windows Registry	Select Windows Registry directories or registry key values to capture and compare.	Live
Windows Services	Select Windows services.	Live
Windows Users and Groups	Users and groups information on a Windows Unix servers.	Live



A **Windows COM+** category (folder) that does not have any objects will not be included in a snapshot or audit, even though SA will display an empty COM+ folder in the Device Explorer.



SA audit and remediation does not support device files or sockets.

Audit & Remediation Rules

When create an audit or snapshot specification, you must configure audit and remediation rules. These rules define:

- The type of server object to snapshot or audit and compare. These are objects such as the server's file system, hardware information, application configurations, installed patches or software, users and groups, and so on.
- Information about the object to audit or snapshot. For example, for a server's file system, you can capture Windows NT file's Access Control Levels. For an application, you can capture the application configuration values you want to snapshot or audit, plus any remediation values that specify whether differences are discovered between the rule and the actual value that is on the target server.

A rule can contain a custom script that seeks to determine if all passwords stored in a file match a certain character length. A rule can also include a check to determine whether a particular Windows Service is running or disabled on a server. For some rules, you can also specify the remediation value for the server object if the value defined in the audit or snapshot differs from the server's value after the audit has run. For example, if a Windows Service is disabled, you can specify that the remediation value should restart the service. Remediation values are implemented manually, after the audit has run, from the Audit Results window

Configuration Rules

Some rules are very simple to configure and define and do not require anything more than selecting the server objects that you want to snapshot or audit. Some rules might check to determine whether a value or property exists on a configuration file on a server, without the need for setting any advanced parameters.

For example, the Discovered Software rule checks for all registered and unregistered software that is installed or deployed on a target servers. The Hardware rule allows you to check the CPU, memory, or storage values that exist on target servers. In this case, no extra rule parameters are necessary.

Other rules are more complex and require more advanced configuration, such as specifying an expression that looks for a range of values and specifies remediation that replaces undesired values.

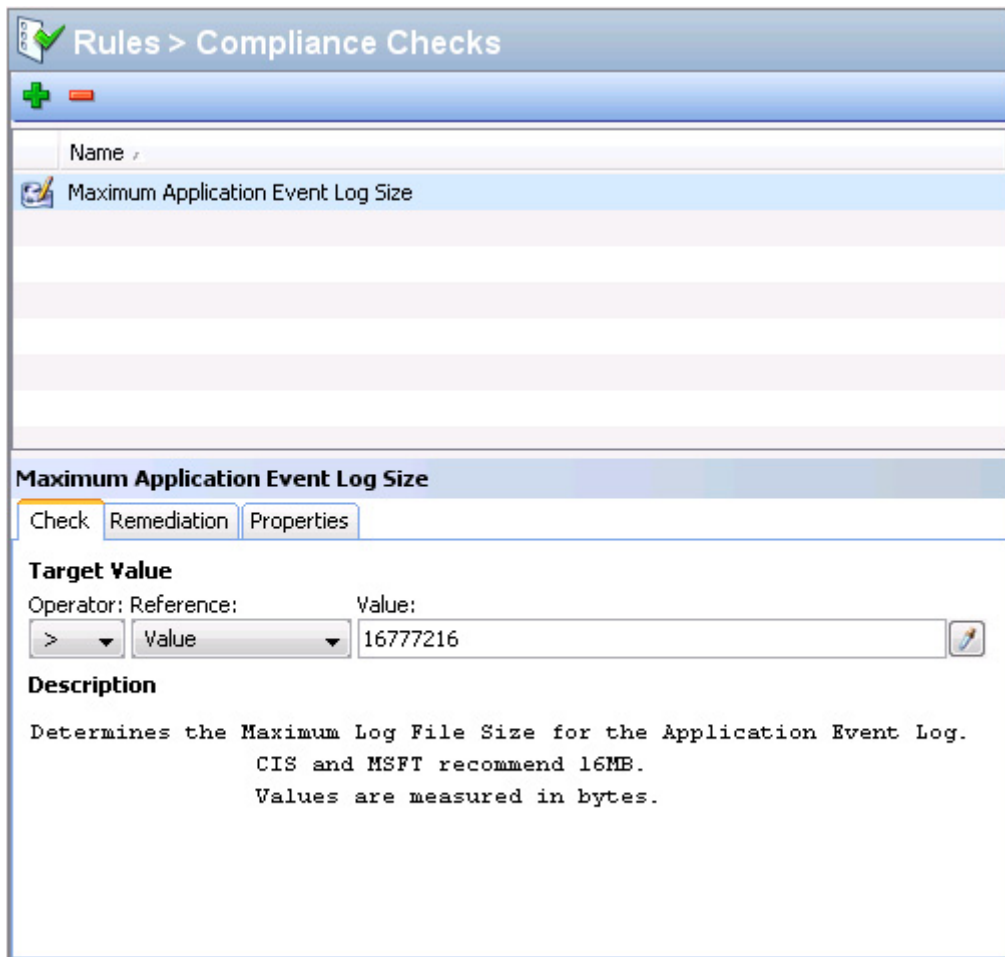
In an audit and audit policy, you can also define what, if any, remediation value you would like the object to have. Remediation values are used only if a server object is found to be different than the desired state—that is, the configuration on the target server is out of compliance with the rules of the audit. Remediation values are implemented manually, after the audit has been run, from the Audit Results window.

An audit rule consists of the following components:

- **Server Object:** This is a specific server configuration that an audit can evaluate, such as a server's file system, application configuration values, hardware information, installed software (patches and packages), Windows Registry entries, and so on. A server object usually consists of several other things that you can check as well. For example, on a Windows server you might want to know if a specific Windows service exists on target servers and whether or not it is enabled.
- **Target Value:** This is value or setting you want to check for on the target server, or the desired value. For example, you might want to determine if a specific directory exists on a server, or if an application is configured properly, or a particular service is enabled, and so on.
- **Remediation Value:** This is the value that you want to change for the server object during remediation, if the target value is not found on the target server. Remediation value is not implemented automatically; you must make the remediation change after the audit has run.

Figure 5 illustrates an audit rule defined for a Windows Service named File Replication.

Figure 5 Custom Audit Rule Configured with Remediation Values



In [Figure 5](#), the audit rule has been configured in the following manner:

- **Rules > Compliance Checks:** Lists the selected rule (Maximum Application Event Log Size) from the BSA Essentials Subscription Services.
 - **Rules Details Check**
 - **Target Value:** This is the desired value compared against the value on the server that is the target of the audit. In this example, the rule is configured to determine whether the target server's Application Event Log file size has not exceeded 16777216 bytes. For example, the Target Value parameters in this example have been set to: > Value 16777216.
 - **Description:** Describes the value that is being checked on the target server. In this example, the audit will check to see if the Application Event Log file size has not exceeded the CIS and MSFT recommended size limit of 16MB (16777216 bytes).
- This information instructs the audit to evaluate the target server's Application Event Log file size and determine whether it exceeds 16MB.
- **Remediation:** The remediation value determines the action to take if the value on the target server does not match the value you defined in the audit (target value). In this example, the remediation value is set to the CIS and MSFT recommended size limit of 16MB (16777216 bytes). You can remediate this value from the Audit Results window, after the audit has run, and only if the target server's value fails the rule criteria.

Audit and Snapshot Rules



You must have permissions to create and configure audit and remediation rules. To obtain these permissions, contact your SA administrator. See the *SA Administration Guide* for more information on permissions.

For information about rules you can set for each type of server object, see one of the following sections for the specific server object that you want to configure a rule for:

- [Configuring Application Configuration Rule](#)
- [Configuring COM+ Rule](#)
- [Configuring Custom Scripts Rule](#)
- [Configuring the Discovered Software Rule](#)
- [Configuring the File Rule](#)
- [Configuring Hardware Rule](#)
- [Configuring IIS Metabase Rule](#)
- [Configuring IIS Rule](#)
- [Configuring IIS 7.0 Rule](#)
- [Configuring Local Security Settings Rule](#)
- [Configuring Registered Software Rule](#)
- [Configuring Storage Rule](#)
- [Configuring Windows .NET Framework Configurations Rule](#)
- [Configuring Windows Registry Rule](#)
- [Configuring Windows Services Rule](#)
- [Configuring Windows/UNIX Users and Groups Rule](#)

- [Configuring Compliance Checks](#)



Some SA cores may contain legacy content, such as Event Logging, Operating System, and Users and Groups rules with compliance checks. These checks have been integrated into the CIS policies available from the EP.

Configuring Application Configuration Rule

The application configuration audit rule allows you to audit configuration file values on managed servers, to check that those files are configured the way you want them to be.

You can choose from a list of predefined application configuration templates which serve as the basis of comparison for the target configuration file you want to audit. You can also choose from custom application configurations that a user in your organization has created and made available for usage in an audit, snapshot specification, or audit policy.

An application configuration in an audit models the values and structure of an application's configuration file, which allows you to set rules that check the values in actual configuration files on managed servers.

When you choose an application configuration inside an audit, snapshot specification, or audit policy and click **View**, you will see the contents of the configuration file from the source of the audit. All key-value pairs that you are able to add to the audit rule will display.

The information displayed inside an audit windows depends on the source of the audit or audit policy (or the target for a snapshot specification):

- If you choose a server as the source of the audit or audit policy, then the application configuration values displayed in the audit rule will be those of the configuration file on the source server, as filtered through the application configuration template.
- If you choose a snapshot as the source of the audit or audit policy, then you will only be able to modify the values that were captured at the time the snapshot was taken.
- If you do not choose any source, then you will not be able to configure a rule for the application configuration file.
- If you choose to configure an application configuration in a snapshot specification, then the values of the configuration will derive from the target server.



In an audit's application configuration rule, you will only see values of the source configuration file that have been modelled in the application configuration. If the application configuration is customized and has no name-value pair defined (but the value exists in the source configuration file), you will not see it in the audit or audit policy.


After you view the contents of the source application configuration file, you can define create your rules by selecting values from the source file and building rules that will be used to check against the target configurations. You can also define remediation values in the event that the audit finds differences between the rules and the target configuration file values.

Creating an Application Configuration Rule

To understand how to configure an application configuration rule, it is useful to look at an example. Your goal is to create an audit rule for a UNIX hosts file (`/etc/hosts`), and then audit a group of servers' `/etc/hosts` files to make sure they contain the correct values.

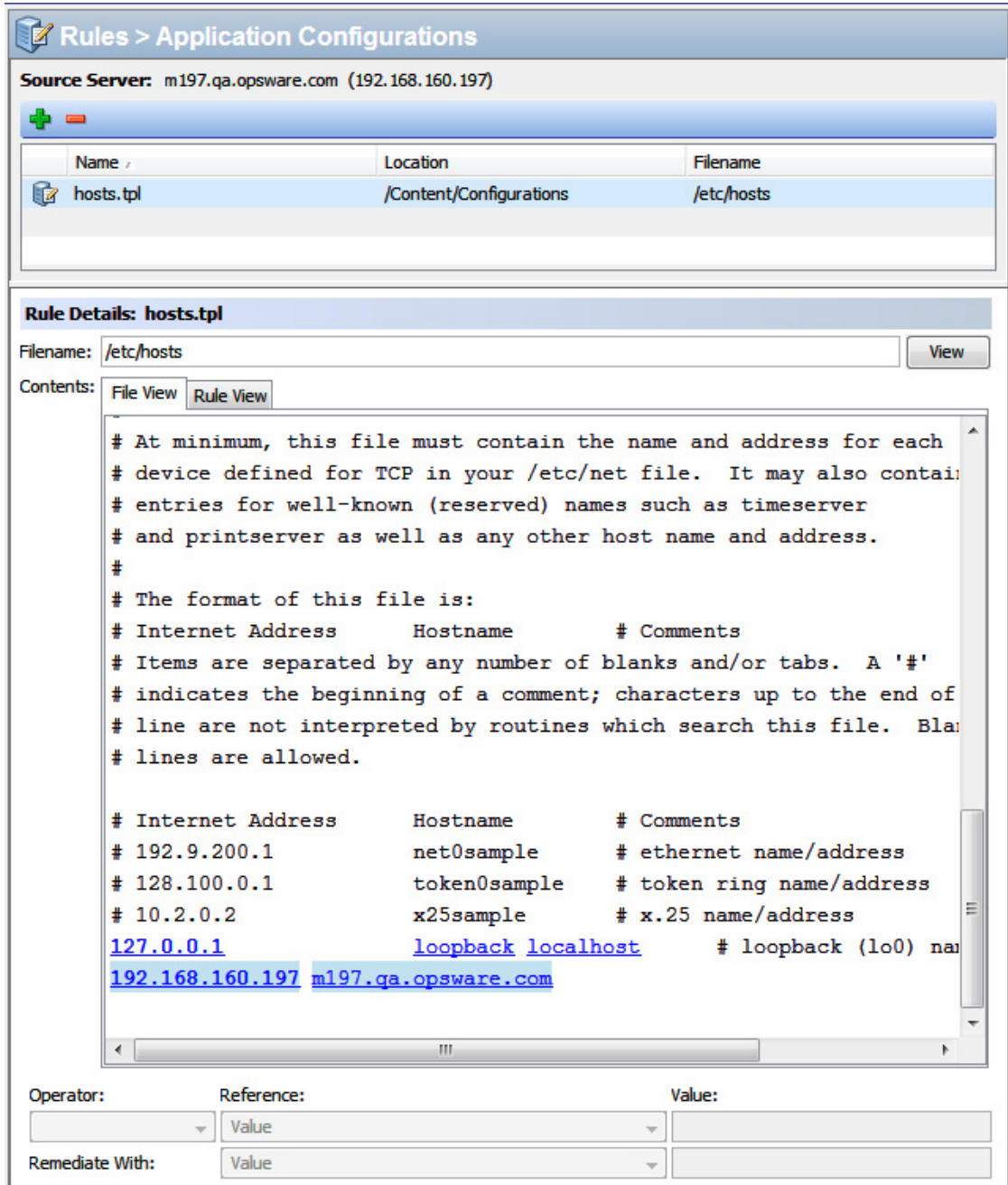
You know that the UNIX hosts file on a particular “golden” server represents the ideal state of hosts file configuration that you would like other servers to conform to. You can choose that golden server as the source for your audit and borrow the values from that file to construct the rule for the audit. After you create the rule and save the audit, you can run the audit against a group of servers to see if their /etc/hosts files are configured correctly (according to the audit rule).

To create an application configuration rule:

- 1 Create an audit from any one of the methods for creating an audit listed at [Creating an Audit](#) on page 19. (If you want to create this rule for a snapshot specification, see [Creating a Snapshot Specification](#) on page 108.)
- 2 Select an Audit Source: Server, Snapshot, Snapshot Specification, or No Source. The source selected for the audit will determine what types of rules, if any, you can create for an application configuration. You must choose a source or you will not be able to configure the application configuration rule.
- 3 In the Audit window, in the Views pane, select Rules ► Application Configurations.
- 4 In the content pane, click  to access all available configuration templates.
- 5 In the Select Configuration Templates window, select one or more templates you would like to add to the audit rule and then click **OK**.
- 6 Select the template you want to configure. Its contents appear in the template editor.
- 7 Click **View**. (If you cannot view the contents of the configuration file, you might need to enter the correct path in the Filename section.) You see the contents of the configuration file in the File View tab.

For example, if you view a UNIX hosts file, you would see information similar to the example in [Figure 6](#):

Figure 6 Application Configuration Audit Rule for Hosts File



You can see the contents, the IP address/host name pairs, from the source hosts file, highlighted in blue text.

- 8 To create an audit rule for this configuration file, choose a key-value pair from the hosts file on the source server (the server you choose as the source for the audit).
- 9 To create this rule, first select an IP addresses in the File View tab area, which shows the contents of the file obtained from the source server. In the example in Figure 6, you can select an IP address such as 127.0.0.1. After you select the IP address, the element becomes highlighted in blue. This means that the element is ready to have a rule created from it.

For more information on the color scheme used when configuring an application configuration audit rule, see Table 2.

After you have selected the IP address in the contents area, notice that the value in the Operator field in the below is set to blank. This means that an operator has not yet been added to the rule. To add the value to the rule, you can either double-click it, or enter the following parameters in the rule expression area below the contents:

- **Operator:** Choose = (equals). When you change the operator to =, then the equals operator immediately becomes added to the rule. If you change the operator back to no selection, then the operator is immediately removed from the rule.
- **Reference:** Choose Value.
- **Value:** Enter 127.0.0.1.
- **Remediation:** Enter 127.0.0.1.

This expresses that you want to look for an IP address with the value of 127.0.0.1. If this is not found, then the remediation should be 127.0.0.1, so you can add this to any host files on the target servers that do not contain this IP address.

- 10 Select a host name in the File View tab area. Notice that the initial IP address you selected in the previous step has turned green. This means that the next rule parameter you set will be paired with the IP address you previously selected.
- 11 In the Rule section, set the following parameters:
 - **Operator:** Choose = (equals).
 - **Reference:** Choose Value. (If you choose a custom attribute here for the rule definition, this custom attribute must also exist on the target servers or the audit for this rule will fail.)
 - **Value:** Choose host.
 - **Remediation:** Choose host. This adds the final part of the rule that will check the target server for the key-value pair of IP address 127.0.0.1 matched with host.
- 12 Select the Rules View tab. The rule will be expressed as:

“Check that there is an entry where IP address is equal to value 127.0.0.1 and Hostnames contains an entry equal to value host.”

This rule is what will be used to audit the hosts file on the target server or snapshot specification.
- 13 To configure more application configuration rules, select more application configurations from the Available for Audit section.
- 14 To finish configuring the audit, define other rules and set the target servers, schedule, and notification for the audit.
- 15 Save the audit.
- 16 To run the audit, from the **Actions** menu, select **Run audit**. For more information about running an audit, see [Running an Audit](#) on page 21.

Application Configuration Audit Rule Color Scheme

When you first view an application configuration, all elements that can be used to build an audit rule will appear in blue underlined text. After you start selecting and building rules, then the colors will change. Table 2 describes the color scheme used for configuring application configuration audit rules.

Table 2 Application Configuration Audit Rule Color Scheme

Text Color	Description
Blue underlined	This shows all elements in the source configuration file that can be used in a rule.
Highlighted Dark Blue	This shows an element is selected but has no rule has been associated with it.
Highlighted Light blue	This shows all that you add an element to a rule.
Highlighted Medium blue	This shows all that an element is both selected and has a rule associated with it.
Green	<p>This shows all that the element is a primary key and is related to the current selected element. This means that the element will be used in the same rule that the current selected element will be used in.</p> <p>If the currently selected element is given a comparison value (=, contains, matches...) then the other elements with the green text will automatically be given a comparison value of “=”.</p> <p>An example of this would be:</p> <pre>127.0.0.1 localhost</pre> <p>If localhost is selected, then 127.0.0.1 would be green. If localhost is given a comparison value, then 127.0.0.1 will also be given an automatic comparison value, giving you a rule such as:</p> <p>There is an entry where ip is equal to 127.0.0.1 AND hostname is equal to localhost.</p>
Bold	This represents a primary key.
Italicized	This shows a custom attribute or SA attribute.

Configuring COM+ Rule

To configure a Windows COM+ rule, select the source COM+ objects that you want to audit or snapshot on a target server. The COM+ rule also checks Access Control Levels (ACLs) for the selected object as well as any ACLs that are inherited.

COM+ objects are categorized based on attributes of the object, where the COM+ object specifies zero or more categories. The audit or snapshot window displays all COM+ objects in one node in the Rules section of the COM+ object tree. To add a COM+ rule to the audit or snapshot, select it and click the right arrow button.

If you would like to be able to remediate COM+ rules in your audit or snapshot results, select the “Archive all associated files” option when you select the COM+ object or category.

Selecting the “Archive all associated files” option will also include all AccessPermissions and LaunchPermissions associated with the COM+ object in the audit or snapshot rule, including those that are inherited parent COM+ objects.



You cannot audit the COM+ root folder, but can audit as many of the COM+ individual objects or sub categories as you wish.

To configure a COM+ rule:

- 1 Create the new audit using one of the methods for creating an audit listed in [Creating an Audit](#) on page 19. (If you want to create this rule for a snapshot specification, see [Creating a Snapshot Specification](#) on page 108.)
- 2 Select an Audit Source: Server, Snapshot, Snapshot Specification, or No Source. (Some audit rules, such as Application Configuration and Windows User’s and Groups, must have a source.)
- 3 In the Audit window, from the View pane, select Rules ► COM+.
- 4 In the content pane of the Audit window, expand the top level node in the Available for Audit section and select a COM+ object or object category.
- 5 Click the right arrow button to move the COM+ object or object category into the Selected for Audit section. All COM+ object or object categories you select will be audited on the target servers or snapshot specification. (You can select individual and COM+ categories for the rule, but you cannot select the root folder to add to the audit rules.)
- 6 You can now choose an option from the bottom of the rule window:
 - Select the “Archive all associated files” option if you want to be able to remediate COM+ rules in your audit or snapshot results.
 - Select Compare only the file name and not the full pathname if you want the COM+ rule to check only the selected filename and not the full path.
- 7 To finish configuring the audit, define any other COM+ object or object category rules you want and set the target servers, schedule, and notification for the audit.
- 8 To save the audit, from the **File** menu, select **Save**. You can also save the Audit as a policy. For more information, see [Saving an Audit or a Snapshot Specification as an Audit Policy](#) on page 83.
- 9 To run the audit, from the **Actions** menu, select **Run Audit**. For more information about running an audit, see [Creating an Audit Policy](#) on page 79.

Configuring Custom Scripts Rule

The custom script rule allows you to define your own script (batch, Python 1.5.2, or Visual Basic) to get and compare values used in an audit, audit policy, or snapshot specification. You can also write your own remediation scripts.

When you configure a custom script rule, you specify the target value, which is the expected values you want the script to return. The audit can gather this information in two ways:

- **Comparison-Based Audit:** Execute the script on the source server. The return values from the script (exit code or standard output) are compared with the output of the script after it has run on the target server or servers. This option is named: Source.

- **Value-Based Audit:** Specify your own value. This is compared with the output of the script after it has run on the target server. You can enter this value manually, if you know what the expected results of the script should be, or, you can execute the script on the source server and use those return values. When the audit is run, this value is compared with the returned results from the script after it has executed on the target server or servers. The option is named “Value.”

For an audit, you can also configure a remediation script, which can be used if differences are found between the rule and the value returned after the script has run on the target server.

For a snapshot, the script results will be generated by running the script (as defined in the rule detail) on target servers, and then captured in the snapshot. When you set up a snapshot specification, you can also add a remediation script. This type of script can be used to force remediation on target servers. You can execute the snapshot’s remediation script on target servers on an individual server basis from the Snapshot window.

To configure a custom script rule:

- 1 Create the new audit using one of the methods for creating an audit in [Creating an Audit](#) on page 19. (If you want to create this rule for a snapshot specification, see [Creating a Snapshot Specification](#) on page 108.)
- 2 Select an Audit Source: Server, Snapshot, Snapshot Specification, or No Source. (Some audit rules, such as Application Configuration and Windows User’s and Groups, must have a source.)
- 3 To build a script and define the audit rule, you can choose the following options:

Source

- **Rules:** Click **Add Rule** to add a new custom script rule.

Rule Details

- **Name:** Enter a name for the script.
- **Type of Script:** Choose from Batch, Python 1.5.2, PowerShell, or Visual Basic (VBS).
- **Script:** Type or copy and paste the script contents here. Or, click **Import Script** to import a script from your computer.


Success Criteria

- **Output:** Either Exit Code or Standard Output.
- **Operator:** Choose an Operator, such as equals (=), not equals (<>), less than (<()), greater than (>), and so one.
- **Reference:** Choose the source of the script output.
- **Source:** Select this option if you want the rule to execute the script on the source when an audit is run, and gets the value that the script requests. It will then compare that value with the value retrieved from the script that was run on the target server.

If you choose this option for a snapshot specification, then the script will run on the target, and the results of the script execution will be captured in the snapshot (results).

If the source of the audit is a snapshot, then the custom script rule will use the custom script definition configured in the snapshot specification.

- **Value:** Enter your own value. This option uses the value you enter and compares it with the value returned from the script after it is run on the target server. Using this option means that the script does not run on the source server at audit runtime. However, you can get the output from the script

immediately from the source server, if you click the eyedropper  icon. The returned value is displayed in the text box, which you can accept as is or edit to your liking.

If the source of the audit is a snapshot, then the custom script rule will use the Custom Script definition configured in the snapshot specification.

- **Server Attribute:** Select this option to compare a server attribute found on the source server with the output from the script that is run on the target server.
- **Custom Attribute:** Select this option to compare a custom attribute found on the target server with the output from the script that is run on the target server. Custom attributes for this option derive from the selected source server for the audit.

If you choose a custom attribute here for the rule definition, this custom attribute must also exist on the target servers or the audit for this rule will fail.

If you do not choose a source for the audit, this list will be empty.

Remediation

- **Type of Script:** Choose from Batch, Python 1.5.2, PowerShell, or Visual Basic (VBS).
 - **Script:** Type or copy and paste the script contents here. Or, click **Import Script** to import a script from your computer.
- 4 (Optional) You can add a remediation script to run if the audit comparison fails. The remediation will not be applied automatically; you can only run the remediation script from the audit results after the audit has run.

For a snapshot, the remediation script you define here can be executed on target servers on an individual server basis.

- 5 To finish configuring the audit, set the target servers, schedule, and notification for the audit.
- 6 To save the audit, from the **File** menu, select **Save**. You can also save the Audit as a policy. For more information, see [Saving an Audit or a Snapshot Specification as an Audit Policy](#) on page 83.
- 7 To run the audit, from the **Actions** menu, select **Run audit**. For more information about running an audit, see [Creating an Audit Policy](#) on page 79.

Custom Scripts Example

The following is an example of a custom VB script rule designed to enable a Windows user account and set the user's password.

(Note that this script will only work on Windows OS versions later than Windows NT 4.0. If you wish to enable a user account and set the password on Windows NT 4.0, you will have to do so manually.)

```
strComputer = "."
strAccountName = "red2"
Set objUser = GetObject("WinNT://" & strComputer & "/" & strAccountName )
objUser.AccountDisabled = False
objUser.SetPassword "AiH345^hjq"
objUser.SetInfo
```


Configuring the Discovered Software Rule

The Discovered Software rule provides a signature-based software discovery mechanism for Windows and UNIX managed servers to help you audit and snapshot applications and software that are not managed by SA.

Specifically, the Discovered Software can:

- Discover unregistered software which is not currently managed by SA
- Create an inventory of software that is not installed as part of an OS-registered application, or that was custom built
- Give you the ability to create snapshots of the discovered software on a server and then periodically audits against the snapshots over time
- Enable you to track in-house or custom built software

To configure the discovered software rule:

- 1 Create a new audit using one of the methods in [Creating an Audit](#) on page 19. (If you want to create this rule for a snapshot specification, see [Creating a Snapshot Specification](#) on page 108.)
- 2 Select an Audit Source: Server, Snapshot, Snapshot Specification, or No Source.
- 3 In the Audit window, from the View pane, select Rules ► Discovered Software.
- 4 In the content pane of the Audit window, in the Available for Audit section expand the Software icon. This may take a few moments to load if this is the first time you are loading the rule and you have selected a source for the audit or snapshot.
- 5 Select an element from the list and then click the right arrow button to move the rule object into the Selected for Audit section, which enables you to create a rule for the element.
- 6 For each check you want to configure in the rule, in the lower section of the audit window you can select one of the following rule criteria types:
 - **Property Values:** A values-based check that checks individual properties of the target object. For this type of check, each object requires that you build an expression that defines properties related to the object using the drop down lists at the bottom of the rule window. You can specify a unique operator which, depending on the type of object, can be a String, a Number (integer or float), Boolean (comparing values of 'true' and 'false'), Date (a date compare, not a time of day compare), or an Array.
 - **Equivalent to source:** A comparison check that performs a one to one comparison between the object on the source vs. the target servers. In this type of check, the values of each property selected from both the source and target servers must match exactly for the object to be compliant.
 - **Non-existence:** Checks for the non-existence of an object, to determine if it does not exist on the target server. If the object exists on the target server, then the rule is out of compliance.
- 7 You can also configure the rule based on a wildcard search by selecting the Wildcard rule object . When you select this object, in the rule configuration section at the bottom of the window displays a Name field, into which you can type a name (primary key) that will be searched on the target server. For example, you could enter simply * which would match everything on the target, P* would match all objects that begin with a capital P, while *P would match all elements ending with uppercase character 'P'.


After you enter a name or wildcard string, you can configure the rule parameters as you did in step 6.

It is important to notice that when using wildcard, all matching objects are restricted by the rule configuration. This type of audit rule is considered compliant if all found objects match the rule parameters.

- 8 To finish configuring the audit, set the target servers, any rule exceptions, the schedule, and the notification for the audit.
- 9 To save the audit, from the **File** menu, select **Save**. You can also save the Audit as a policy, which enables other users to access the rule set you create in the audit. For more information, see [Saving an Audit or a Snapshot Specification as an Audit Policy](#) on page 83.
- 10 To run the audit, from the **Actions** menu, select **Run Audit**. For more information about running an audit, see [Running an Audit](#) on page 21.

Configuring the File Rule

The file rule allows you to audit and compare files and directories on a target server by specifying the following options:

- **Directory Name:** The absolute path of the selected file or directory.
 -  (Optional) You can add a reference to an environment variable (`${varName}`) or a custom attribute (`@varName@`). See [Parameterizing Filenames for SA/Custom Attributes](#) on page 74 and [Environment Variables in Pathnames](#) on page 75.
- **Scope:** The default scope is directories + files. The Scope Example diagram in the Directory Options pane shows the scope use case hierarchy that is based on the options you selected. This diagram does not show exclusions. Click **View Exclusions** to view exclusions in the Set Includes/Excludes window.
 - Recurse Directory Structure**—Includes contents of all subdirectories for a selected file system folder to the audit, such as directories + files (recursive), files only (recursive), and directories only (recursive).
 - Include Directory(s)**—Specify directories in the file system you want included in and excluded from the audit. See [File Inclusion and Exclusion Rules](#) on page 69.
 - [Include Files]**—Specify files in the file system you want included in and excluded from the audit. See [File Inclusion and Exclusion Rules](#) on page 69.

The following list identifies 8 common use cases, in priority order. See the following [Common Scope Cases with Diagrams](#):

Scope Case 1: [Directories + Files \(recursive\)](#) on page 47

Scope Case 2: [Directories + Files \(default\)](#) on page 47

Scope Case 3: [Files Only](#) on page 47

Scope Case 4: [Files \(recursive\)](#) on page 48

Scope Case 5: [Directories \(recursive\)](#) on page 48

Scope Case 6: [Directory Only](#) on page 48

Scope Case 7: [Directories Only](#) on page 49

Scope Case 8: [Recursive Only](#) on page 49

- **Check Differences:**
 - By Properties**

Checksum: Performs a checksum on the contents of the selected file or files in a directory. You can choose to audit the entire contents of the file (Full) or only the first 1MB of the file (Partial).

Modification Date: Audits the file modification date to use for file or folder comparison.

User and Group Access Rights (*Unix only*): Audits the user and group access related to the file and directories.

Windows ACLs (*Windows only*): Audits the Windows Access Control List (ACL) for files and directories.

Note: If you are checking ACLs for the file rules and the user and group ACL does not exist on the target, after the audit and remediation processes complete, a temporary user and group will be created and assigned an unknown name. The next time you run an audit, the user and group displays as unknown. For more information on remediation, see [Audit Results](#) on page 84.

Version Numbers: For certain Windows file types (.exe, .dll, .ocx, .olb, .scr, .rll, .sys, .drv, .acm), the author of the file can set a file version and a product version. This option compares these version numbers. If they are different, the rule is considered non-compliant and the actual values on the target file can be viewed in the audit results.

Note: Not all files with these extensions always have a product version or a file version attribute.

Archive Files for Remediation: Archives the entire file. This option enables the audit to check for differences of a specified file, based on the differences you specify in the rule. Use this option when you want to remediate and view file differences found between the rule and the target file. If differences are found, remediating the differences will copy the source file to the target server and replace the target file with the source.

Note: This option can potentially create disk space demands on the SA core's database, depending on the size and number of files being compared.

By Application Configuration Value Sets: Uses an application configuration to evaluate configuration files on a target server. This option (including the **Advanced Association Settings**) lets you use a configuration template to compare any differences in values between a source configuration file and one on a target server. See [Comparing Files in Audits with Configuration Templates](#) on page 51.

- **Remediation Summary:** Remediate by copying the file and its properties from the source when selected properties do not match.

Common Scope Cases with Diagrams

The following examples show Windows directory options for each type of scope use case and related file system diagrams. For Windows, the **Windows ACLs** option is available. For Unix, the **User and Group Access Rights** option is available.

- [Scope Case 1: Directories + Files \(recursive\)](#) on page 47
- [Scope Case 2: Directories + Files \(default\)](#) on page 47
- [Scope Case 3: Files Only](#) on page 47
- [Scope Case 4: Files \(recursive\)](#) on page 48
- [Scope Case 5: Directories \(recursive\)](#) on page 48
- [Scope Case 6: Directory Only](#) on page 48
- [Scope Case 7: Directories Only](#) on page 49
- [Scope Case 8: Recursive Only](#) on page 49

Figure 7 is an example of options required for Directories + Files (recursive).

Figure 7 Scope Case 1: Directories + Files (recursive)

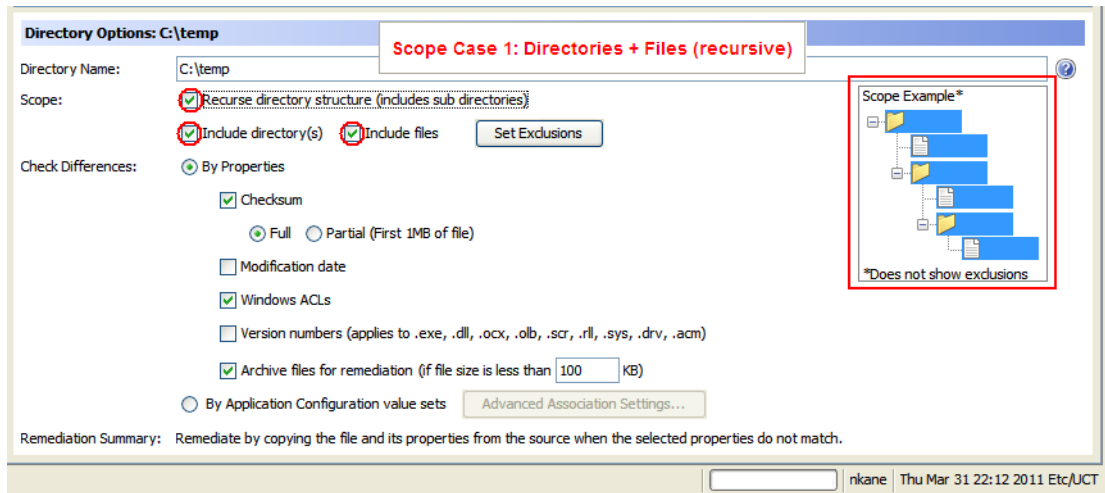


Figure 8 is an example of options required for Directories + Files. These are the default options.

Figure 8 Scope Case 2: Directories + Files (default)

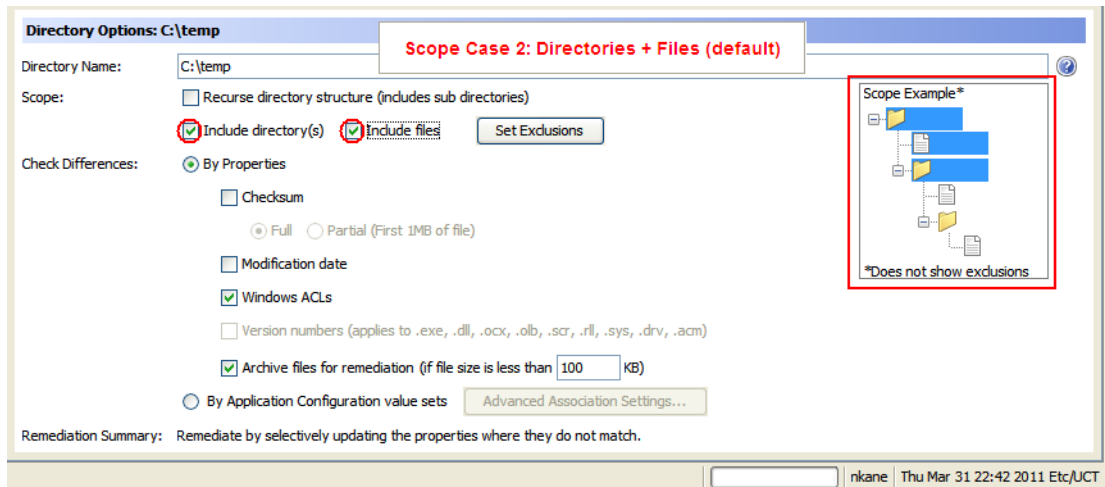


Figure 9 is an example of options required for Files Only.

Figure 9 Scope Case 3: Files Only

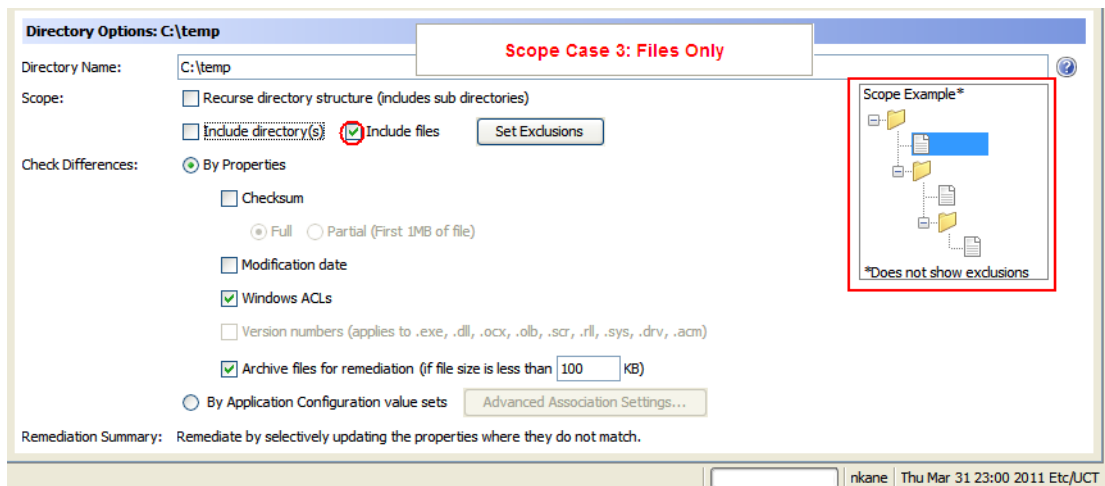


Figure 10 is an example of options required for Files (recursive).

Figure 10 Scope Case 4: Files (recursive)

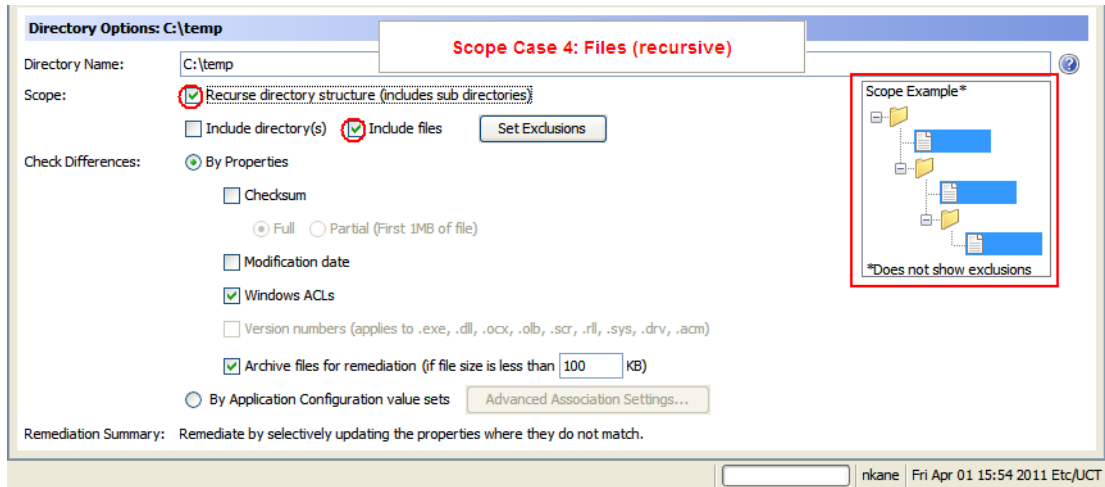


Figure 11 is an example of options required for Directories (recursive).

Figure 11 Scope Case 5: Directories (recursive)

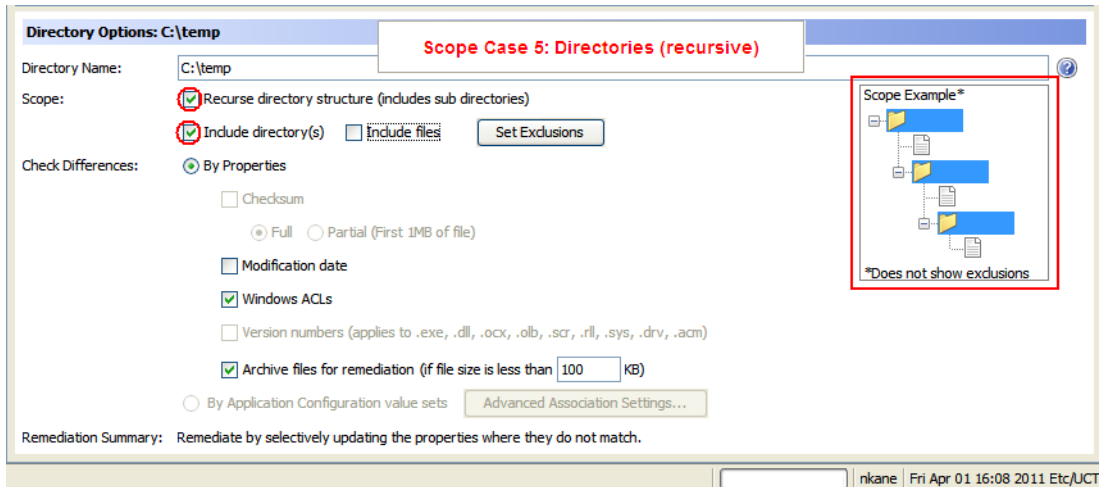


Figure 12 is an example of options required for Directory Only.

Figure 12 Scope Case 6: Directory Only

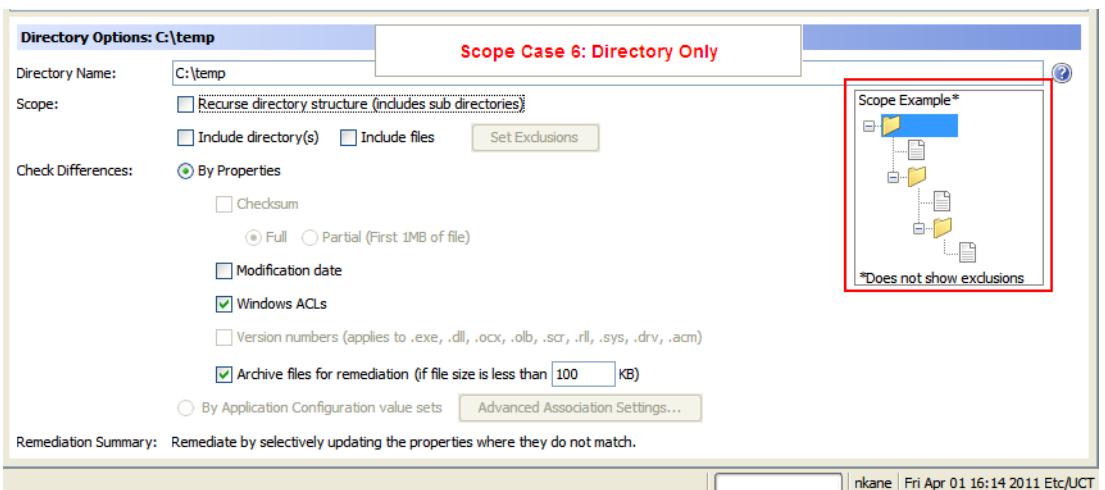


Figure 13 is an example of options required for Directories Only.

Figure 13 Scope Case 7: Directories Only

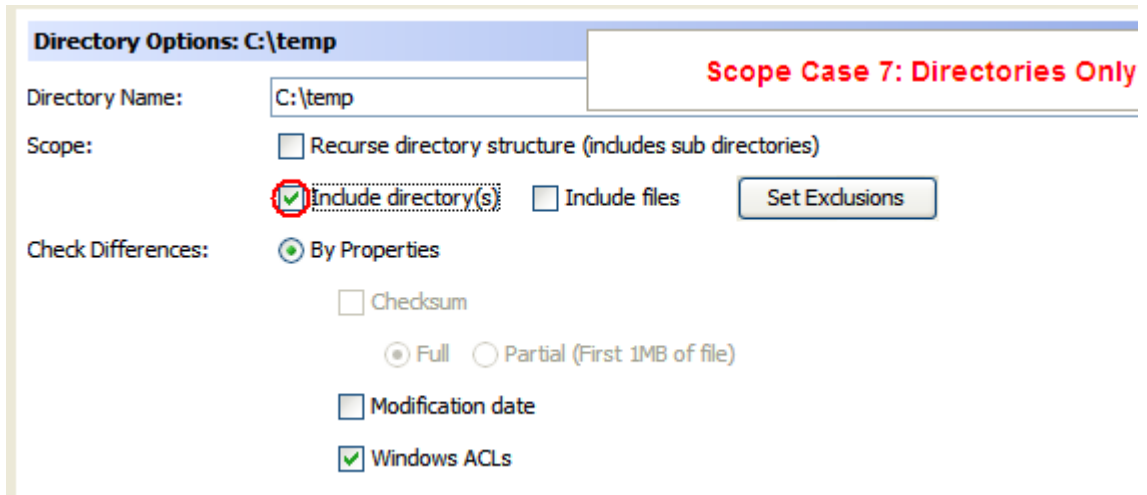
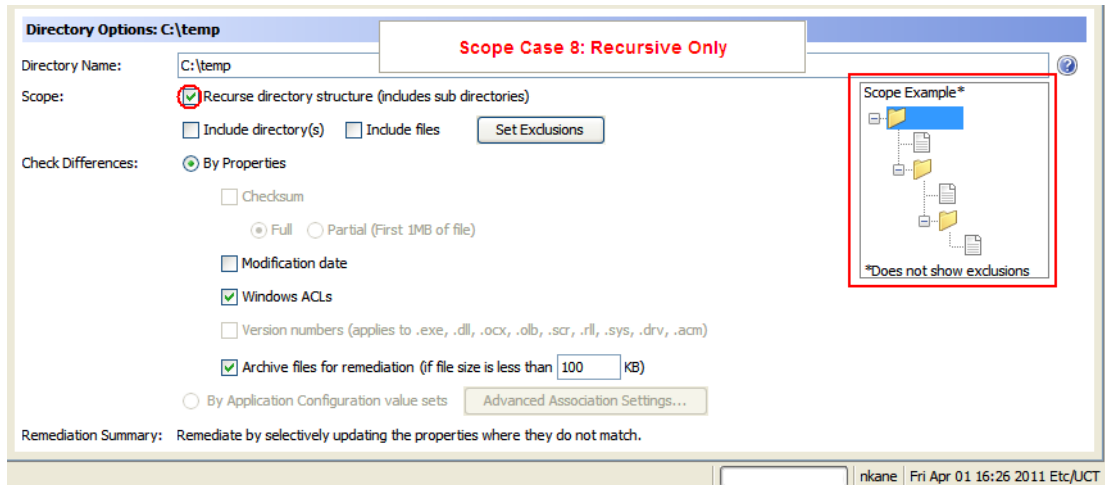


Figure 14 is an example of options required for Recursive Only.

Figure 14 Scope Case 8: Recursive Only



Ways to Add a Rule to an Audit

There are several ways you can add a rule to an audit.

You can:

- (Recommended) Link to an existing audit policy. See [Linking an Audit Policy to an Audit or a Snapshot Specification](#) on page 81 and [Linking Audit Policies to a Master Audit Policy](#) on page 82.
- Import an audit policy. See [Importing Audit Policy Rules](#) on page 83.
- Select a rule inside an audit.

To configure a file rule:

- 1 Create the new audit using one of the methods in [Creating an Audit](#) on page 19. If you want to create this rule for a snapshot specification, see [Creating a Snapshot Specification](#) on page 108.
- 2 Specify the source of the reference data against which target values will be compared.



Best Practice: The source should represent the ideal configuration of the server or its applications.

- a In the Audit window, in the Views pane, select **Source**.
- b In the Source pane, specify the source of the reference data against which target values will be compared, such as **No Source**, **Server**, **Snapshot-One for All Targets**, or **Snapshot Specification-Most Recent per target**. If you select a snapshot, you will only be able to compare those files captured in the snapshot. Some audit rules, such as Application Configurations and Windows Users and Groups, must have a source.

Depending on which Source you select, one of the following windows appears:

If you select **Server**, the Select Server window appears.

If you select **Snapshot-One for All Targets**, the Select Snapshot window appears.

If you select **Snapshot Specification-Most Recent per target**, the Select Snapshot Specification window appears.

- c Make your selection and click **OK** to save your settings and close the selection window.

3 Select the file rule:

- a In the Audit window, in the Views pane, select **Rules** ► **Files**.

(Recommended) In the Rules content pane, click  to open the Select an Audit Policy window. Select a policy and then click **OK**.



Best Practice: This selection allows you to create a *linked rule*, which is a link to an existing audit policy. This means that any changes made to the policy will also be reflected in this audit rule.

Or

- b (Optional) If you want to create an *unlinked rule*, check **Enable unlinked rules (prevents linking to predefined audit policies)**.

In the Rules content pane, click **Import Rules** to open the Select an Audit Policy window. Select a policy and then click **OK**.


Or

- c (Optional) In an audit or audit policy, check **Enable unlinked rules (prevents linking to predefined audit policies)**.

Click  to open the Select Files window. Expand the file system and select files or directories. Click **OK** to add selected rules to the audit.

4 Select the files and directories you want to audit:

- a In the Audit window, in the Views pane, select **Rules** ► **Files**.



In the Source Server content pane, click  to open the Select Files window.

- b In the Available for Audit section, expand the top level node and select a folder or file to apply the rule to.
- c Make your selections and then click **Select** to save your settings and close the Select Files window.


Or

- a In the Audit window, in the Views pane, select **Rules** ► **Files**.

In the Source Server content pane, select a file or directory to modify the File Options or the Directory Options in the details pane.

- b (Optional) For folders, you can select a file/directory wildcard option to specify files and directories that you want to include or exclude from the audit.
- c Click  to add a new rule or click  to remove a rule. For more information on how to enter files and directories and how this affects the audit, see [File Inclusion and Exclusion Rules](#) on page 69.

- 5 (Optional) If you want to use an application configuration to compare configuration files, select **By Application Configuration Value Sets** and then click **Advanced Association Settings**.

In the AppConfig File Comparison Associations window, in the AppConfig Templates list, select the template you want to use to compare a source and a target configuration file. In the Associated Files section, use the default path to the source configuration file or edit the path. Click  to add another path to a source configuration file that you want to compare with a configuration file on the target.

When you are finished, click **OK**.

- 6 To finish configuring the audit, set the target servers, schedule, and notification for the audit.
- 7 To save the audit, from the **File** menu, select **Save**. You can also save the Audit as a policy. For more information, see [Saving an Audit or a Snapshot Specification as an Audit Policy](#) on page 83.
- 8 To run the audit, from the **Actions** menu, select **Run Audit**. For more information about running an audit, see [Creating an Audit Policy](#) on page 79.

Comparing Files in Audits with Configuration Templates

Another way you can audit files on a target server is to compare them with a source server file, using application configuration (AppConfig) templates as the basis of the comparison.

Configuration templates model the structure of a configuration file and determine its contents and organization. When you use configuration templates in an audit's file rule to compare files, the audit uses the configuration template to filter both the source and the target files' contents for the comparison. This ensures that you are comparing only the value sets defined in the template when you run the audit and compare the files.

For example, you might want to compare the `/etc/passwd` file on several target servers to make sure they contain only the values defined in the `/etc/passwd` file on a *golden server* that you know has acceptable values. Using the configuration file comparison feature, you select a configuration template that models the `/etc/passwd` file (`passwd.tpl`) and associate that configuration template with the actual `passwd` file on both the golden source server and the servers that are targeted by the audit.

You create the association by selecting the template and then by entering the file pathname to where the file exists on the target servers. You can also compare multiple files using this feature. For example, you can select a directory that you know contains several configuration files to compare and you can associate configuration templates with directories you know contain the files you want to compare.

To use the configuration file comparison feature in an audit:

- 1 Create the new audit using one of the methods in [Creating an Audit](#) on page 19.
- 2 Specify the source of the reference data against which target values will be compared.



Best Practice: The source should represent the ideal configuration of the server or its applications.


- a In the Audit window, in the Views pane, select **Source**.
- b In the Source pane, specify the source of the reference data against which target values will be compared, such as **No Source**, **Server**, **Snapshot-One for All Targets**, or **Snapshot Specification-Most Recent per target**. If you select a snapshot, you will only be able to compare those files captured in the snapshot. Some audit rules, such as Application Configurations and Windows Users and Groups, must have a source.


Depending on which Source you select, one of the following windows appears:

If you select **Server**, the Select Server window appears.

If you select **Snapshot-One for All Targets**, the Select Snapshot window appears.

If you select **Snapshot Specification-Most Recent per target**, the Select Snapshot Specification window appears.

- c Make your selection and click **OK** to save your settings and close the selection window.
- 3 In the Audit window, in the Views pane, select **Rules** ► **Files**.
- 4 In the Audit window, in the details pane, select **By Application Configuration Value Sets** and then click **Advanced Association Settings**.
- 5 In the AppConfig File Comparison Associations window, in the AppConfig Templates list, select the template you want to use to compare a source and a target configuration file. In the Associated Files section, use the default path to the source configuration file or edit the path. Click  to add another path to a source configuration file that you want to compare with a configuration file on the target.
- 6 In the Associated Files section, enter the pathname to where the actual source and target configuration file exists on both the source and the target servers.

Note: The files you want to compare with the configuration template must exist in the same directory.
- 7 (Optional) If you want to make more than one association for a template, click  to add another directory. Each directory you add applies to whatever template you have selected in the AppConfig Templates section. You can make as many associations as you want in this window.
- 8 When you are finished, click **OK**.
- 9 To finish configuring the audit, set the target servers, the schedule, and the notification for the audit.
- 10 To save the audit, from the **File** menu, select **Save**. You can also save the Audit as a policy. For more information, see [Saving an Audit as an Audit Policy](#) on page 80.
- 11 To run the audit, from the **Actions** menu, select **Run Audit**. For more information about running an audit, see [Creating an Audit Policy](#) on page 79.

Configuring Hardware Rule

Configuring a hardware rule allows you to audit the following information about a server's hardware:

- **Interfaces:** Compares duplex mismatch and all network interfaces on a server.
- **CPU:** Compare CPU type and specification of target server.
- **Memory:** Compare memory of the target server.
- **Storage:** Compare storage capacity on the target server.
- **Interfaces:** Compare all network interfaces attached to the device.



If you are auditing or taking a snapshot of the Hardware rule on a server that just recently had the SA Agent installed on it, it is possible that the hardware has not been fully registered with the Model Repository, and you will not be able to audit or snapshot accurate hardware information. (The SA Agent registers hardware usually within 24 hours after agent installation.) If you are not sure, contact your SA Administrator or the person who installed the SA Agent on the server. See the *SA User Guide: Server Automation* for instructions on how to register a server's hardware manually.

To configure hardware rules:

- 1 Create the new audit using one of the methods for creating an audit listed in [Creating an Audit](#) on page 19. (If you want to create this rule for a snapshot specification, see [Creating a Snapshot Specification](#) on page 108.)
- 2 Select an Audit Source: Server, Snapshot, Snapshot Specification, or No Source. (Some audit rules, such as Application Configuration and Windows User's and Groups, must have a source.)
- 3 In the Audit window, from the View pane, select Rules ► Hardware.
- 4 In the content pane of the Audit window, expand the top level node in the Available for Audit section and select a hardware category to create a rule for.
- 5 Click the right arrow button to move the hardware item into the Selected for Audit section. All items that you select will be used to audit or snapshot the target server.
- 6 To finish configuring the audit, set the target servers, the schedule, and the notification for the audit.
- 7 To save the audit, from the **File** menu, select **Save**. You can also save the Audit as a policy. For more information, see [Saving an Audit or a Snapshot Specification as an Audit Policy](#) on page 83.
- 8 To run the audit, from the **Actions** menu, select **Run Audit**. For more information about running an audit, see [Creating an Audit Policy](#) on page 79.

Configuring IIS Metabase Rule

The IIS Metabase audit rule allows you to select IIS Metabase objects and objects folders to compare in your audit. The audit will capture IIS Metabase object property information such as ID, name, path, attributes, and so on.

If you are checking ACLs for Metabase rule, and the user and group ACL does not exist, then after the audit is run and after remediation, if user and group does not exist on target a temporary user and group will be created as unknown name. The next time you run the audit, it shows up as unknown, which shows name other than the source user.

Additionally, if you create an IIS Metabase rule from a source server and the metabase object selected for the rule inherits its values from a parent Metabase object, differences will show after an audit is run. For example, if you remediate once and then rerun the audit, if the source key was not inherited and the attribute has an IED when it gets created on target server, the object will be created based on parent key inheritance. When you rerun the audit, the results will show the IED as a difference for the object's attribute.

For more information on remediation, see [Audit Results](#) on page 84.



If you want to audit Microsoft IIS 7.0 on a Windows 2008 server, create and configure the IIS 7.0 rule in your audit. See [Configuring IIS 7.0 Rule](#) on page 55.

To configure IIS Metabase rules:


- 1 Create the new audit using one of the methods for creating an audit listed at [Creating an Audit](#) on page 19. (If you want to create this rule for a snapshot specification, see [Creating a Snapshot Specification](#) on page 108.)
- 2 Select an Audit Source: Server, Snapshot, Snapshot Specification, or No Source. (Some audit rules, such as Application Configuration and Windows User's and Groups, must have a source.)
- 3 In the Audit window, from the View pane, select Rules ► IIS Metabase.
- 4 In the content pane of the Audit window, expand the top level node in the Available for Audit section and select an IIS Metabase folder or object to create a rule for. (You can select any metabase folder or object for the rules, but you cannot select the root folder to use as a rule.)
- 5 Click the right arrow button to move the IIS Metabase folder or object into the Selected for Audit section. All items you select will be used to audit or snapshot the target server.
- 6 To finish configuring the audit, set the target servers, the schedule, and the notification for the audit.
- 7 To save the audit, from the **File** menu, select **Save**. You can also save the Audit as a policy. For more information, see [Saving an Audit or a Snapshot Specification as an Audit Policy](#) on page 83.
- 8 To run the audit, from the **Actions** menu, select **Run Audit**. For more information about running an audit, see [Creating an Audit Policy](#) on page 79.

Configuring IIS Rule

The Microsoft Internet Information Server rule allow you to use real time information about IIS for your audit, such as a Windows server, such as server name, server type, server state, log file path, document file path, and so on.

To configure the Internet Information Server rule:

- 1 Create the new audit using one of the methods in [Creating an Audit](#) on page 19. (If you want to create this rule for a snapshot specification, see [Creating a Snapshot Specification](#) on page 108.)
- 2 Select an Audit Source: Server, Snapshot, Snapshot Specification, or No Source. (Some audit rules, such as Application Configuration and Windows User's and Groups, must have a source.)
- 3 In the Audit window, from the View pane, select Rules ► Internet Information Server.
- 4 In the content pane of the Audit window, expand the top level node in the Available for Audit section and select an Internet Information Server rule that you want to create a rule from.
- 5 Click the right arrow button to move the rule object into the Selected for Audit section. All Internet Information Server rules that you configure will be audited on the target servers or snapshot specification.
- 6 For each rule, select one of the following check types:
 - **Property Values:** A values-based check that checks individual properties of the target object. For this type of check, each object requires that you build an expression that defines properties related to the object using the drop down lists at the bottom of the rule window. You can specify a unique operator which, depending on the type of object, can be a String, a Number (integer or float), Boolean (comparing values of 'true' and 'false'), Date (a date compare, not a time of day compare), or an Array.

- **Equivalent to source:** A comparison check that performs a one to one comparison between the object on the source vs. the target servers. In this type of check, the values of each property selected from both the source and target servers must match exactly for the object to be compliant.
 - **Non-existence:** Checks for the non-existence of an object, to determine if it does not exist on the target server. If the object exists on the target server, then the rule is out of compliance.
- 7 You can also configure a rule based on a wildcard search by selecting the Wildcard rule object *. When you select this object, in the rule configuration section at the bottom of the window displays a Name field, into which you can type a name (primary key) that will be searched on the target server. For example, you could enter simply * which would match everything on the target, P* would match all objects that begin with a capital P, while *P would match all elements ending with uppercase character 'P'. After you enter a name or wildcard string, you can configure the rule parameters as you did in step 6. It is important to notice that when using wildcard, all matching objects are restricted by the rule configuration. This type of audit rule is considered compliant if all found objects match the rule parameters.
 - 8 To finish configuring the audit, set the target servers, any rule exceptions, the schedule, and the notification for the audit.
 - 9 To save the audit, from the **File** menu, select **Save**. You can also save the Audit as a policy. See [Saving an Audit or a Snapshot Specification as an Audit Policy](#) on page 83.
 - 10 To run the audit, from the **Actions** menu, select **Run Audit**. See [Creating an Audit Policy](#) on page 79.

Configuring IIS 7.0 Rule

In SA 9.10, you can create audit and snapshot specification rules for Microsoft IIS 7.0 running on Windows 2008. You can expand and browse IIS 7.0 Application Pools, Web Sites, and features and add them to your audits or snapshot specifications to determine whether they meet your organization's compliance standards. After your audit or snapshot has run, you can view the results and remediate any discrepancies found (with some exceptions).

For example, you might want to audit several Windows 2008 servers running IIS 7.0 to make sure that Anonymous Authentication is enabled on each server.

To perform this compliance check, select a Windows 2008 server that has Anonymous Authentication enabled to be the *source* server of the audit. Then, configure the audit rule to check that Anonymous Authentication is enabled on all servers targeted by the audit.

When you run the audit (which you can schedule on a recurring basis), the rule will check the target servers and discover if any do not have Anonymous Authentication enabled. If the audit finds any discrepancies, you can remediate those servers to enable their IIS 7.0 Anonymous Authentication.



You cannot remediate ISAPI filters for the IIS 7.0 audit rule in this release.

To configure the IIS 7.0 rule:

- 1 Create a new audit using one of the methods in [Creating an Audit](#) on page 19. (If you want to create this rule for a snapshot specification, see [Creating a Snapshot Specification](#) on page 108.)
- 2 Select an Audit Source: Server, Snapshot, Snapshot Specification, or No Source.

Some audit rule types, such as Application Configuration and Windows User's and Groups, must have a source server on which to base the rule. Some specific rules and criteria, such as checking IIS 7.0 Anonymous Authentication, also require that you select a source server. If you do not select a source server, you will be limited on the specificity of the rule.

- 3 In the Audit window, from the View pane, select Rules ► IIS 7.0.
- 4 In the content pane of the Audit window, in the Available for Audit section expand one of the IIS 7.0 elements you want to create a rule for, such as Application Pools, Sites, or Features. This may take a few moments to load if this is the first time you are loading one of the elements.
- 5 Select an element from the list and then click the right arrow button to move the rule object into the Selected for Audit section, which enables you to create a rule for the element. For example, you could expand the Authentication folder and select Anonymous Authentication, then click the right arrow button to add the selection to your audit.
- 6 For each rule, in the lower section of the audit window you can select one of the following rule criteria types:

- **Property Values:** A values-based check that checks individual properties of the target object. For this type of check, each object requires that you build an expression that defines properties related to the object using the drop down lists at the bottom of the rule window. You can specify a unique operator which, depending on the type of object, can be a String, a Number (integer or float), Boolean (comparing values of 'true' and 'false'), Date (a date compare, not a time of day compare), or an Array.

- **Equivalent to source:** A comparison check that performs a one to one comparison between the object on the source vs. the target servers. In this type of check, the values of each property selected from both the source and target servers must match exactly for the object to be compliant.


Remediation of the IIS 7.0 rule is possible only when an audit is setup with the Equivalent to source check.

- **Non-existence:** Checks for the non-existence of an object, to determine if it does not exist on the target server. If the object exists on the target server, then the rule is out of compliance.

For example, if you wanted to check that a target server (or group of servers) running IIS 7.0 has Anonymous Authentication enabled, in the bottom of the audit window, you would select:

- Property Values
- Status
- =
- Enabled

This tells the audit to find out if each target server's IIS 7.0 Anonymous Authentication is enabled.

- 7 You can also configure a rule based on a wildcard search by selecting the Wildcard rule object *. When you select this object, in the rule configuration section at the bottom of the window displays a Name field, into which you can type a name (primary key) that will be searched on the target server.

For example, you could enter simply * which would match everything on the target, P* would match all objects that begin with a capital P, while *P would match all elements ending with uppercase character 'P'.

After you enter a name or wildcard string, you can configure the rule parameters as you did in step 6.


It is important to notice that when using wildcard, all matching objects are restricted by the rule configuration. This type of audit rule is considered compliant if all found objects match the rule parameters.

- 8 To finish configuring the audit, set the target servers, any rule exceptions, the schedule, and the notification for the audit.
- 9 To save the audit, from the **File** menu, select **Save**. You can also save the Audit as a policy, which enables other users to access the rule set you create in the audit. See [Saving an Audit or a Snapshot Specification as an Audit Policy](#) on page 83.
- 10 To run the audit, from the **Actions** menu, select **Run Audit**. See [Running an Audit](#) on page 21.

Configuring Local Security Settings Rule

The Local Security Settings rule allows you to use real time information about security settings, such as password policy, audit policy, user rights, and security options in your rule.

To configure the Local Security Settings rule:

- 1 Create the new audit using one of the methods in [Creating an Audit](#) on page 19. (If you want to create this rule for a snapshot specification, see [Creating a Snapshot Specification](#) on page 108.)
- 2 Select an Audit Source: Server, Snapshot, Snapshot Specification, or No Source. (Some audit rules, such as Application Configuration and Windows User's and Groups, must have a source.)
- 3 In the Audit window, from the View pane, select Rules ► Local Security Settings.
- 4 In the content pane of the Audit window, expand the top level node in the Available for Audit section and select an Internet Information Server rule that you want to create a rule from.
- 5 Click the right arrow button to move the rule object into the Selected for Audit section. All Internet Information Server rules that you configure will be audited on the target servers or snapshot specification.
- 6 For each rule, select one of the following check types:
 - **Property Values:** A values-based check that checks individual properties of the target object. For this type of check, each object requires that you build an expression that defines properties related to the object using the drop down lists at the bottom of the rule window. You can specify a unique operator which, depending on the type of object, can be a String, a Number (integer or float), Boolean (comparing values of 'true' and 'false'), Date (a date compare, not a time of day compare), or an Array.
 - **Equivalent to source:** A comparison check that performs a one to one comparison between the object on the source vs. the target servers. In this type of check, the values of each property selected from both the source and target servers must match exactly for the object to be compliant.
 - **Non-existence:** Checks for the non-existence of an object, to determine if it does not exist on the target server. If the object exists on the target server, then the rule is out of compliance.
- 7 You can also configure a rule based on a wildcard search by selecting the Wildcard rule object . When you select this object, in the rule configuration section at the bottom of the window displays a Name field, into which you can type a name (primary key) that will be searched on the target server.

For example, you could enter simply * which would match everything on the target, P* would match all objects that begin with a capital P, while *P would match all elements ending with uppercase character 'P'.

After you enter a name or wildcard string, you can configure the rule parameters as you did in step 6.


It is important to notice that when using wildcard, all matching objects are restricted by the rule configuration. This type of audit rule is considered compliant if all found objects match the rule parameters.

- 8 To finish configuring the audit, set the target servers, any rule exceptions, the schedule, and the notification for the audit.
- 9 To save the audit, from the **File** menu, select **Save**. You can also save the Audit as a policy. See [Saving an Audit or a Snapshot Specification as an Audit Policy](#) on page 83.
- 10 To run the audit, from the **Actions** menu, select **Run Audit**. See [Running an Audit](#) on page 21.

Configuring Registered Software Rule

The Registered Software rule allows you to audit use all installed packages or patches actually installed on a source server to build your rule, whether or not the patches or packaged have been registered by the SA model repository.

To configure the Registered Software rule:

- 1 Create the new audit using one of the methods in [Creating an Audit](#) on page 19. (If you want to create this rule for a snapshot specification, see [Creating a Snapshot Specification](#) on page 108.)
- 2 Select an Audit Source: Server, Snapshot, Snapshot Specification, or No Source. (Some audit rules, such as Application Configuration and Windows User's and Groups, must have a source.)
- 3 In the Audit window, from the View pane, select Rules ► Registered Software.
- 4 In the content pane of the Audit window, expand the top level node in the Available for Audit section and select a patch or a package that you want to create a rule from.
- 5 Click the right arrow button to move the rule object into the Selected for Audit section. All rules that you configure will be audited on the target servers or snapshot specification.
- 6 For each rule, select one of the following check types:
 - **Property Values:** A values-based check that checks individual properties of the target object. For this type of check, each object requires that you build an expression that defines properties related to the object using the drop down lists at the bottom of the rule window. You can specify a unique operator which, depending on the type of object, can be a String, a Number (integer or float), Boolean (comparing values of 'true' and 'false'), Date (a date compare, not a time of day compare), or an Array.
 - **Equivalent to source:** A comparison check that performs a one to one comparison between the object on the source vs. the target servers. In this type of check, the values of each property selected from both the source and target servers must match exactly for the object to be compliant.
 - **Non-existence:** Checks for the non-existence of an object, to determine if it does not exist on the target server. If the object exists on the target server, then the rule is out of compliance.
- 7 You can also configure a rule based on a wildcard search by selecting the Wildcard rule object . When you select this object, in the rule configuration section at the bottom of the window displays a Name field, into which you can type a name (primary key) that will be searched on the target server. For example, you could enter simply * which would match everything on the target, P* would match all objects that begin with a capital P, while *P would match all elements ending with uppercase character 'P'.

After you enter a name or wildcard string, you can configure the rule parameters as you did in step 6.

It is important to notice that when using wildcard, all matching objects are restricted by the rule configuration. This type of audit rule is considered compliant if all found objects match the rule parameters.

- 8 To finish configuring the audit, set the target servers, any rule exceptions, the schedule, and the notification for the audit.
- 9 To save the audit, from the **File** menu, select **Save**. You can also save the Audit as a policy. See [Saving an Audit or a Snapshot Specification as an Audit Policy](#) on page 83.
- 10 To run the audit, from the **Actions** menu, select **Run Audit**. See [Running an Audit](#) on page 21.

Configuring Storage Rule

The storage rule allows you audit servers for storage devices and SAN devices and connections in your data center, if your core is configured to connect to SE.



In order to audit and snapshot SAN objects, Storage Essentials (SE) version 6.1.1 or later is required and the Server Automation SE Connector component must be installed and configured on your SA core. For more information, see your SA administrator or the Storage Visibility and Automation documentation.

To configure the storage rule:

- 1 Create the new audit using one of the methods in [Creating an Audit](#) on page 19. (If you want to create this rule for a snapshot specification, see [Creating a Snapshot Specification](#) on page 108.)
- 2 Select an Audit Source: Server, Snapshot, Snapshot Specification, or No Source. (Some audit rules, such as Application Configuration and Windows User's and Groups, must have a source.)
- 3 In the Audit window, from the View pane, select Rules ► Storage.
- 4 In the content pane of the Audit window, expand the top level node in the Available for Audit section and select a Storage rule that you want to create a rule from. Each storage audit rules check for the acceptable values for each category. You can configure the rule to check for minimum, maximum, or exact numbers.
 - **Unmounted Volume Capacity:** Acceptable total capacity of unmounted volumes in bytes.
 - **Unmounted Volume Count:** Acceptable number of unmounted volumes.
 - **Fabrics:** Acceptable number of fabrics.
 - **FCA:** Acceptable number of Fibre Channel Adapters (FCAs).
 - **Initiator Ports:** Acceptable number of initiator ports
 - **Switches:** Acceptable number of SAN switches.
 - **Target Ports:** Acceptable number of target ports.
 - **RAID Types:** Acceptable RAID types on the target storage array. (**Note:** The audit will fail if this rule is selected and no RAID type is specified.)



The compliance rules that involve ports, switches, or fabrics, check active ports only. These types of compliance rules do not check for physical port connectivity.


- 5 Click the right arrow button to move the rule object into the Selected for Audit section. All storage rules that you configure will be audited on the target servers or snapshot specification.
- 6 For each rule, select one of the following check property:
 - An operator, such as equal to (=), less than (<), less than or equals to (<=), and so on.
 - A value, depending on the rule type, such as a number.

- 7 To finish configuring the audit, set the target servers, any rule exceptions, the schedule, and the notification for the audit.
- 8 To save the audit, from the **File** menu, select **Save**. You can also save the Audit as a policy. See [Saving an Audit or a Snapshot Specification as an Audit Policy](#) on page 83.
- 9 To run the audit, from the **Actions** menu, select **Run Audit**. See [Running an Audit](#) on page 21.

Configuring Windows .NET Framework Configurations Rule

The Windows .NET Framework Configuration rule allows you to use time information about Assembly Cache and Configured Assembly List, such as assembly name, version, locale, public key token, cache file (GAC or ZAP), processor architecture, custom, and file name in your audits.

To configure the Windows .NET Framework Configuration rule:

- 1 Create the new audit using one of the methods in [Creating an Audit](#) on page 19. (If you want to create this rule for a snapshot specification, see [Creating a Snapshot Specification](#) on page 108.)
- 2 Select an Audit Source: Server, Snapshot, Snapshot Specification, or No Source. (Some audit rules, such as Application Configuration and Windows User's and Groups, must have a source.)
- 3 In the Audit window, from the View pane, select Rules ► Windows .NET Framework Configuration.
- 4 In the content pane of the Audit window, expand the top level node in the Available for Audit section and select a Windows .NET Framework Configuration rule that you want to create a rule from.
- 5 Click the right arrow button to move the rule object into the Selected for Audit section. All Windows .NET Framework Configuration rules that you configure will be audited on the target servers or snapshot specification.
- 6 For each rule, select one of the following check types:
 - **Property Values:** A values-based check that checks individual properties of the target object. For this type of check, each object requires that you build an expression that defines properties related to the object using the drop down lists at the bottom of the rule window. You can specify a unique operator which, depending on the type of object, can be a String, a Number (integer or float), Boolean (comparing values of 'true' and 'false'), Date (a date compare, not a time of day compare), or an Array.
 - **Equivalent to source:** A comparison check that performs a one to one comparison between the object on the source vs. the target servers. In this type of check, the values of each property selected from both the source and target servers must match exactly for the object to be compliant.
 - **Non-existence:** Checks for the non-existence of an object, to determine if it does not exist on the target server. If the object exists on the target server, then the rule is out of compliance.
- 7 You can also configure a rule based on a wildcard search by selecting the Wildcard rule object . When you select this object, in the rule configuration section at the bottom of the window displays a Name field, into which you can type a name (primary key) that will be searched on the target server.

For example, you could enter simply * which would match everything on the target, P* would match all objects that begin with a capital P, while *P would match all elements ending with uppercase character 'P'.

After you enter a name or wildcard string, you can configure the rule parameters as you did in step 6.

It is important to notice that when using wildcard, all matching objects are restricted by the rule configuration. This type of audit rule is considered compliant if all found objects match the rule parameters.

- 8 To finish configuring the audit, set the target servers, any rule exceptions, the schedule, and the notification for the audit.
- 9 To save the audit, from the **File** menu, select **Save**. You can also save the Audit as a policy. See [Saving an Audit or a Snapshot Specification as an Audit Policy](#) on page 83.
- 10 To run the audit, from the **Actions** menu, select **Run Audit**. See [Running an Audit](#) on page 21.

Configuring Windows Registry Rule

The Windows Registry rule allows you to select Windows Registry folders and keys to compare in your audit. The audit compares the selected registry folders and keys and determines if these keys and folders exist on the target servers.

There are two categories of Windows Registry rules that you can define in an audit or snapshot specification. The following categories appear in the Available for Audit section of the Audit window:

- **Windows Registry:** These are comparison-based rules, which enable you to select a Windows Registry key or folder from the source of the audit or snapshot specification and compare these with the target servers. The purpose for this kind of rule is to determine if the Windows Registry key or folder exists and its properties. You cannot set a target or remediation value in the rule.

The Windows Registry object allows you to capture registry keys, values, and subkeys. A registry key is a directory that contains registry values, where registry values are similar to files within a directory. A subkey is similar to a subdirectory. The content area in this window excludes subkeys. The audit and remediation feature supports the following Windows Registry keys: HKEY_CLASSES_ROOT, HKEY_CURRENT_CONFIG, HKEY_LOCAL_MACHINE, and HKEY_USERS.

Valid control characters audited and captured for the contents of the key entry (Data) include: #x9, #xA, [#xD, #x20-#xD7FF], [#xE000-#xFFFFD], and [#x10000-#x10FFFF]. Invalid control characters cannot be stored by the SA Client and will be converted to XML entities and will display as &#. For example, if the data value is 00 00 (in bytes), � will display in the audit or snapshot specification results.

You can also choose to compare Access Control Levels (ACLs) for registry rule.



If you are checking ACLs for Registry rule, and the user and group ACL does not exist, then after the audit is run and after remediation, if user and group does not exist on target a temporary user and group will be created as unknown name. The next time you run the audit it shows up as unknown, which shows name other than the source user. For more information on remediation, see [Audit Results](#) on page 84.

To configure Windows Registry audit rules:

- 1 Create the new audit using one of the methods for creating an audit listed in [Creating an Audit](#) on page 19. (If you want to create this rule for a snapshot specification, see [Creating a Snapshot Specification](#) on page 108.)
- 2 Select an Audit Source: Server, Snapshot, Snapshot Specification, or No Source. (Some audit rules, such as Application Configuration and Windows User's and Groups, must have a source.)
- 3 In the Audit window, from the View pane, select Rules ► Windows Registry.
- 4 In the content pane of the Audit window, expand the top level node in the Available for Audit section and select a Windows Registry folder or key to create a rule for.
- 5 Click the right arrow button to move the Windows Registry folder or key into the Selected for Audit section. All items that you select will be used to audit or snapshot the target server.
- 6 For each registry entry key rule you create, you can set two options to include when the audit checks the target:

- Also Compare Contents of Sub-Keys: Will evaluate all subkeys belonging to the selected registry key.
 - Also Compare ACLs: Will also compare ACLs of the selected registry key.
 - Use case-insensitive compare:
- 7 To finish configuring the audit, set the target servers, the schedule, and the notification for the audit.
 - 8 To save the audit, from the **File** menu, select **Save**. You can also save the Audit as a policy. See [Saving an Audit or a Snapshot Specification as an Audit Policy](#) on page 83.
 - 9 To run the audit, from the **Actions** menu, select **Run Audit**. See [Running an Audit](#) on page 21.

Configuring Windows Services Rule

The windows service rule allows you to select windows services to compare in your audit or snapshot specification. The audit or snapshot specification compares the selected services with services on the target servers to determine if the services exist and if the services are started, stopped or disabled.

There are two categories of windows services rules that you can define in an audit or snapshot specification. The following rule appear in the Available for Audit section of the Audit window:

- **Windows Services:** These comparison-based rules enable you to select a service from the source of the audit or snapshot specification and compare them with the target servers. The purpose of windows services rule is to determine if the service exists and its settings. You cannot set a target or remediation value with this type of rule.


To configure windows services rules:

- 1 Create the new audit using one of the methods for creating an audit listed in [Creating an Audit](#) on page 19. (If you want to create this rule for a snapshot specification, see [Creating a Snapshot Specification](#) on page 108.)
- 2 Select an Audit Source: Server, Snapshot, Snapshot Specification, or No Source. (Some audit rules, such as Application Configuration and Windows User's and Groups, must have a source.)
- 3 In the Audit window, from the View pane, select Rules ► Windows Services.
- 4 In the content pane of the Audit window, expand the top level node in the Available for Audit section and select a windows services to create a rule for. (You can select any available service for the rule, but you cannot select the root folder for all services.)
- 5 Click the right arrow button to move the selected windows services into the Selected for Audit section. All items that you select will be used to audit or snapshot on the target server.
- 6 To finish configuring the audit, set the target servers, the schedule, and the notification for the audit.
- 7 Save the audit.
- 8 To run the audit, from the **Actions** menu select **Run Audit**. See [Running an Audit](#) on page 21.

Configuring Windows/UNIX Users and Groups Rule

The Windows or Unix Users and Groups rule allows you to access local users and groups information from Windows and Unix servers.

To configure the Users and Groups rule:

- 1 Create the new audit using one of the methods in [Creating an Audit](#) on page 19. (If you want to create this rule for a snapshot specification, see [Creating a Snapshot Specification](#) on page 108.)
- 2 Select an Audit Source: Server, Snapshot, Snapshot Specification, or No Source. (Some audit rules, such as Application Configuration and Windows User's and Groups, must have a source.)
- 3 In the Audit window, from the View pane, select Rules ► Windows/Unix Users and Groups.
- 4 In the content pane of the Audit window, expand the top level node in the Available for Audit section and select a Users and Groups rule that you want to create a rule from.
- 5 Click the right arrow button to move the rule object into the Selected for Audit section. All Users and Groups rules that you configure will be audited on the target servers or snapshot specification.
- 6 For each rule, select one of the following check types:
 - **Property Values:** A values-based check that checks individual properties of the target object. For this type of check, each object requires that you build an expression that defines properties related to the object using the drop down lists at the bottom of the rule window. You can specify a unique operator which, depending on the type of object, can be a String, a Number (integer or float), Boolean (comparing values of 'true' and 'false'), Date (a date compare, not a time of day compare), or an Array. For some property types you can select the values from the 'value selector box'.
 - **Equivalent to source:** A comparison check that performs a one to one comparison between the object on the source vs. the target servers. In this type of check, the values of each property selected from both the source and target servers must match exactly for the object to be compliant.
 - **Non-existence:** Checks for the non-existence of an object, to determine if it does not exist on the target server. If the object does exist on the target server, then the rule is out of compliance. The rule is considered compliant if no objects are found.
- 7 You can also configure a rule based on a wildcard search by selecting the Wildcard rule object *. When you select this object, in the rule configuration section at the bottom of the window displays a Name field, into which you can type a name (primary key) that will be searched on the target server. For example, you could enter simply * which would match everything on the target, P* would match all objects that begin with a capital P, while *P would match all users with name ending with uppercase character 'P'.

After you enter a name or wildcard string, you can configure the rule parameters as you did in step 6.

It is important to notice that when using wildcard, all matching objects are restricted by the rule configuration. This type of audit rule is considered compliant if all found objects match the rule parameters.
- 8 To finish configuring the audit, set the target servers, any rule exceptions, the schedule, and the notification for the audit.
- 9 To save the audit, from the **File** menu, select **Save**. You can also save the Audit as a policy. See [Saving an Audit or a Snapshot Specification as an Audit Policy](#) on page 83.
- 10 To run the audit, from the **Actions** menu, select **Run Audit**. See [Running an Audit](#) on page 21.

Configuring Compliance Checks

If you subscribe to the BSA Essentials Subscription Services, you have access to dozens of compliance rules and their components, known by content developers as *compliance checks*.

The kinds of checks you have access to depends on your content subscription, but can include such checks as the latest patch supplements for Microsoft Windows, current regulatory compliance policies (for example, FISMA, Sarbanes-Oxley), user-created checks distributed by the content developer community, daily updated vulnerability content, and so on.





If you do not subscribe to BSA Essentials Subscription Services, you will not see any compliance checks in your audits, audit policies, snapshots, or the Compliance Check Editor. If you would like more information on content subscriptions and obtaining compliance checks, contact your BSA Essentials Subscription Services sales representative.

While each compliance check is slightly different and requires its own configuration values, the basic parameters for each check require that you define the Target Value — the expected value you want to find on the server — and an optional Remediation Value.

For more information on managing your core's compliance checks, such as editing check property data or creating compliance check groupings, see [Compliance Checks](#) on page 66.

To configure compliance checks in audits or snapshot specifications:

- 1 Create an audit or snapshot using one of the methods described in [Creating an Audit](#) on page 19. (If you want to create this rule for a snapshot specification, see [Creating a Snapshot Specification](#) on page 108.)
- 2 Select an Audit Source: Server, Snapshot, Snapshot Specification, or No Source.
- 3 In the Audit window, from the View pane expand the Rules object.
- 4 Select the Compliance Checks  rule.
- 5 In the content pane of the Audit window (right side of window), click the Add  button.
- 6 In the Select Check window, from the Browse tab, you can browse for the compliance checks categories and select a check for the audit or snapshot.

Alternately, you can select the Search tab and search for check by name. The check search tool searches on the name of a check and any words in a check's description. For example, if you wanted to find all rules that check for maximum password length, you could enter `max password` in the Keywords field.

The Advanced search option allows you to set more specific parameters to find checks.

- 7 When you select a check (or multiple checks using CTRL or SHIFT + click), click **OK** to add the checks to your audit.


- 8 Select the check and then define or set the following parameters:

Input Value

Some custom checks require an input value as part of the configuration of the target value. For those checks, you will need to specify a success or failure which you can set to true or false. The Description section of the audit rule explains the recommended values.

Target Value

Specify the value that you expect to be on the target server or servers of the audit, or the value you want to capture in a snapshot. You can change the following parameters:

- **Operator:** To build an expression from the output of the script, choose an Operator, such as equals (=), not equals (<>), less than (<), greater than (>), and so on.
- **Reference:** Choose the source of the script output.
- **Source:** This will use the value from the source server and compare that value to with the value found on the target server or servers.
- **Value:** Enter your own value. This option uses the value you enter and compares it with the value returned on the target server. You can get the value from the source server if you click the eyedropper  icon. The returned value is displayed in the text box, which you can accept as is or edit to your liking.
- **Server Attribute:** Select to compare a server attribute located on the source server.
- **Custom Attribute:** Select to compare a custom attribute found on the target server.

Remediation Value

Each remediation value setting will be different depending on the type of rule, so choose accordingly.

- 9 To finish configuring the audit, set the target servers, the schedule, and the notification for the audit.
- 10 To save the audit, from the **File** menu, select **Save**. You can also save the Audit as a policy. See [Saving an Audit or a Snapshot Specification as an Audit Policy](#) on page 83.
- 11 To run the audit, from the **Actions** menu, select **Run Audit**. See [Running an Audit](#) on page 21.

Renaming Compliance Checks

You can easily rename instances of compliance checks in an audit, audit policy, or snapshot specification using the right-click menu.

For information on renaming compliance checks and editing their properties, see [Compliance Checks](#) on page 66.

To rename a compliance check name:

- 1 In the navigation pane, select Library ► By Type ► Audit and Remediation ► and open an audit, audit policy, or snapshot specification.
- 2 In the Audit (or Audit Policy or Snapshot Specification) window, from the Views pane, select a specific rule that contains custom checks. For example, Users and Groups.
- 3 In the Contents pane of the window (right side), in the Available for Audit section, select a custom rule check, right-click and select **Rename Rule** to rename the rule.






You cannot rename a rule check if the audit or snapshot specification is linked to an audit policy.

Searching for Compliance Checks from the Audit/Snapshot Specification Window

Since your SA core can potentially contain dozens, if not hundreds, of compliance checks, you can use the search tool inside the Audit or Snapshot Specification window to find the checks you want.

To search for compliance checks from inside an audit or snapshot specification:

- 1 In the Audit or Snapshot Specification window, from the View pane expand the Rules object.
- 2 Select the Compliance Checks  rule.
- 3 In the content pane of the window (right side), click **Add** .
- 4 In the Select Check window, from the Browse tab, you can browse for the compliance checks categories and select a check for the audit or snapshot.
- 5 Select the Search tab to search for checks by name. The check search tool searches on the name of a check and any words in a check's description. For example, if you wanted to find all rules that check for maximum password length, you could enter `max password` in the Keywords field.
- 6 Click the Advanced Search link to build more specific search criteria. Advanced search allows to look for a text string plus restrict the query to values in the check's properties, such as Security Level, External ID, Platforms, and Test ID. Click  to add additional advanced search parameters.
For information on how to add a Test ID, Security Level, or External ID to your compliance check properties, see [Editing Compliance Check Properties](#) on page 67.
- 7 To execute the search, click **Search**.
- 8 In the search results, you can select the checks you want to add to the audit or snapshot specification and then click **OK**.

Compliance Checks



You must have permissions to access the Compliance Check Editor. To obtain these permissions, contact your SA administrator or see the *SA Administration Guide* for more information.

The Compliance Check Editor allows you to browse, regroup, and edit property information (metadata) about your core's BSA Essentials Subscription Services compliance checks.

For example, your organization might require that an external numbering system be associated with all compliance checks that you run against servers in your data center. Using the Compliance Check Editor, you can add an external ID to those checks. You can also create custom groupings for checks you modify with this external ID, so that when you need to access those checks, you can easily find them in the custom folder. This external ID can also be used as search criteria for finding all checks with the ID number or string.

You can also edit information about custom check, such as changing a check's name, adding a custom security level, or modifying descriptive information about a check. For example, you can add to a check's remediation description to clarify what happens during remediation. This provides valuable information about its behavior for someone else who wants to use the check.

Editing Compliance Check Properties


The Compliance Check Editor allows you to modify a compliance check's properties, such as renaming it, adding a description, modifying its property information, adding an external ID to it, and so on.


To edit compliance check property information:

- 1 In the SA Client, from the **Tools** menu, select **Compliance Check Editor**. If you do not see the menu item, contact your SA administrator to obtain access permissions.
- 2 In the Compliance Check Editor window, in the Browse tab, expand the different Custom Checks categories to find the check you want to edit. Narrow the list by selecting an operating system in the Platform filter drop-down list.
- 3 Select the Search tab if you want to search for a check by a name or a keyword in its name and Description fields.

For example, if you want to find all rules that check for security logs, enter `security log` in the Keywords field. If you want to narrow the search further, add the keyword `size` to find all checks that audit for security log file size.

The Advanced Search option allows you to set more specific parameters to find checks. Using advanced search, you can filter by other properties such as security level, external ID, platform, or test ID.

To add additional search parameters, click .

- 4 To edit a check's property information, select the check from the Browse tab or Search tab results.
- 5 On the right side of the Compliance Check Editor, in the Properties tab, edit the following check information:
 - **Name:** Double-click inside the Name's value field to modify the check's name.
 - **Categories:** Click the "Click to edit" link to add the check to a custom folder. For example, click the link and in the Categories window, press ENTER on your keyboard and then type a name to create a new compliance check category. Click **Apply**. To create the custom grouping folder, click **Apply Changes** at the bottom of the Compliance Check Editor window. For information on creating custom grouping for your checks, see [Creating Custom Compliance Check Categories](#) on page 68.
 - **External ID:** Double-click inside the value field to add or modify an External ID.
 - **Security Level:** Double-click inside the value field to enter or modify security level for the check.
- 6 Click **Apply Changes** at the bottom of the Compliance Check Editor window to apply the modifications to the checks.
- 7 To edit a check's descriptions, select the Description, Remediation Description, or Technical Description tabs to edit the descriptive text for each.
- 8 To access the HTML editor for the description, click the edit icon .
- 9 In the HTML editor, click the HTML Edit icon at the bottom left of the description window.
- 10 Edit the HTML description.
- 11 Click **Apply**. If you want to undo any changes, from the **File** menu, select **Revert**.
- 12 Click **Apply Changes** at the bottom of the Compliance Check Editor window to apply the description modifications to the checks.

Creating Custom Compliance Check Categories

The Compliance Check Editor allows you to create your own custom categories that contain compliance checks installed on your core. For example, you can create a custom category that contains all checks that audit user and group settings on your Windows servers. Or, you might only be interested in accessing specific Linux services-related checks and can create a category that contains them.

To create custom compliance check categories:

- 1 In the SA Client, from the **Tools** menu, select **Compliance Check Editor**. If you do not see the menu item, contact your SA administrator to obtain access permissions.
- 2 In the Compliance Check Editor window, in the Browse tab, expand the different Custom Checks categories to find the check you want to edit. Narrow the list by selecting an operating system in the Platform filter drop-down list.
- 3 Select a compliance check.
- 4 In the upper right side of the Compliance Check Editor window, Properties tab, Categories row, click the “Click to edit” link.
- 5 In the Categories window, place your mouse point at the end of the main check category name and then press ENTER on your keyboard.
- 6 Type a name to create a new compliance check category. This creates a new compliance check category in the Compliance Check Editor. To add more categories, press ENTER again to start a new line and then type the name of the category. The selected check will be added to each new category.
- 7 Click **Apply**.
- 8 To create the custom grouping folder, click **Apply Changes** at the bottom of the Compliance Check Editor window.
- 9 To delete the custom category, repeat the process and delete the name of the category in the Categories window.

Restoring Compliance Checks to Defaults

If you want to restore all of your compliance checks to their default state—their original state when they were first downloaded from the BSA Essentials Subscription Services portal—use the restore defaults operation. Restore defaults deletes any customizations made to your compliance checks and then reverts them to their original released state.

To restore compliance checks to their default state:

- 1 In the SA Client, from the **Tools** menu, select **Compliance Check Editor**. If you do not see the menu item, contact your SA administrator to obtain access permissions.
- 2 In the Compliance Check Editor window, from the Edit menu, select **Restore defaults**.
The restore defaults action applies only to selected compliance checks.

Showing Deprecated Checks

For compliance checks that have been deprecated, you can choose to show them in the Compliance Check Editor.

To show deprecated checks in the Compliance Check Editor:

- 1 In the SA Client, from the **Tools** menu, select **Compliance Check Editor**. If you do not see the menu item, contact your SA administrator to obtain access permissions.
- 2 From the **View** menu, select **Show Deprecated Checks**.
- 3 Expand any of the checked categories to view any deprecated checks.
Deprecated checks display in grayed out, italic font.

Setting Inclusions & Exclusions for Checks



You can specify the files or directories that you want included in or excluded from your compliance checks.

To specify the files or directories that you want to include or exclude:

- 1 In the Audit browser, in the Views pane, expand Rules and then select Files.
- 2 In the Rules > Files content pane, in Directory Options, click **Set Exclusions**.
- 3 In the Set Includes/Excludes window, specify Include or Exclude from each drop-down list.
- 4 Click **Browse** to select files or directories from the source server or enter a file path.

Valid wildcard characters include the asterisk (*) and percent sign (%). For example, if you want to exclude all .exe files from your compliance checks, enter “*.exe”, without the quotation marks, in the Exclude field.

When you select a directory, you can recursively browse to files and sub-directories that are under that directory. You do not have to start browsing from your c: directory or from the root directory.

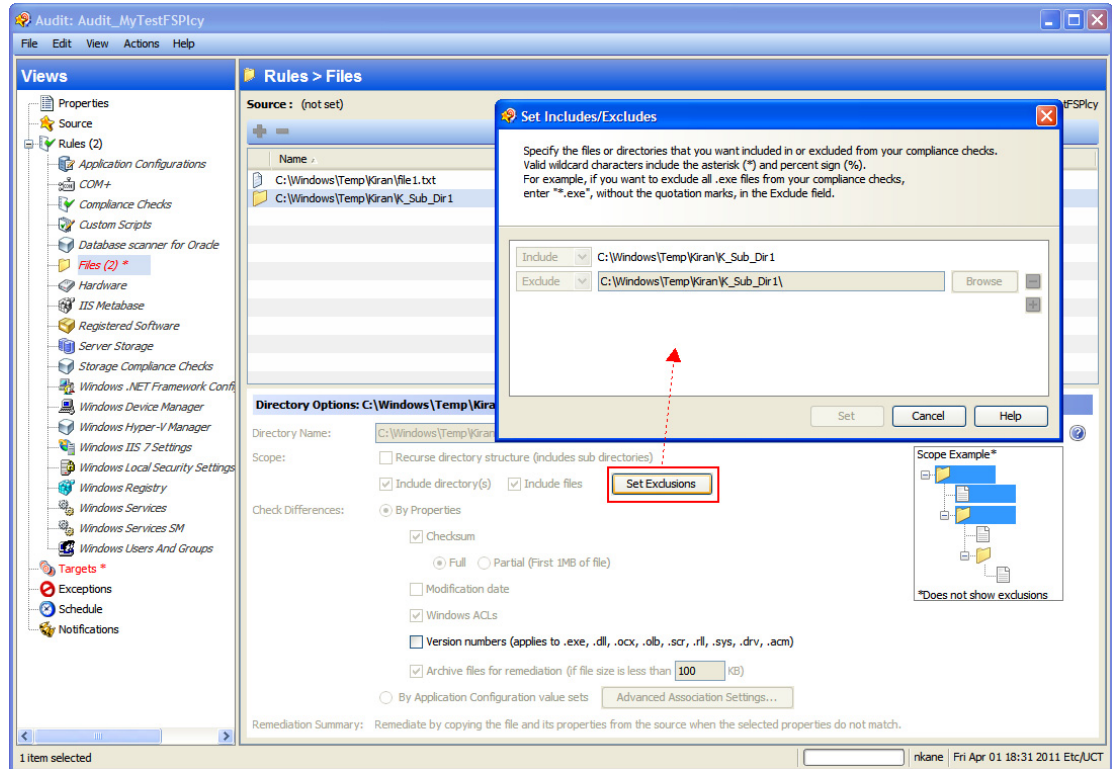
- 5 Click  to add another row or click  to remove a row.
- 6 In the Browse window, click **Select** to save your choices.
- 7 In the Set Includes/Excludes window, click **Set** to save your settings.


File Inclusion and Exclusion Rules

When configuring a file rule inside an audit, audit policy, or snapshot specification, you can specify the directories and files that you want included in and excluded from an audit or a snapshot. This section explains what the inclusion and exclusion rules are and how these rules are applied to the relative subset of the absolute path of the file.

Inclusions and exclusion rules inside of an audit’s file rule are found at the bottom of the audit or snapshot specification window, as shown in [Figure 15](#).

Figure 15 File System File/Directory Wildcard Inclusion and Exclusion Rules



When you configure the file rule in an audit or snapshot specification, you can enter inclusion/exclusion rules in the File/Directory Wildcard field. After you enter a rule, you can choose either Include or Exclude from the drop-down list. To add a new inclusion or exclusion rule, click  .

For information on how to create and configure file system rules for an audit or snapshot specification, see [Configuring the File Rule](#) on page 45.

Inclusion and Exclusion Rule Types

audit and remediation provides the following types of inclusion and exclusion rules configuring a file rule:

- A file-type rule applies to the file name path and contains neither a “/” or a “\”.
- A relative-type rule applies to the relative path and can contain a “/” for Unix and a “\” for Windows, and is not fully qualified.
- An absolute-type rule applies to the absolute path. In Unix, an absolute path begins with a “/”. In Windows, an absolute path begins with a volume letter that is followed by “:\” and is fully qualified, such as “C:\”, “d:\”, “f:\”, and so on. If you use a “/” (forward slash) for Windows paths, audit and remediation will convert it to a “\” (backslash) to use it as a valid path.
- Environment variable and custom attribute parameterization for filenames and path. For more information, see [Parameterizing Filenames for SA/Custom Attributes](#) on page 74.

audit and remediation processes all exclusion rules first. After all exclusion rules are applied, then the inclusion rules are applied. The default for include is to include all objects in the file system. In many cases, inclusion rules might not even be processed because, combined with the exclusion rules (which occur first), they might become a moot point.

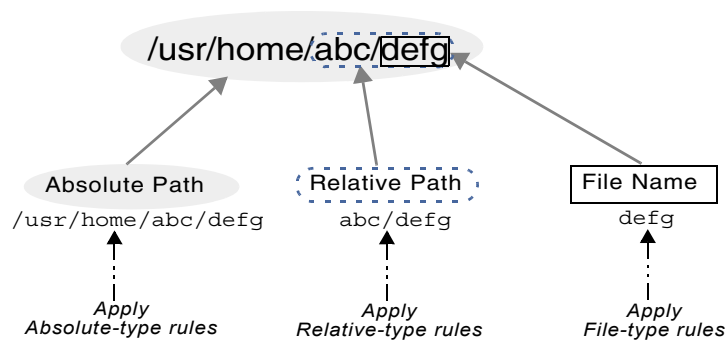
You can also use the asterisk (*) and the question mark (?) as valid wildcards in inclusion and exclusion rules. The wildcard character is a placeholder for matching a path, or one or more characters.

Depending on the type of inclusion and exclusion rule, the rule is applied only to the relevant subset of the absolute path of the file. In audit and remediation, there is one top level for each snapshot or audit. Each file that you compare against the inclusion and exclusion rules has an absolute path. In [Figure 16](#), the absolute path is `/usr/home/abc/defg`. A snapshot or an audit looks down the `/usr/home/abc/defg` absolute path and sees `abc/defg` as the relative path and `defg` as the file name. In this example, the inclusion and exclusion rules apply in the following manner:

- A file-type rule applies to the file name path `defg`.
- A relative-type rule applies to the relative path `abc/defg`.
- An absolute-type rule applies to the absolute path `/usr/home/abc/defg`.

See [Figure 16](#) for an illustration of how audit and remediation applies the inclusion and exclusion rules to a relative subset of the path of the file.

Figure 16 How Inclusion and Exclusion Rules Apply



To best explain how these rules are applied, the following examples are provided.

A sample file system structure used in [Example: Including all .txt Files in a Snapshot or Audit](#) on page 71 and [Example: Including last temp.txt file and exclude all else](#) on page 72 is as follows:

```

/dir1/dir2/a
/dir1/dir2/b
/dir1/dir2/names.txt
/dir1/dir2/temp.txt
/dir1/dir2/version1.exe
/dir1/dir2/subdir/version2.exe
  
```

Example: Including all .txt Files in a Snapshot or Audit

If you want to include all files with the `.txt` extension in your snapshot or audit, your inclusion and exclusion rules would be:

- `/dir1/dir2`
- `include *.txt` (This is a file-type rule.)
- `exclude *` (This is a file-type rule.)

The following steps explain how audit and remediation iterates through the file structure and applies any corresponding inclusion and inclusion rules:

- a The * causes /dir1/dir2/a to be excluded. Then *.txt is applied against the file portion of /dir1/dir2/a (a) and there is no match. The file is not included.
- b The * causes /dir1/dir2/b to be excluded. Then *.txt is applied against the file portion of /dir1/dir2/b (b) and there is no match. The file is not included.
- c The * matches names.txt, but *.txt matches names.txt as well, which causes the file to be excluded.
- d Same as step 3.
- e Compare a to *, which is a match; compare a to a, which is a match. The file is included.
- f Compare b to *, which is a match; compare b to a which is not a match. The file is excluded.

These step numbers correspond to the paths in the sample file structure, with the numbering starting with the top-level path.

Example: Including Only File a in a Snapshot or Audit

If you want to include only the file in your snapshot or audit, your inclusion and exclusion rules would be:

- /dir1/dir2
- exclude * (This is a file-type rule.)
- include a (This is a file-type rule.)

The following steps explain how audit and remediation iterates through the file structure and applies any corresponding inclusion and inclusion rules:

- a The * causes /dir1/dir2/a to be excluded. Then *.txt is applied against the file portion of /dir1/dir2/a (a) and there is no match. The file is not included.
- b The * causes /dir1/dir2/b to be excluded. Then *.txt is applied against the file portion of /dir1/dir2/b (b) and there is no match. The file is not included.
- c The * matches names.txt, but *.txt matches names.txt as well, which causes the file to be included.
- d Same as step 3.
- e Compare a to *, which is a match; compare a to a, which is a match. The file is included.
- f Compare b to *, which is a match; compare b to a which is not a match. The file is excluded.

These step numbers correspond to the paths in the sample file structure, with the numbering starting with the top-level path.

Example: Including last temp.txt file and exclude all else

If you want to include the last temp.txt file and exclude everything else in your snapshot or audit, your inclusion and exclusion rules would be:

- /dir1/dir2
- exclude * (This is a file-type rule.)
- include dir3/temp.txt (This is a relative-type rule.)

The following steps explain how audit and remediation iterates through the file structure and applies any corresponding inclusion and inclusion rules:

- a The * causes /dir1/dir2/a to be excluded. Then *.txt is applied against the file portion of /dir1/dir2/a (a) and there is no match. The file is not included.

- b The * causes /dir1/dir2/b to be excluded. Then *.txt is applied against the file portion of /dir1/dir2/b (b) and there is no match. The file is not included.
- c The * matches names.txt, but *.txt matches names.txt as well, which causes the file to be included.
- d Same as step 3.
- e dir3/temp.txt is compared against the relative portion of /dir1/dir2/dir3/temp.txt and there is a match.
- f Compare a to *, which is a match; compare a to subdir/version2.exe, which is not a match. The file is excluded.

These step numbers correspond to the paths in the sample file structure, with the numbering starting with the top-level path.

File Rule Overlap

When you include a parent directory (with options) in a rule and a child directory (with different options) as additional parameters, the parent directory snapshot and the child directory snapshot will overlap each other as one snapshot. This logic also applies to Windows NT ACL collection and content collection options, and Windows Registry content collection options. The following examples explain how audit rules for a parent and child directory overlap.

Consider the following file system, where an ending forward slash (/) represents a directory:

```
/cust/app/bin/
/cust/app/bin/file1
/cust/app/bin/conf/
/cust/app/bin/conf/conf1
/cust/app/bin/conf/conf2
/cust/app/bin/conf/dev/
/cust/app/bin/conf/dev/conf3
```

Example A

If you create a snapshot using the following two rules:

Directory /cust/app/bin (recursive, no checksum)

Directory /cust/app/bin/conf (not recursive, checksum)

The snapshot will record the following file system information:

```
/cust/app/bin/ (directory)
/cust/app/bin/file1 (no checksum)
/cust/app/bin/conf/ (directory)
/cust/app/bin/conf/conf1 (*checksum*)
/cust/app/bin/conf/conf2 (*checksum*)
/cust/app/bin/conf/dev/ (directory)
/cust/app/bin/conf/dev/conf3 (no checksum)
```

As you can see, even though /cust/app/bin was recursive and had no checksum, the /cust/app/bin/conf directory overrode it and all files in that directory have checksums recorded for them.

Example B

If you create a snapshot using the following two audit rules (by switching the options used in Example A):

```
Directory /cust/app/bin (recursive, checksum)
```

Directory /cust/app/bin/conf (not recursive, no checksum)

The snapshot will record the following file system information:

```
/cust/app/bin/ (directory)
/cust/app/bin/file1 (checksum)
/cust/app/bin/conf/ (directory)
/cust/app/bin/conf/conf1 (*no checksum*)
/cust/app/bin/conf/conf2 (*no checksum*)
/cust/app/bin/conf/dev/ (directory)
/cust/app/bin/conf/dev/conf3 (checksum)
```

Example C

If you create a snapshot using the following three audit rules (by adding a file option):

Directory /cust/app/bin (recursive, checksum)

Directory /cust/app/bin/conf (not recursive, no checksum)

File /cust/app/bin/conf/conf1 (checksum)

The snapshot will record the following file system information:

```
/cust/app/bin/ (directory)
/cust/app/bin/file1 (checksum)
/cust/app/bin/conf/ (directory)
/cust/app/bin/conf/conf1 (*checksum*)
/cust/app/bin/conf/conf2 (no checksum)
/cust/app/bin/conf/dev/ (directory)
/cust/app/bin/conf/dev/conf3 (checksum)
```

In this example, the very detailed audit rules for conf1 override the /cust/app/bin/conf audit rule.

Parameterizing Filenames for SA/Custom Attributes

When you create a file rule in an audit or snapshot specification, you can also reference environment variables and custom attributes in the file name. In the File/Directory Wildcard area of the rule window, you can edit the file name to add these references.

To add a reference to a Windows environment variable, the syntax is %envVarName% and for Unix, the syntax is \${varName}.

The syntax for specifying custom attributes is @varName@. For example:

```
@/customattribute/custAttributeNAME@\rest\of\the\path
@/customattribute/FacilityCustomAttributeNAME@\rest\of\the\path
@/customattribute/CustomerCustomAttributeNAME@\rest\of\the\path
@/customattribute/ServerAttributeNAME@\rest\of\the\path
@/customattribute/GrpAttributeNAME@\rest\of\the\path
```

This allows for auditing relative paths on both source and target servers using a parameterized environment variable or custom attribute in the filename.

Examples of Parameterizing Filenames

For example, on the servers you want to audit you know the relative path to an application, but not necessarily the absolute path for all servers. You can parameterize the path in your audit's File rule so the relative pathname is eliminated and the audit checks the relative path anywhere it exists on the target server.

For example, you want to audit a target servers against a golden source server where '%ProgramFiles%' is ': \Program Files' against target servers where %ProgramFiles% is D:\Program Files.

In the File/Directory Wildcard section of the File rule, you can specify the root of the directory rule in the audit to be %ProgramFiles%\Company\MyApp. The audit will remove %ProgramFiles% from the paths of the servers it targets when you run the audit. In other words, C:\Program Files\Company\MyApp\file1.txt on the source server will be compared with D:\Program Files\Company\MyApp\file1.txt on the target servers.

In another example, you may want to audit an application that is installed into two completely different subdirectories on two different servers.

For example, in your audit you choose from a golden source server configuration the installation path of the following:

```
/usr/local/app-version-1232/prog
```

And, your target servers have the application installed anywhere under this path:

```
/usr/local/app
```

In order to audit the target server, you can defines a custom attribute APP_INSTALL_LOC with a value of /usr/local/app-version-1232/prog for the golden server and /usr/local/app for the production servers. The File rule in the audit would look something like this:

```
@/customattribute/APP_INSTALL_LOC@/prog
```

This would cause the audit to treat @/opsware/customattribute/APP_INSTALL_LOC@ as if it were an environment variable on the target server and do a path replacement.

If you wanted to reference a server attribute, the path would be entered like this:

```
@/server/APP_INSTALL_LOC@/prog
```

Environment Variables in Pathnames



Best Practice: If you want to use environment variables in file name PATH on Unix (commonly known as *parameterized checks*), it is best to define those environment variables under the following file and directory: `etc/opt/opsware/snapshot/env`. Be sure that you do not use `/etc/profile` to source environment variables on Unix.

To define environment variables that can be sourced for the File rule configuration, you can create a file with the variables on the managed server you want to audit or snapshot.

Example:

- 1 ssh to the managed server that you want to audit or snapshot.
- 2 Create a new directory in the following location:

```
mkdir /etc/opt/opsware/snapshot
```
- 3 Create a new empty file, such as:

```
touch /etc/opt/opsware/snapshot/env
```

- 4 Define the environment variables you want to source from the file rule by entering them in the new file.
Example:

```
TEST1='/tmp/test1'  
TEST2='/home/test2'  
export TEST1 TEST2
```
- 5 When you have finished editing, save the file.

Audit Rule Exceptions

For most audit rules, you can create temporary or permanent rule exceptions on selected target servers (or groups of servers) in the audit. This means you can exclude specific rules on selected targets of the audit when the audit runs.

For example, in an audit that is auditing several servers, you might want to suspend one or more of the rules for a subset of the servers targeted by the audit. You might have a collection of Windows servers that are regularly audited to make sure that the IIS service is disabled, for example, to meet company security standards. Your audit is configured to check each of those servers to make sure IIS is disabled. If IIS is enabled on any of the servers, the audit will fail.

However, for a short period of time you might want to run a business application that requires the IIS service to be enabled in order to run on a few of the servers targeted in the audit. You can create a rule exception for the rule governing the IIS service and associate the exception with the servers that need to run the application. This ensures that the audit can still run and not fail when it encounters the servers that do have the IIS service enabled.

You can set an expiration date for the rule exceptions to make sure that when the rule exception is no longer needed or permitted, the rule will be applied to all servers in the audit. You can also write a reason for the exception and associate a ticket ID with it. Exceptions you create in one audit do not affect rules in any other audits.

Rules That Cannot Have Exceptions

Most audit rules can have exceptions created for them. However, rule categories that include ALL of a set of rules cannot have exceptions.

Considerations When Applying Exceptions to Device Groups

When you set an audit rule exception for a device group, the exception will be applied to all servers in the group. It is possible that one of the servers in the group with the exception also belongs to another device group, which also happens to be the target of an audit that has no exceptions applied to it.

In this situation, the rule exception always applies to the server, even though the server also belongs to a device group with no exceptions. As a rule of thumb, keep in mind any servers in a device group that has a rule exception applied to it will have the audit rule excepted, whether or not the server belongs to another device group that is targeted by an audit and has the same rule applied without an exception.


Adding a Rule Exception to an Audit

To create an audit rule exception, select any of the rules configured in your audit and using the Add Rule Exception window, associate them with a target server in the audit. When you run the audit, the selected rule and the target servers or snapshots associated with the rule will not be applied.

You can also apply rule exceptions to device groups. You can set the rule exception to run indefinitely, or to expire at some future point in time. You can add a comment to explain why you are creating the exception, and also associate a ticket ID with the exception.

Some audit rules and audit rule collections cannot be excepted. For more information, see [Rules That Cannot Have Exceptions](#) on page 76.

To add a rule exception to an audit:

- 1 First, create an audit. For information see [Creating an Audit](#) on page 19.
- 2 Configure audit rules for the audit. For information on configuring audit rules, see [Audit & Remediation Rules](#) on page 33.
- 3 In the audit view pane on the left, select the Exception  icon.
- 4 Next, from the content pane, click **Add**.



You can also select any rule in the Audit window, right-click, and select **Add Exception**. However, if the audit is referencing a linked audit policy, right-clicking a rule to add an exception will not work.


- 5 In the Add Exception window, from the Select Target Server section, select a server, multiple servers, or device groups to which you want to apply the rule exception.
- 6 Next, from the Select Rule section, select one or more rules you want to associated with the servers you selected in the previous step.
- 7 (Optional) In the Reason for Exception section, add an explanation.
- 8 (Optional) In the Ticket ID section, add the ticket ID associated with this exception.
- 9 In the Expires section, either enter a date to indicate when the exception expires, or select a date from the drop down list.
- 10 When you are finished configuring the exception, click **Add**.
- 11 You now see a list of rule exceptions that will be applied when you run the audit.

Editing or Deleting a Rule Exception

You can edit an exception in one of two ways:


- Double-click the exception to modify the reason for the exception, the ticket ID, and the exception expiration date
- Click the **Add** to edit a rule (overwrite the existing rule)

To edit an exception:

- 1 Open an audit window.
- 2 In the audit's View pane on the left, select the Exception  icon.
- 3 In the Contents pane, double-click an exception.

- 4 In the Edit Exception window, you can edit any of the exceptions and servers or device groups they are assigned to. When you have edited the exception, click **Add**.
- 5 If you want to completely change and the rule, click **Add** and then in the Add Exception window, change the rule by selecting target server and one or more rules. When you are finished, click **Add** to change the exception.

To delete an exception:

- 1 Open an audit window.
- 2 In the audit view pane on the left, select the Exception  icon.
- 3 In the contents pane, select the exception you want to select, and then click **Delete**.

Audit Policy Management

An audit policy allows you to define and store a centralized and reusable collection of server configuration compliance rules. You can link an audit policy to audits, snapshot specifications, and other audit policies.

An audit policy is typically created by a policy setter who understands the compliance standards that a company wants its servers to meet. Another set of users, whose job it is to manage and audit actual servers, can use predefined audit policies by linking them to their audits or snapshot specifications. If changes are made to the audit policy, the audit or snapshot specification that links to it will reference the audit policy's updated rules. Users who audit servers can be sure their audits always reflect the latest compliance standards in their organization.

Audit policies can link to other audit policies. For example, you could combine several different discrete audit policies together as one master policy that defines how Windows services should be configured. After you run the audit, if any discrepancies are discovered you can remediate them from the audit results.

You can create an audit policy from scratch or you can save the rules of an audit, snapshot specification (or another audit policy) as an audit policy. All audit policies are stored in the SA Client Library.

Linking & Importing an Audit Policy

An audit policy can be used inside audits and snapshot specifications, or other audit policies, through *linking*. Audits and snapshot specifications also use audit policies through *importing*.

Linking an Audit Policy



Best Practice: *Linking* an audit policy to an audit or snapshot specification enables the audit or snapshot specification to use the exact same rule set of the audit policy. If any of the rules in the audit policy change, the same changes are reflected in the audit and snapshot specification's rules the next time they are run, since they link to the rule set defined in the audit policy.

You can break this link by selecting the **Enable unlinked rules (prevents linking to predefined audit policies)** option. See [Configuring the File Rule](#) on page 45.

Audit policies can be also be linked to other audit policies, and you can link as many audit policies as you want into an audit policy. When you link one or more audit policies to an audit policy, the linked audit policies become children of the parent audit policy. If you create an audit that links to the parent audit policy, when you run the audit on a target server, the rules from all linked policies are run against on the target server.

Importing an Audit Policy

Importing an audit policy into an audit or snapshot specification imports all rules from the audit policy. After they are imported, the rules are editable. When you import an audit policy into an audit, you can choose to replace any current values in the audit or merge rules from the audit policy with those in the audit or snapshot specification. Audit policies cannot import rules from another audit policy; however, they can link to other audit policies.

Rule Overlap with Multiple Linked Audit Policies

Because you can link your audit or snapshot specifications to an audit policy that may references other audit policies, it is possible that some of the linked policies might contain the same rules but with different configuration options.

Rules become merged in audit results when you identify the same object for a rule and the only way to customize the rule is by setting options. The options may or may not be different, but they still get merged into one rule before running and there is only one result. If the options are different, the options are OR'ed together into the single rule. Examples include file rules, registry rules, metabase rules (legacy comparison type), Windows Service rules, etc.

Rules that take parameters or you specify the compliance criteria are merged if and only if the parameters and the criteria are exactly the same. Otherwise they are executed as separated rules. Examples include compliance (pluggable) rules, custom script rules, and server module based rules.

Creating an Audit Policy

When you create an audit policy, you have the option of creating its rules using a live server as a source to pick and choose for rules, by creating your own custom rules, or linking to the rules of another audit policy.

Using a source server for building audit policy rules allows you to base the audit policy's rules on the actual configurations of a managed server. The source server used to build rules is not used after the audit policy is linked to an audit or snapshot specification.





All audit policies must be saved to a folder in the SA Client Library. To save an audit policy to a folder, you must have permissions to write to that folder. For more information about folder permissions, see the *SA Administration Guide*.

To create an audit policy:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Audit and Remediation** ► **Audit Policies**.
- 2 Select an operating system: Windows or Unix.
- 3 From the **Actions** menu, select **New**.
- 4 In the Properties content pane, enter a name and description (*optional*).
- 5 Click **Select** to specify a location in the SA Library where you want to save the audit policy.

- 6 In the Select Folder window, select a folder for the location. You must have permissions to write to the folder where you save the policy.
- 7 After you have chosen the location, click **Select**.
- 8 In the Audit Policy window, in the Views pane, select **Source** if you would like use a managed server to base the audit policy's rules on.
- 9 In the Source content pane, click **Select** to choose a source server for the audit policy.
- 10 In the Select Server window, after you have selected a server, click **OK**.
- 11 In the Audit Policy window, in the Views pane, select **Rules**.

If you want to link other audit policies to this audit, click  to select an audit policy.

If you want to edit any of the linked audit policies, from the Rules list, select an audit policy and then click  to open the Audit Policy window.

- 12 In the Select an Audit Policy window, select one or more audit policies to link to the audit policy, and then click **OK** to save your selections.

If you link one or more audit policies to an audit policy, you can still configure individual rules in the audit policy. All rules from an externally referenced audit policy will be combined with any rules you create to build one single rule set.

- 13 In the Views pane, in the Rules list, create any other rules you want to include in the audit policy. For more information on how to configure specific audit and remediation rules, see [Audit and Snapshot Rules](#) on page 35.
- 14 When you are finished configuring the audit, from the **File** menu select **Save**. After it is saved, the audit policy is ready to be linked to an audit, snapshot specification, or another audit policy.

Saving an Audit as an Audit Policy

You can save an audit as an audit policy. This action saves only the rules from the audit and then creates a new audit policy.



All audit policies you create must be saved in the SA Library in a folder. You must have permissions to write to the folder you want to save the audit policy to. For more information on folder permissions, see the *SA User Guide: Server Automation* or contact your SA Administrator.

To save an audit so that it creates an audit policy:

- 1 In the Audit or Snapshot Specification window, from the File menu, select **Save As**.
- 2 In the Save As window, enter a name. If you are renaming an audit or snapshot specification, you must use a unique name.
- 3 *(Optional)* Enter a description.
- 4 From the Type drop-down list, select Audit or Audit Policy.
- 5 If you selected Audit Policy, from the Location section, click **Select**.
- 6 Select a folder in the SA library to save the audit policy to. You must have write permission on the folder to save the audit policy.
- 7 Click **OK**.

Ways to Link & Import Audit Policies

You can import or save an audit policy to an audit, snapshot specification, or another audit policy:

- [Linking an Audit Policy to an Audit or a Snapshot Specification](#)
- [Linking Audit Policies to a Master Audit Policy](#)
- [Importing Audit Policy Rules \(replace or merge\)](#)
- [Saving an Audit or a Snapshot Specification as an Audit Policy](#)

Linking an Audit Policy to an Audit or a Snapshot Specification

Linking an audit policy to an audit or snapshot specification creates a link that uses the rules from the audit policy for the audit or snapshot specification.



Best Practice: Linking to an audit policy is useful when a policy setter wants to define a server configuration policy for servers and then have other users link their audits and snapshot specifications to the same audit policy. If the policy setter makes any changes to the audit policy, the changes will be reflected in the audits or snapshot specifications that are linked to the policy.

When an audit policy is linked to an audit or snapshot specification, the rules cannot be modified in the context of the audit or snapshot specification. However, you can access the audit policy and edit its rules if you have the required user permissions.



If the audit or snapshot specification you are linking the audit policy to already has rules defined, all pre-existing rules in the audit or snapshot specification will be *overwritten* when you link to an external audit policy.

To link an audit policy to an audit or snapshot specification:

- 1 Open an existing audit or snapshot specification from the SA Library:
 - a In the navigation pane, select **Library** ► **Audit and Remediation** ► **Audits**. Select an operating system: Windows or Unix. From the content pane, open an audit.
 - b In the navigation pane, open an existing snapshot specification from select **Library** ► **Audit and Remediation** ► **Snapshot Specifications**. From the content pane, open a snapshot specification.
- 2 From the **Actions** menu, select **Link to Policy**.
- 3 In the Select an Audit Policy window, select an audit policy to link to the audit or snapshot specification. You can only link to *one* audit policy per audit or snapshot specification. However, you can link *multiple* audit policies to *one* audit policy. See [Creating an Audit Policy](#) on page 79 or [Linking Audit Policies to a Master Audit Policy](#) on page 82.
- 4 After you have selected an audit policy, click **OK**.

If you are linking an audit policy to an audit or snapshot specification that already has rules defined, a message prompts you to confirm whether you want to *overwrite* any existing rule definitions. Click **Yes** to import the audit policy and overwrite pre-existing rules.

- 5 From the **File** menu, select **Save** to save the audit or snapshot specification.



Linking Audit Policies to a Master Audit Policy

Linking an audit policy to another audit policy enables you to combine multiple audit policies into a single, *master audit policy*. Because you can link as many audit policies as you want to an audit policy, you can build and reuse existing audit policies as a single audit policy that meets a specific auditing need.


When you link one or more audit policies to an audit policy, the linked audit policies become children of the parent (or master) audit policy. If you create an audit that links to the parent audit policy, when you run the audit on a target server, the rules from all linked policies are run against the target server.

Example: Your SA Library contains several individual audit policies that define compliance standards for a group of HP-UX servers. One policy contains rules that check to make sure the FTP services are enabled. Another policy contains rules that check to make sure that cron logging is always enabled. In this example, you can create a single *master audit policy* that links to these two policies. This *master audit policy* can, subsequently, be referenced to by other audits.

To link audit policies to a master audit policy:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Audit and Remediation** ► **Audit Policies**.
- 2 Select an operating system: Windows or Unix.
- 3 Select an existing audit policy or create a new audit policy. See [Creating an Audit Policy](#) on page 79.
- 4 In the Audit Policy window, in the Views pane, select **Source** if you want to use a managed server to base the audit policy's rules on.
 - a Click **Select** to choose a source server for the audit policy.
 - b In the Select Server window, select a server and then click **OK**.
- 5 In the Audit Policy window, in the Views pane, select **Rules**
 - a If you want to link other audit policies to this audit, click  to select an audit policy.
 - b If you want to edit any of the linked audit policies, from the Rules list, select an audit policy and then click  to open the Audit Policy window.
- 6 In the Select an Audit Policy window, select one or more audit policies to link to the audit policy and then click **OK** to save your selections.

If you link one or more audit policies to an audit policy, you can still configure individual rules in the audit policy. All rules from an externally referenced audit policy will be combined with any rules you create in the audit policy.
- 7 In the Views pane, in the Rules list, create any other rules you want to include in the audit policy. See [Audit and Snapshot Rules](#) on page 35.

If you want to edit any of the linked audit policies, from the Rules list, select an audit policy and then click then click .
- 8 When you are finished configuring the audit policy, from the **File** menu select **Save**. After it is saved, the audit policy is ready to be linked to another audit policy.

Importing Audit Policy Rules

Importing an audit policy into an audit or snapshot specification allows you to import (and optionally merge) an audit policy's rules into an audit or a snapshot specification, without keeping a link to the audit policy.

After you import an audit policy, there is no longer a connection to that audit policy. Any changes made to the source audit policy are not reflected where the audit policy was imported into.

To import an audit policy into an audit:

- 1 Open an existing audit or snapshot specification from the SA Library:
 - a In the navigation pane, select **Library > Audit and Remediation > Audits**. Select an operating system: Windows or Unix. From the content pane, open an audit.
 - b In the navigation pane, open an existing snapshot specification from select **Library > Audit and Remediation > Snapshot Specifications**. From the content pane, open a snapshot specification.
- 2 From the **Actions** menu, select **Link to Policy**.
- 3 If the audit or snapshot specification already has rules defined, choose to either to overwrite the existing rules or merge the audit policy rules with the existing rules.



Best Practice: Depending on the rule type, merging rules can produce different results. As a best practice, review all resulting rules to make sure that the merged audit policy rules meet your requirements or need to be modified.

If you click **Yes**, the audit policy will *overwrite* any existing rules in the audit or snapshot specification.

If you click **No**, the audit policy will *merge* the audit policy rules with any existing rules. If any conflicts are found, the audit policy rules will *overwrite* any existing rules.

- 4 From the **File** menu, select **Save** to save the audit or snapshot specification.

Saving an Audit or a Snapshot Specification as an Audit Policy

You can save an audit or a snapshot specification's rules as an audit policy. The audit policy can then be used in another audit or snapshot specification.



All audit policies you create must be saved in the SA Library in a folder. To save an audit policy to a folder, you must have permissions to write to that folder. For more information on folder permissions, see the *SA User Guide: Server Automation* or contact your SA administrator.

To save an audit or snapshot specification as an audit policy:

- 1 Open an existing audit or snapshot specification from the SA Library:
 - a In the navigation pane, select **Library > Audit and Remediation > Audits**. Select an operating system: Windows or Unix. From the content pane, open an audit.
 - b In the navigation pane, open an existing snapshot specification from select **Library > Audit and Remediation > Snapshot Specifications**. From the content pane, open a snapshot specification.
- 2 After you have configured the audit's or the snapshot specification's rules, from the **File** menu, select **Save As**.
- 3 In the Save As window, enter a name and description.
- 4 In the Type list, select Audit Policy.

- 5 Click **Select**.
- 6 In the Select Folder window, choose a folder where you want to save the audit policy and then click **OK**. The audit policy is saved and can be accessed at **Library** ► **Audit and Remediation** ► **Audit Policies**.

Locating an Audit Policy in the Folder Library

After you create and save an audit policy to the folder library, you can easily find the audit policy in the SA Library by using the Locate in Folders feature.

To locate an audit policy in folder:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Audit and Remediation** ► **Audit Policies**, and then select **Windows** or **Unix**.
- 2 Select an audit, right-click, and then select **Locate in Folders**. The location where the audit policy is saved is displayed.

Exporting an Audit Policy to HTML or CSV

If you want to get a list of all the rules contained and configured in an audit policy, you can export the policy to either HTML or CSV.

To export an audit policy to HTML or CSV:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Audit and Remediation** ► **Audit Policies**.
- 2 Select Windows or Unix.
- 3 Open an audit policy:
 - a Select an audit and then double-click.Or
 - b Select an audit, right-click, and then select **Open**.
- 4 From the Actions menu, select **Export** ► **HTML** or **CSV**.
- 5 Select a path and filename for the file, and then click **Export**.
- 6 Open the file to view the exported information.

Audit Results

An audit defines the server configurations that you want to check on a server, according to the audit's rules. Audit results are produced by running an audit. These results show the differences between the audit rules and the actual server configuration values for each target server or target snapshot.

Whether or not you can remediate a rule depends on the rule type. The rule must support remediation and the source of the audit rule for that server must contain enough data to support the remediation.

Example: Some rules do not support remediation, such as a Hardware rule. You cannot remediate a server's physical memory or hardware. If your audit is using a snapshot as a source and the snapshot was unable to gather sufficient information from a rule, then that rule will also not be remediated.

For those audits that link to audit policies, the results will show all rules in the audit; however, the results do not show the audit policy or policies where the rules were originally defined.

For more information, see the following topics:

- [Remediating Rules with Inherited Values](#) on page 85
- [Audit Results Window](#) on page 86
- [Audit Results Summary](#) on page 87
- [Remediation Methods: All, By Server, or By Rules](#) on page 88
- [Remediating Audits Attached to Servers](#) on page 141
- [Viewing and Remediating Audit Results Differences](#) on page 92
- [Viewing Audit Results with Exceptions](#) on page 95


Remediating Rules with Inherited Values


If you create an audit rule based on an object that inherits properties from a parent object, be aware that if you remediate the rule, the target server object will not inherit the parent object's properties.

For example, if you created a rule for a Registry entry, and that registry entry inherited some values from a parent, when you remediate the rule on to a target server, none of the values inherited from its parent will be remediated, and the rule will show in the audit results as a difference.

Additionally, if your audit checks ACLs for the File, Registry, or IIS Metabase rules, and the user and group ACL does not exist, then after the audit is run and after remediation, if user and group does not exist on target a temporary user and group will be created as unknown name. The next time you run Audit it shows up as unknown, which shows name other than the source user.

Additionally, if you create an IIS Metabase rule from a source server and the metabase object selected for the rule inherits its values from a parent Metabase object, differences will show after an audit is run. For example, if you remediate once and then rerun the audit, if the source key was not inherited and the attribute has an IED when it gets created on target server, the object will be created based on parent key inheritance. When you rerun the audit, the results will show the IED as a difference for the object's attribute.

 If you have Audit Results with differences from Audits that were created in SA 5.1, and you have upgraded to SA 6.x, when you view those Audit Results in the upgraded version of the SA Client, the Differences column in the Audit Results list will incorrectly display the value of -1 differences. To view the actual number of results, simply open the Audit Results window (double-click it) and you will see all the actual differences in the results.

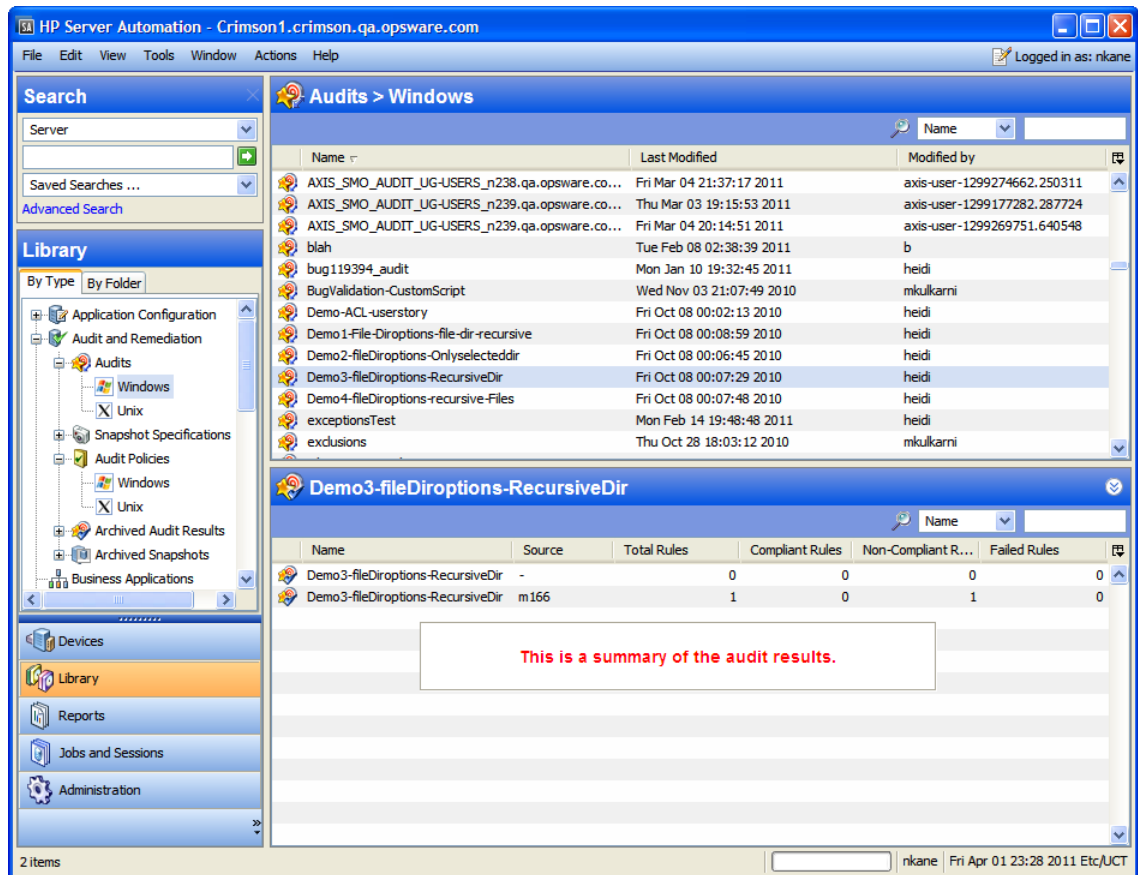
 SA does not support the remediation of the following two values on Windows 2000 servers for the Windows Local Security Settings rule, under Security Options: Rename AdministratorAccount and Rename Guest Account.

 You cannot remediate ISAPI filters for the IIS 7.0 audit rule in this release.

Viewing Audit Results

In the SA Client, you can view audit results for any audit, as shown in Figure 17.

Figure 17 Audit Results



When you select an audit in the library, all results associated with the audit appear in the details pane below.

Audit Results Window

The Audit Results window provides information about the audit job, such as differences between servers targeted by the audit and the rules defined in the audit. This information helps you determine the extent to which the servers that have been audited are in compliance with the standards set for your data center.

For those audits that link to an audit policy, the results show all of the rules in the audit; however, the results do not show the audit policy or policies where the rules were originally defined.

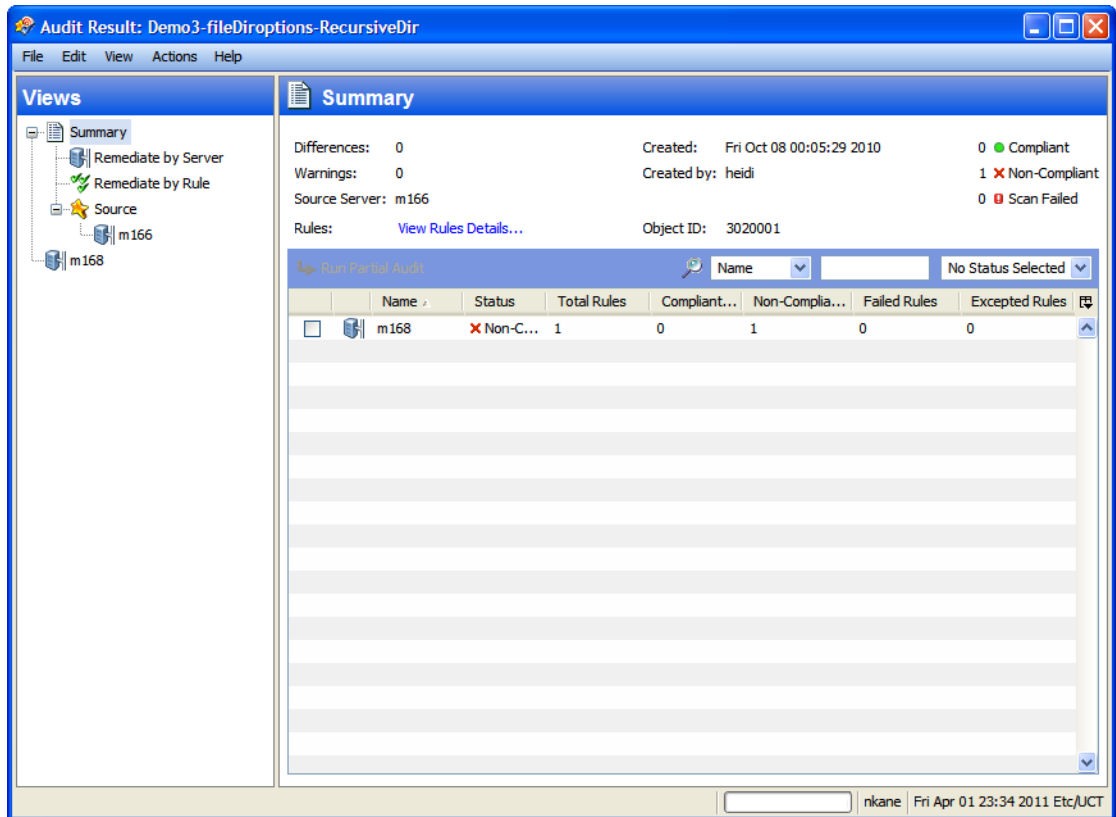
If you have a rule checking installation of a certain package with a certain version number on a server and the audit finds a package with the same package name but with a different version number, SA does not indicate that it is the package you are looking for. Instead, SA indicates that the rule did not find the package. It is a known limitation that SA does not assume that only the name uniquely identifies the package.

Each Audit Results window provides two main elements:

- **Summary:** A an overview of the audit job that provides a compliance status for the audit and remediation options that allow you to remediate by server, by rule, or remediate all rules on all servers. Remediation is only available in instances where the target server configurations do not match the rule definitions in the audit.

- **Server List:** A list of all servers that the audit was run against and a list of all rules from the audit, showing which rules, if any, are out of compliance.

Figure 18 Audit Results: Summary View



Audit Results Summary

The audit results summary view describes the following information about an audit job:

- **Differences:** The number of differences discovered during the audit. This is the sum total of all configuration differences found on all target servers that are defined in the audit rules.
- **Source:** The source server used in the audit that the results are based on.
- **Created, Created By:** When the audit was created and the name of the user who created it.
- **View Rule Details:** This link launches the audit browser so that you can view the audit's rule.
- **Run Partial Audit:** This link allows you to select servers and re-run the audit on only those rules that have a Non-Compliant or Scan Failed compliance status.
- Compliance information identifies how many rules in the audit are:

Compliant: ● The number of rules for which target server configurations matched the rules in the audit.

Non-Compliant: ✘ The number of target server configurations that did not match the rules in the audit.

Scan Failed: ! The number of rules for which the audit was unable to determine the target server configuration.

- Server list information includes the number of **Total Rules**, **Compliant Rules**, **Excepted Rules**, **Failed Rules**, and **Non-Compliant Rules** for each managed server that the audit was run against.


For more information about audit remediation types, such as **Remediate by Server** or **Remediate by Rule**, see [Remediation Methods: All, By Server, or By Rules](#) on page 88.

Remediation Methods: All, By Server, or By Rules

In the Audit Results window, there are three different ways to remediate non-compliant rules in audit results:

- **Remediate All**: In the Audit Results window, from the Actions menu, select Remediate all to remediate differences found in the audit results.
- **Remediate by Server**: Remediate by servers targeted by the audit results.
- **Remediate By Rule**: Remediate specific, individual audit rules.

Remediate All

You can select to remediate all differences found in an audit result for all rules that are remediable. This option remediates all remediable rules on all servers targeted by the audit. Rules that have a status of Compliant  are not remediated when the audit is run.

To remediate all differences found in an audit results:

- 1 In the navigation pane select **Library** ► **By Type** ► **Audit and Remediation** ► **Audits**.
- 2 Select an audit. In the details pane below the audit list, all audit results associated with the audit are displayed.
- 3 Select an audit result, right-click, and then select **Open**.
- 4 In the Audit Result window, from the Actions menu select **Remediate All**.
- 5 In the Remediate Audit window, step one shows the name of the audit, the target of the audit, and the total number of rules defined in the audit. If you want to bypass all audit task steps, click **Start Job** to immediately run the audit job.
- 6 Click **Next**.
- 7 In the Scheduling page, specify whether you want the audit to run immediately or at a later time and date. To run the audit at a later time, select Run Task At and then specify a day and time.
- 8 Click **Next**.
- 9 In the Notifications page, by default your user will have a notification email sent when the audit completes, whether or not the audit job is successful. To add an email notifier, click **Add Notifier** and enter an email address.
- 10 *(Optional)* You can specify whether you want the email to be sent on success or failure of the audit job.
- 11 *(Optional)* You can specify a Ticket Tracking ID in the Ticket ID field. The ticket ID field is only used when HP Professional Services has integrated SA with your change control systems. Otherwise, leave this field empty.
- 12 Click **Next**.
- 13 In the Job Status page, click **Start Job** to run the audit. When the audit has run, click **View Results** to view the results of the audit.

Remediate By Rule

You can remediate specific differences found in rules in audit results by selecting individual rules that are out of compliance, and then re-running the audit to remediate only the rules you select. You can select to remediate by individual rule for all servers targeted by the audit, or choose only selected servers to have rules remediated.

To remediate specific differences found in audit results:

- 1 In the navigation pane select **Library** > **By Type** > **Audit and Remediation** > **Audits**.
- 2 Select an audit.
- 3 In the details pane below the audit list, you see all audit results associated with the audit.
- 4 Select an audit result, right-click, and select **Open**.
- 5 In the Audit Result window, expand the Summary list, and then select Remediate By Rule. All differences discovered by rule in the audit results are displayed.
- 6 For each rule you want to remediate, select the check mark in the list in the All Servers column. This means that when you remediate the audit results, the rule will be remediated on all servers targeted by the audit that the rule is applied to.

If you want to globally select all rules, right-click and then select **Select All**. To deselect all rules, right-click and then select **Deselect All**.
- 7 When you have selected the rules you want to remediate, from the **Actions** menu, select **Remediate**.
- 8 In the Remediate Audit window, step one shows the name of the audit, the target of the audit, and the total number of rules defined in the audit. If you want to bypass all audit task steps, click **Start Job** to immediately run the audit job.
- 9 Click **Next**.
- 10 In the Scheduling page, specify whether you want the audit to run immediately or at a later time and date. To run the audit at a later time, select Run Task At and then specify a day and time.
- 11 Click **Next**.
- 12 In the Notifications page, by default your user will have a notification email sent when the audit completes, whether or not the audit job is successful. To add an email notifier, click **Add Notifier** and enter an email address.
- 13 *(Optional)* You can specify whether you want the email to be sent on success or failure of the audit job.
- 14 *(Optional)* You can specify a Ticket Tracking ID in the Ticket ID field. The ticket ID field is only used when HP Professional Services has integrated SA with your change control systems. Otherwise, leave this field empty.
- 15 Click **Next**.
- 16 In the Job Status page, click **Start Job** to run the audit. When the audit has run, click **View Results** to view the results of the audit.

Remediate by Server

You can remediate specific differences found in rules in audit results by the server that the audit targets. You can select to remediate all rules on all servers, or, for all rules on selected servers.

To remediate specific differences found in an audit results by server:

- 1 In the navigation pane select **Library > By Type > Audit and Remediation > Audits**.
- 2 Select an audit.
- 3 In the details pane below the audit list, all audit results associated with the audit are displayed.
- 4 Select an audit result, right-click, and then select **Open**.
- 5 In the Audit Result window, expand the Summary list.
- 6 The contents pane lists servers targeted by the audit. For each server you want to audit, select the check box next to the server, and then click **Run Partial Audit**.

Or

You can expand the list of servers in the Views pane, and for each server you see all differences discovered on all servers targeted by the audit.

For each server you want to remediate, select the check mark in the list in the All Rules column. This means that when you remediate the audit results, all rules will be remediated on the selected servers.

Or

If you want to globally select all servers in the audit results, right-click and then select **Select All**. To deselect all servers, right-click and then select **Deselect All**.

- 7 When you have selected the servers you want to remediate, from the **Actions** menu, select **Remediate**.
- 8 In the Remediate Audit window, step one shows the name of the audit, the target of the audit, and the total number of rules defined in the audit. If you want to bypass all audit task steps, click **Start Job** to immediately run the audit job.
- 9 Click **Next**.
- 10 In the Scheduling page, specify whether you want the audit to run immediately or at a later time and date. To run the audit at a later time, select Run Task At and then specify a day and time.
- 11 Click **Next**.
- 12 In the Notifications page, by default your user will have a notification email sent when the audit completes, whether or not the audit job is successful. To add an email notifier, click **Add Notifier** and enter an email address.
- 13 *(Optional)* You can specify whether you want the email to be sent on success or failure of the audit job.
- 14 *(Optional)* You can specify a Ticket Tracking ID in the Ticket ID field. The ticket ID field is only used when HP Professional Services has integrated SA with your change control systems. Otherwise, leave this field empty.
- 15 Click **Next**.
- 16 In the Job Status page, click **Start Job** to run the audit. When the audit has run, click **View Results** to view the results of the audit.

Remediating Comparison-Based Audit Results

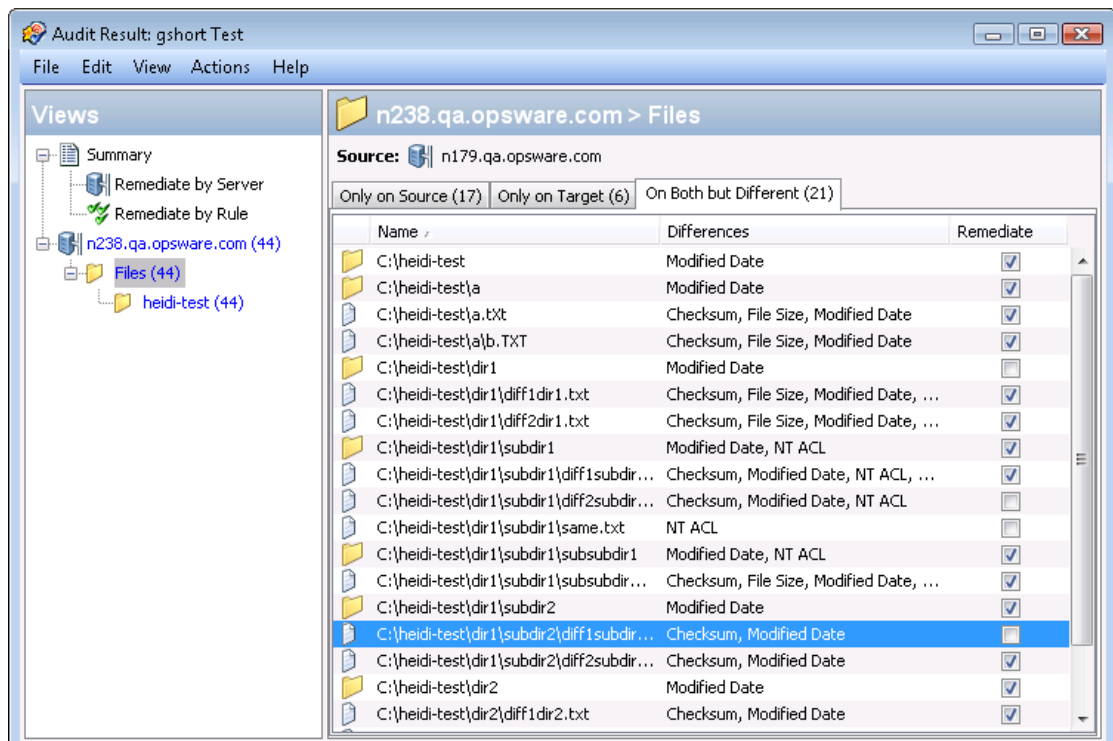
Audit results based on a comparison-based audit allow you to view differences between the source server or snapshot and target servers or snapshot. If the audit results fails—that is, it finds differences between source and target—you can remediate the differences (for most rule types). You can remediate the rule values of the source objects in the audit and overwrite the values on the target (or add values that exist on the source, but do not exist on the target.)

The Audit Result window shows all the objects defined in the audit in the Views pane. It also shows the audit results that failed, the differences found between the audit and the target servers are highlighted in light blue font.

For example, Figure 19 shows audit results for a windows file system rule, where the selected file and path exist on both the source (audit rule source server) and the target, but are different, located under the Only Both But Different tab of the Audit Result window.

In the Audit Result window, you can select the Files rule, and from the **Actions** menu select **Remediate**.

Figure 19 Audit Results for a Comparison-Based Audit Rule



In this example where file difference were found between the source and the target, you can double-click the rule to view those differences in a separate window. Review the differences information to make sure you want to perform the remediation. Then, you can select **Remediate** from the **Actions** menu and remediate the out-of-compliance rule or schedule the audit to run at a later time. When you remediate, the values from the audit (derived from the source) will replaces those on the target server.



When remediating COM+ objects from snapshot or audit results, the SA Client does not check the version of the COM+ object. SA will always remediate the object, whether or not there is any difference between them.

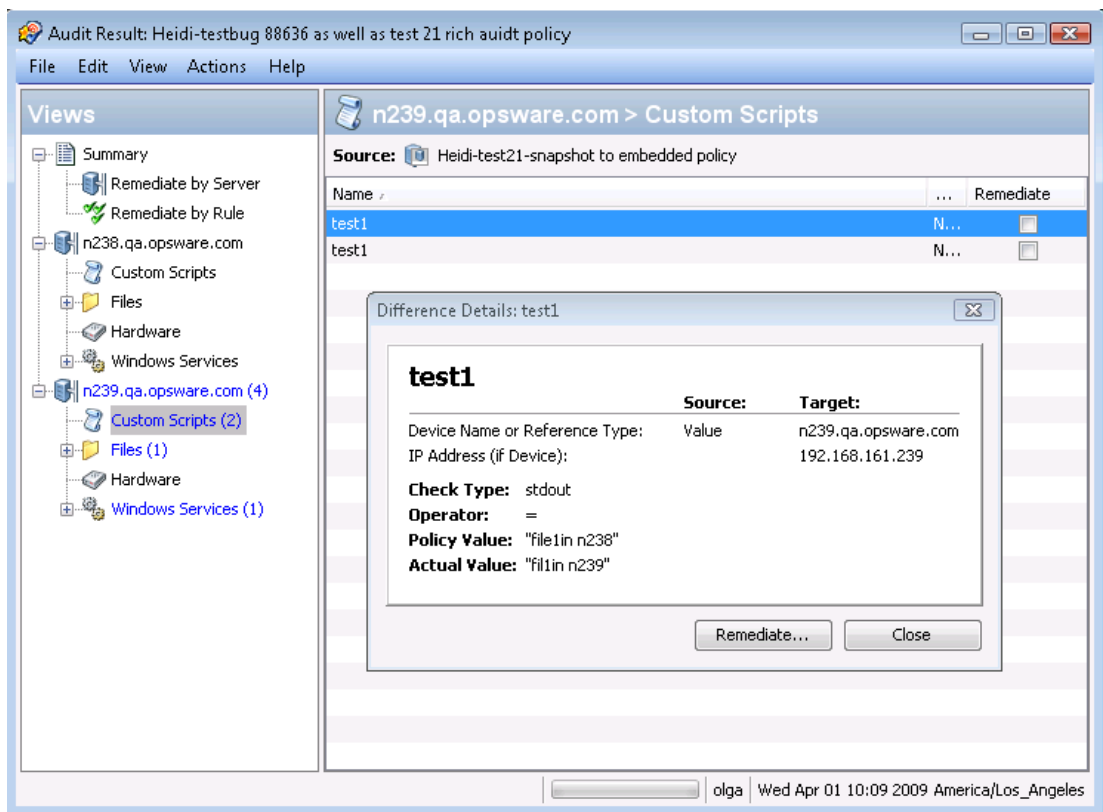
Viewing Value-Based Audit Results–Audit Rule Remediation

Value-based audit results indicates if the server configuration matches the values defined in the audit rule. You can view the differences between what was defined as the expected value in the rule and the actual value found on the target server. Depending on the rule, you can remediate the difference found on the target server by replacing it with the value specified in the rule.

Some value-based rules are not remediable. For example, Windows/Unix users and groups, the Property value check is not remediable.

Figure 20 shows a value-based audit rule in the form of a custom script where the output of the script was different than the results of the same script run on the source server. The Status column for the rule indicates Non-Compliant, which means the output of the script rule is different between the source and the target. To fix the discrepancy, select the Remediate option and select **Remediate** from the **Actions** menu. Or, double-click the rule and click **Remediate**.

Figure 20 Audit Results for a Value-Based Audit Rule



Viewing and Remediating Audit Results Differences

For some objects in an audit result, you can view those differences between object that exist on both the target and the source and that have differences between them. You can also see what is different about them and remediate them, if necessary.

For some audit rules, you can view general differences, such as a service's status, the release number for a patch, a registry key's value, and so on. For other server objects, such as files, you can view the differences of the file's contents.

Viewing and Remediating File Differences

For some rules, such as file system, you can view differences between files side by side and line by line. You can see lines that were added, deleted, or modified.

To view and remediate contents of two files that differ in an audit:

- 1 In the navigation pane select **Library** ► **By Type** ► **Audit and Remediation** ► **Audits**.
- 2 Select an audit.
- 3 In the details pane below the audit list, you see all audit results associated with the selected audit.
- 4 Select an audit result, right-click, and select **Open**.
- 5 In the Views pane of the Audit Result window, expand one of the target servers and select a result.
- 6 In the content pane, expand a target server and select one of the results.
- 7 Next, in the content pane, select the On Both but Different tab.
- 8 Select a file, right-click, and select View Differences.
- 9 In the Comparison window, select an item from the Encoding drop-down list to specify the character encoding of the data displayed.



If the file in question exceeds 2MB in file size, audit and remediation cannot display the file differences.

- 10 Click the arrows to find the first, next, previous, or last lines that were added, deleted, or modified. Differences are highlighted according to the following color scheme:
 - **Green**: This content was added.
 - **Blue**: This content was modified.
 - **Red**: This content was deleted.
 - **Black**: No changes were made to this content.
- 11 Click **Close** to close this window.
- 12 To remediate file differences, from inside the Audit Results window, select either the the Only On Source tab or On Both But Different tab, select a file, right-click and select **Remediate**.
- 13 In the Select Server window, select a server you want to copy the file from the source to, and then click **OK**.

Viewing and Remediating Object Differences

For many server objects, such as Users and Groups, IIS Metabase, Windows Registry, and so on, when there are differences between the source object and the target object, you can view differences in object properties side by side. Each server object will show different windows, depending on the object and if the audit rule set was comparison-based (comparison between source and target) or value-based (comparison between user-defined audit rule and target).

For some value-based audit rules, you can remediate the values on the target server.

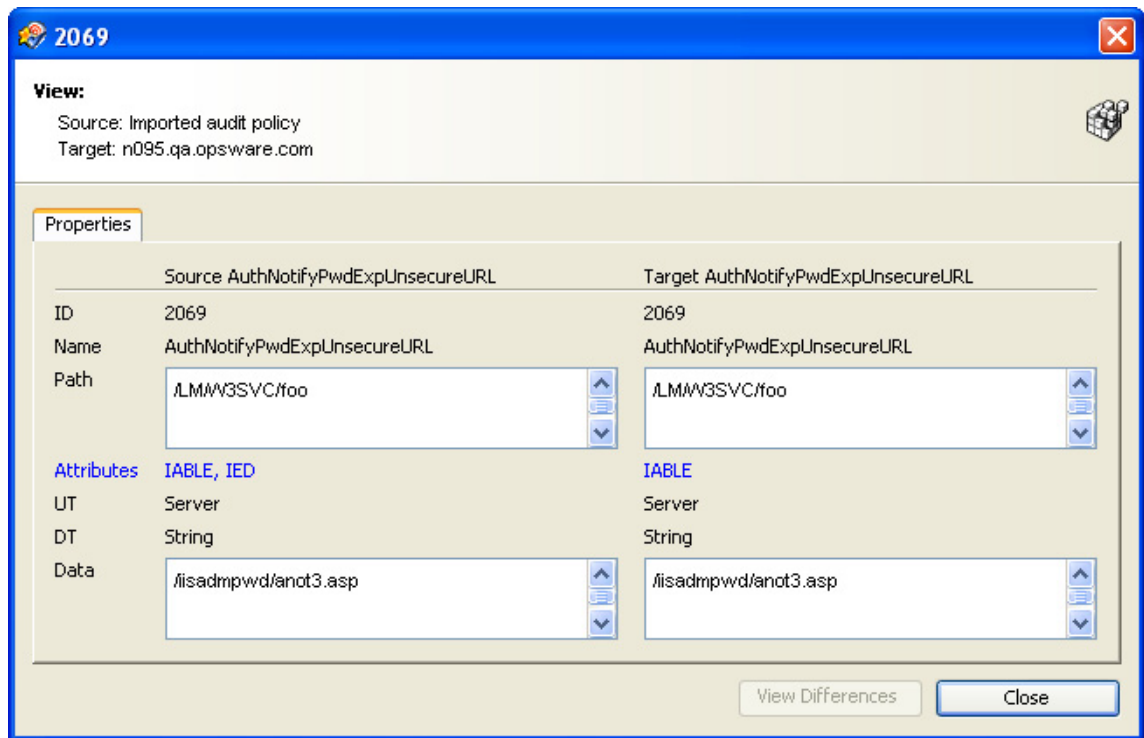
To view the contents of two objects that differ:

- 1 In the navigation pane select **Library** ► **By Type** ► **Audit and Remediation** ► **Audits**.
- 2 Select an audit.
- 3 In the details pane below the audit list, you see all audit results associated with the selected audit.

- 4 Select an audit result, right-click, and select **Open**.
- 5 In the Views pane, expand one of the target servers and select a result.
- 6 In the Views pane, select an object.
- 7 In the content pane, select the On Both but Different tab.
- 8 In the content pane, select an object, right-click, and select **Open**. You will see a window that shows the differences between the object as defined the audit and the object on the target server.

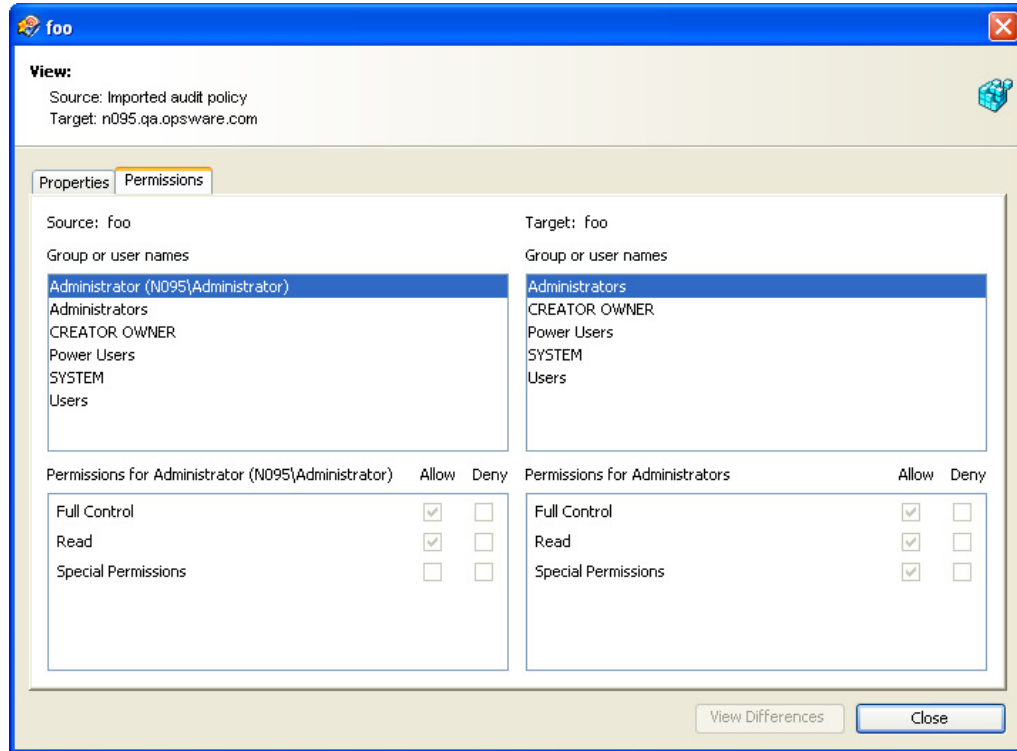
The example in [Figure 21](#) displays the audit Result differences for two IIS Metabase objects, showing an attribute of the object that exists on the server but does not exist on the source server, displayed in blue font.

Figure 21 Comparison-Based Audit Results Difference: IIS Metabase Objects



For a value-based rule, the difference window will be slightly different and will also include a Remediate option, if remediation is possible. This difference window displays the audit rule, including the policy value and the actual value found on the target server. The example in [Figure 22](#) shows the permissions differences for a value-based Windows Registry rule.

Figure 22 Rule-Based Audit Results Difference: Windows Registry Permissions Differences




- 9 To remediate the differences, select the Remediate check mark next to each rule.
- 10 From the **Actions** menu, select **Remediate**.
- 11 In the Remediate window, follow the steps to run or schedule the remediation. For more information on remediating audit results, see [Viewing and Remediating Audit Results Differences](#) on page 92.

Viewing Audit Results with Exceptions

If an audit contains rule exceptions, then the excepted rules are not checked on the target servers when the audit is run. However, your audit results will show which of the rules in the audits are exceptions, including details about the rule exceptions.

The manner in which rule exceptions are displayed in audit results depends on the type of rule that has been excepted:

- Custom script and custom or pluggable check rule exceptions (such as those created by developers or provided by a EP Content Subscription) appear in the Contents pane of the Audit Results window. You can double-click the rule exception for details on the exception.
- All other rule exceptions, such as file system, registry settings, services, IIS Metabase, and COM+ rules, the Audit Results window will display an Exceptions icon  in the Views pane, which you can select and see the details of the exception in the contents pane.

Searching for an Audit

You can use the SA Client Search tool to find audits in your facility. You can search for audits by name, by the operating system, and many other criteria.

To search for audits:

- 1 In the SA Client, make sure the search pane is activated by selecting **View ► Search** pane.
- 2 In the top drop-down list, select **Audit**.
- 3 Click the green arrow button or ENTER to execute the search.
- 4 The results appear in the content pane.

If you want to extend your search criteria, add new criteria in the search parameters section at the top of the content pane. You can also save the search by clicking **Save**, or export the Search results to .html or .csv.

Deleting an Audit

To conserve disk space, you can delete audits that you no longer need. You can choose to archive all audit results generated from the audit, if you would like to keep a record of the results.



When you delete an audit, all schedules associated with it are also deleted.

To delete an audit:

- 1 In the navigation pane, select **Library ► By Type ► Audit and Remediation ► Audits**.
- 2 Choosing either Windows or Unix, select one or more audits and then select **Actions ► Delete**.
- 3 In the Confirmation Dialog, click **Yes** to delete this audit, or click **No** if you do not want to delete it. You can also select the **Archive Audits** option, which will archive all audit results generated from the audit. If you do not select the **Archive** option, all audit results from the selected audit will be deleted.

Deleting Audit Results



Best Practice: Delete audit results that you know you will no longer need.



You must have read permissions for the snapshot to be able to delete it. To obtain these permissions, contact your SA administrator. See the *SA Administration Guide* for more information.

To delete audit results:

- 1 Select a snapshot or select multiple snapshots and then select **Actions ► Delete**.
- 2 In the Confirmation Dialog, click **Yes** to delete this snapshot or click **No** if you do not want to delete it.
- 3 If you want to archive the snapshot instead of delete it, select the snapshot, right-click, and select **Archive**.



When you delete a snapshot, you do not delete the snapshot specification that was used to create it. See [Deleting a Snapshot Specification](#) on page 109.

Archiving Audit Results



Best Practice: Some audits yield numerous results, especially audits that are scheduled to run on a recurring basis. Archive all audit results to keep a record of all audit results run from an audit. When you archive an audit result, SA removes its connection to the original audit; however, the results and targets of the audit are kept intact.

To archive audit results:

- 1 In the navigation pane select **Library ► By Type ► Audit and Remediation ► Audits**.
- 2 Select an operating system: Windows or Unix.
- 3 Select an audit.
- 4 In the details pane below the audit list, you see all audit results associated with the selected audit.
- 5 To archive an audit result, select it, right-click, and then select **Archive**.
- 6 In the Continue Archive Audit Result window, you are asked to confirm that you want to archive the audit result and remove the reference to the audit. Click **Yes** to archive the audit result and remove the link between the result and the audit.
- 7 To view all archived audit results, in the navigation pane, select **Library ► By Type ► Audit and Remediation ► Archived Audit Results**.

3 Snapshots, Snapshot Specifications, & Snapshot Jobs

Snapshots

A *snapshot* captures the configuration of a managed server at a particular point in time and provides a means of capturing the current state of a known working (or a known not working) server. A snapshot is useful for capturing a server configuration that you know represents a desired state of configuration.



Best Practice: You can also compare the snapshot with other servers in your facility by using the snapshot in an audit.

A snapshot is also a useful way to back up a managed server, especially if you plan to make changes to the server and want to keep a record of it before you change anything.

In addition to recording information about objects on managed servers, a snapshot can contain the content of some objects. A server snapshot also identifies attributes of other objects on specific types of operating systems, such as the Windows Registry and Windows Services, application configurations, COM+ objects, hardware information, installed patches, and more. You can even create custom scripts that gather data from the target managed servers.



VMware ESXi servers cannot be the source or the target of a snapshot.

The Snapshot Process

Taking a snapshot of a server configuration requires the two following basic steps:

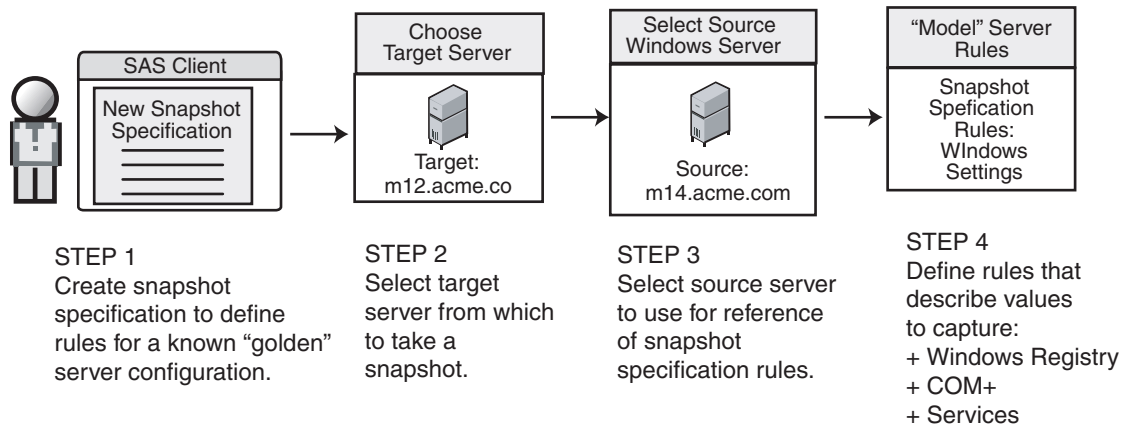
- Creating a snapshot specification, which is a template that defines the configuration parameters captured on a target server.
- Running the snapshot specification job that results in a snapshot.

Figure 23 illustrates an example of the snapshot process.

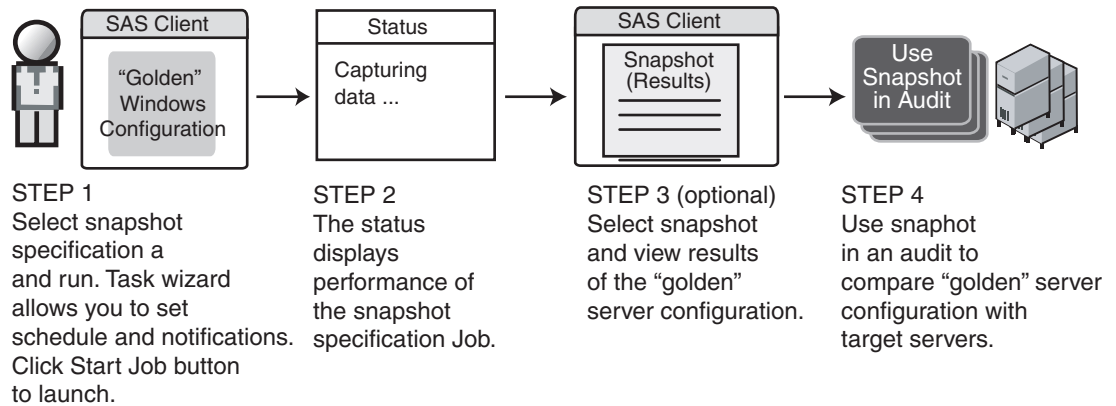
Figure 23 Snapshot Process

SNAPSHOT PROCESS - Windows Server Snapshot

Part A: Create Snapshot Specification to define “Golden” Server Configuration



Part B: Run Snapshot Specification Job and View Results in the Snapshot



Snapshots & Snapshot Specifications

Snapshots are configured in similar way as you configure an audit. First you create a *snapshot specification*, which is like a template that defines exactly what you want to capture of a server’s configuration. Then, you configure the snapshot specification’s rules, and then run it. The results are a snapshot—a picture of a server’s configuration. The main difference between a snapshot and an audit is that a snapshot takes a picture of a server’s configuration, whereas an audit compares a server configuration with the rule values that you define.

You can schedule when you want a snapshot to be created (either once or as a recurring job) and who you want to receive email notification about the status of the job.

Snapshot Used in an Audit

You can use a snapshot in an audit to compare managed servers, groups of servers, and snapshots. By using a snapshot in an audit, you can compare a problematic server (target of the audit) with a known working server (snapshot as source for the audit). To further extend the audit definition, you can also define rules for server objects.

When a snapshot is used as the source for an audit, all server configuration values captured in the snapshot results are available to use as rules for the audit. For more information about using a snapshot in an audit, see [Audit Configuration](#) on page 27.

Snapshot Specification Used in an Audit

You can use a snapshot specification as the source of an audit if you want to keep track of a server's configuration over time and monitor any changes that occur. For example, you might want to keep track of a specific application to make sure that its configuration remains correct over a period of time. If this application runs on several servers, you can create a snapshot specification that defines a desired state of server configuration, and then run the snapshot.

Next, you can create an audit and use the original snapshot specification as the source for your audit. Each server that was targeted by the snapshot are now also included as targets of the audit. Next, when you run the audit (either on-demand or on a scheduled basis), each server's current configuration will be compared with the state originally captured when you took the initial snapshot. Any changes are displayed in the audit results window. See [Audit Configuration](#) on page 27.

Snapshot Specification Elements

An snapshot specification consists of the following elements:

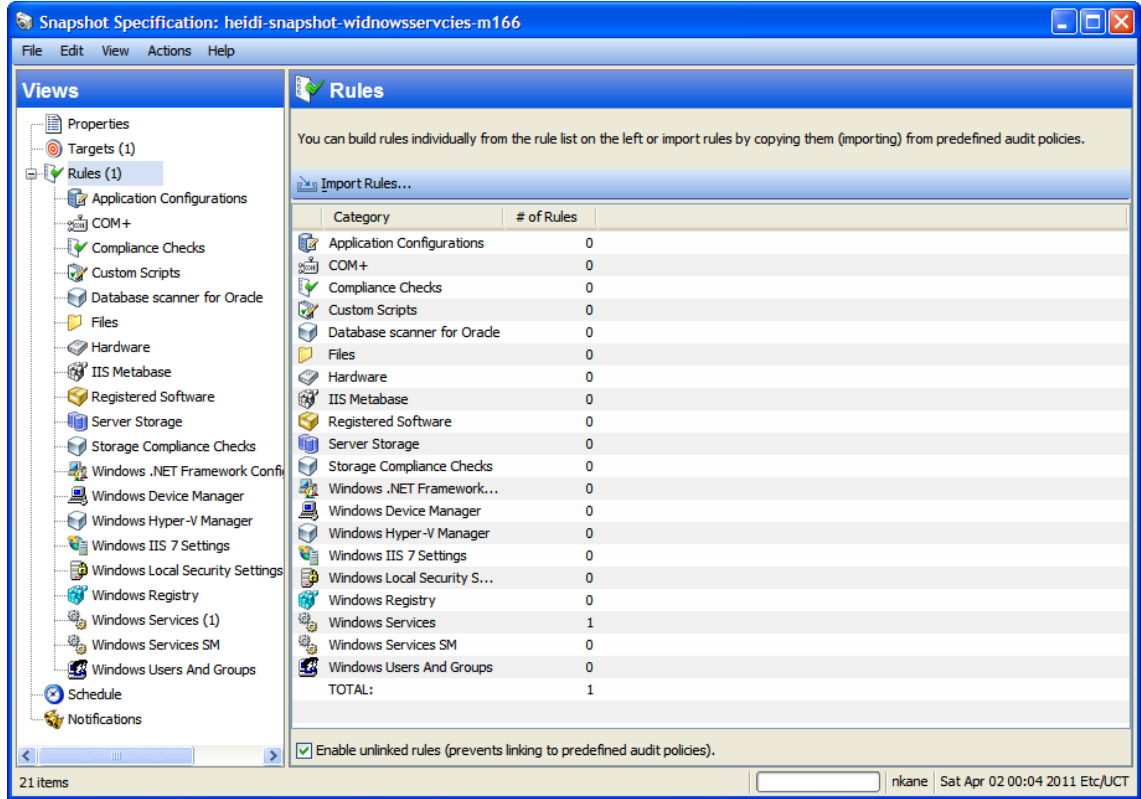
- **Properties:** The name and description of the snapshot specification. If you want to create an inventory of some snapshot specification rules, you can select the Perform Inventory and the snapshot result will collect all information about the specific rules from the target servers. This option is applies to the following rules: Discovered Software, Internet Information Server, Local Security Settings, Registered Software, Windows and Unix Users and Groups.
- **Targets:** The servers that you want to take a snapshot of — that is, capture the specific server configuration as defined in the snapshot specification's rules. You can choose as many servers and groups of servers as you want.
- **Source:** The source of a snapshot specification. If you choose a server then you can select server objects from that server as the basis of your snapshot. The source of a snapshot specification can be a server, or no source at all. (Some rules require a source server. Other rules can be defined by your own custom values without a source.)
- Note that the value of a source parameter is not used when taking a snapshot. It only has meaning when defining a snapshot specification.
- **Rules:** A check on a particular server object with a desired value and an optional remediation value. For example, you might check if a server contains a specific Windows Service, and if found, determine if the service is turned off. For a description of server objects that you can define rules for in a snapshot specification, see [Audit & Remediation Rules](#) on page 33.
- **Schedule:** The time the snapshot will run. You can run the snapshot specification as a job on a onetime basis, or on a recurring schedule.

- **Notifications:** The email notification send after the snapshot has run. You can base the notification on success, failure, or simply the completion of the snapshot specification job.

When you set up a snapshot specification, you select the objects to check for on the target server. You can also apply rules to these objects that define their desired configuration state. For some rules, you can define remediation values, in the event that the resulting snapshot is used as the source for an audit.

Figure 24 shows a snapshot specification that has three rules that will capture configuration information about the target server for event logging, operating system, and windows services.

Figure 24 Snapshot Specification Server Objects



Viewing Snapshots

After you have created a snapshot, you can view it in several locations in the SA Client.

In the SA Library

To view snapshots associated with a specific server:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Audit and Remediation** ► **Snapshot Specifications**.
- 2 Select an operating system: Windows or Unix.
- 3 In the list, select a snapshot specification. The details pane displays all snapshots that were run from the selected snapshot specification.

In the Device Explorer

To view snapshots associated with a specific server:

- 1 In the navigation pane, select **Devices** ► **Servers** ► **All Managed Servers**.
- 2 Select a server from the list, right-click, and then select **Open**.
- 3 In the Device Explorer window, select **Inventory** ► **Snapshot Specification**.
- 4 In the content pane, select a snapshot specification. The details pane displays all associated snapshots.
- 5 To view a snapshot, select it and then double-click to open it.

Searching for Snapshots

You can use the SA Client Search tool to find snapshots in your facility. You can search for snapshots by name, by the operating system, and many other criteria.

To search for snapshots:

- 1 In the SA Client, select **View** ► **Search Pane**.
- 2 From the drop down list, select Snapshot.
- 3 Click the green arrow or ENTER to start the search. The results appear in the content pane. If you want to expand your search criteria, add additional criteria in the search parameters section at the top of the content pane. You can also save the search or export the search results to .html or .csv files.

Viewing Snapshot Results

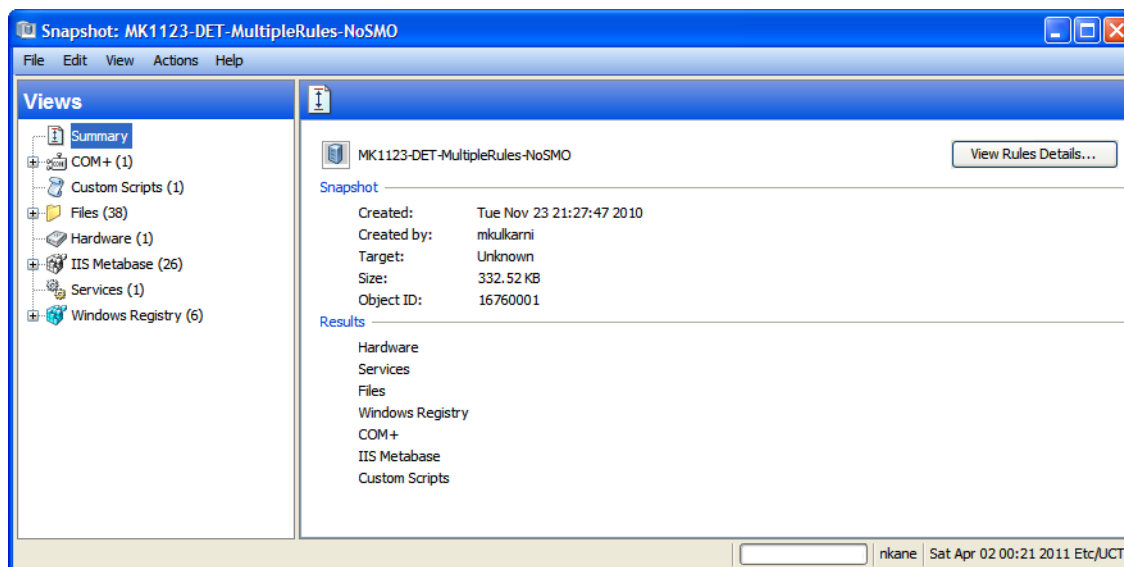
You can view the contents of a snapshot and view detailed information about the server configurations that were recorded.

For information about remediating snapshot results, see [Copying Objects](#) on page 107.

To view the contents of a snapshot:

- 1 From one of the starting points described in [Viewing Snapshots](#) on page 103, open a snapshot.

Figure 25 Snapshot of a Windows Server



- 2 In the Snapshot window, you can select or expand the following server objects in the Views pane:
 - **Summary:** Displays general information about a snapshot, such as the date and time the snapshot was created and by whom, the snapshot source (name of the managed server), the size of the snapshot file, and a snapshot ID number.

You can also click **View Rules Details** to see the snapshot specification which this snapshot is based on.
 - **Compliance Library:** Information relevant to the specific compliance checks configured in the snapshot specification. For more information about the types of BSA Essentials Subscription Services compliance checks available and how to configure them, see [Configuring Compliance Checks](#) on page 64.
 - **Installed Hardware:** Information about the type of CPU processor and speed, cache size, memory size for SWAP and RAM, and storage devices that were recorded in the snapshot.
 - **Installed Patches:** Displays information about the installed patches that were recorded in the snapshot, such as the patch type.
 - **Installed Packages:** Displays information about the installed packages that were recorded in the snapshot, such as package type, package version, and release number.
 - For .zip packages, the Snapshots do not show a version number, but instead displays the install path of the package on the server.
 - **Event Logging:** Displays security, application, and system log files recorded in the snapshot.

- **File System:** Displays the directories, file properties, attributes, and contents of the files recorded in the snapshot.



If a file in the snapshot exceeds 2MB in file size, audit and remediation cannot display the file contents.

- **Windows Services:** Displays information about the running services recorded in a snapshot, such as the name, description, startup state, startup type, and log on account.
 - **Windows Registry:** Displays information about Windows Registry entries in the snapshot, such as the registry key, registry value, and subkey. A registry key is a directory that contains registry values, where registry values are similar to files within a directory. A subkey is similar to a subdirectory. The content area in this window excludes subkeys. audit and remediation supports the following Windows Registry keys: HKEY_CLASSES_ROOT, HKEY_CURRENT_CONFIG, HKEY_LOCAL_MACHINE, and HKEY_USERS.
 - **COM+:** Displays information about Windows COM (Component Object Model) objects in the snapshot, such as the name and GUID (Globally Unique Identifier) of the object, and the path to the in-process server DLL.
 - SA provides warning messages that explain how Windows COM folders were processed. The following scenarios apply:
 - When you create a snapshot and select a Windows COM folder that does not contain any objects, the snapshot window displays a summary. SA displays a warning that the GUID (Globally Unique Identifier) for that folder is invalid, which means that the Windows COM folder does not contain any objects.
 - When you create a snapshot specification and select a Windows COM+ object that does not exist on a target, SA displays a warning that the folder is invalid.
 - When you create a snapshot and select a Windows COM+ folder that does not contain any objects, SA displays a warning that the folder is empty.
 - **Metabase:** Displays information about IIS Metabase objects in the snapshot, such as the ID, name, path, attributes, and data of the object.
 - **Custom Scripts:** Displays information about the custom script rule recorded in the snapshot.
 - **Users and Groups:** Displays information about users and groups on servers, such as user name for last login, whether or not CTRL + ALT + DELETE is enabled, and so on.
- 3 Click **Close** to close the object browser.

Archiving a Snapshot

Some snapshot specification yield numerous snapshots, especially those scheduled to run on a recurring basis. You can archive all snapshots to keep a record of all snapshots run for a server or group of servers.

When you archive a snapshot, it detaches the snapshot from the server and removes its connection to the original snapshot specification.

To archive a snapshot:

- 1 In the navigation pane select **Library** ► **By Type** ► **Audit and Remediation** ► **Audits**.
- 2 Select an audit. In the details pane below the audit list, you see all audit results associated with the selected audit.
- 3 To archive an audit result, select it, right-click, and then select **Archive**.
- 4 You are asked to confirm if you want to archive the audit result, since doing so will remove the link between the result and the audit. Click **Yes** to archive the audit result.
- 5 To view all archived audit results, in the navigation pane, select **Library** ► **By Type** ► **Audit and Remediation** ► **Archived Snapshots**.

Deleting a Snapshot



Best Practice: You should delete snapshots from the Software Repository only if you no longer need them. This helps conserve disk space.



You must have read permissions for the snapshot to be able to delete it. To obtain these permissions, contact your SA administrator. See the *SA Administration Guide* for more information.

To delete a snapshot:

- 1 Select a snapshot or select multiple snapshots and then select **Actions** ► **Delete**.
- 2 In the Confirmation Dialog, click **Yes** to delete this snapshot or click **No** if you do not want to delete it.
- 3 If you want to archive the snapshot instead of delete it, select the snapshot, right-click, and select **Archive**.



When you delete a snapshot, you do not delete the snapshot specification that was used to create it. See [Deleting a Snapshot Specification](#) on page 109.

Exporting/Importing a Snapshot

Use the snapshot filter to tell DET what snapshot to export from an SA core/mesh so that you can then import it into another SA core/mesh. See the *SA Content Utilities Guide*.

Copying Objects

From a Snapshot to a Server

After viewing snapshot contents, you can copy certain objects to a target server. audit and remediation allows you to copy directories, files, windows services (state only), IIS Metabase objects, COM+ objects and categories, and Windows Registry keys to a managed server.



You must have write permission on the destination server to be able to copy an object to it. To obtain these permissions, contact your SA Administrator. See the *SA Administration Guide* for more information on permissions.



In order to copy COM+ rule snapshot results from a snapshot to a server, you must have selected the “Archive all associated files” option when you configured the COM+ rule. Also the COM+ object being copied must not be in use by any application in order for the copy to remediation to work. See [Configuring COM+ Rule](#) on page 40.

Before you copy these objects over to a managed server, it is important to understand what actually gets copied to or created on the destination server:

- When you select a directory, only the directory will be copied to the destination server, excluding any files in that directory. For example, if dir1 contains file1 and file2, and you select dir1, audit and remediation copies only dir1 (not file1 and file2) to the destination server.
- When you select a file and its parent directory does not exist on the destination server, audit and remediation will create the directory on and copy the files to the destination server. For example, if you select file1 and dir1 does not exist on the destination server, audit and remediation will create dir1 on and copy file1 to the destination server.
- When you copy a Windows Services object, you copy the state of the service, such as started, stopped, paused, and so on. You can select one or more Windows Services objects for a single copy process.
- When you copy a Windows Registry object, you can select one or more registry keys and subkeys for a single copy process.
- ACLs are not copied along with COM+ objects or Microsoft IIS objects to the target server.
- When remediating COM+ objects from snapshot results using copy to, the SA Client does not check the version of the COM+ object, and thus will always copy the object, whether or not there is any difference between them.

From a Snapshot to a Server

To copy an object from a snapshot to a managed server:

- 1 Open a snapshot. See [Viewing Snapshots](#) on page 103.
- 2 In the Views pane, select a file system, Windows Services, or a Windows Registry object.
- 3 In the content pane, select one or more objects that you want to copy.
- 4 Select **Actions** ► **Copy To**.

- 5 In the Select Server window, select a destination server.



Use the search tool to dynamically filter this list by entering a server name, IP address, or operating system.

- 6 Click **Select** to copy the object to that managed server or click **Cancel** to close this window without saving your changes.

Snapshot Specifications

The SA Client lets you perform the following tasks to manage your snapshot specifications:

- [Snapshot Specifications & Audit Policies](#) on page 108
- [Creating a Snapshot Specification](#) on page 108
- [Deleting a Snapshot Specification](#) on page 109
- [Configuring a Snapshot Specification](#) on page 109
- [Configuring Snapshot Specification Rules](#) on page 111
- [Saving a Snapshot Specification as an Audit Policy](#) on page 111
- [Running a Snapshot Specification](#) on page 112
- [Scheduling a Recurring Snapshot Job](#) on page 113

Snapshot Specifications & Audit Policies

An audit policy is collection of rules that defines a desired state of a server's configuration. An audit policy can be used inside a snapshot specification, either through linking or importing. An audit policy is useful because it allows a policy setter to define server configuration compliance values, which then can be used by others in their snapshot specifications.

Because an audit policy can be linked to an audit or snapshot specification, whenever a change is made to the policy, the audit or snapshot specification using the policy will also reflect the latest changes. Or, an audit policy can be imported into a snapshot specification, without keeping the link to the source audit policy. When you import an audit policy into a snapshot specification, you can choose to replace any current values in the audit or merge values from the audit policy with those in the snapshot specification.

Creating a Snapshot Specification

You can create a snapshot specification from the following locations in the SA Client:

- [From a Server](#) on page 109
- [From the SA Library](#) on page 109



You must have a set of permissions to create and modify snapshot specifications. To obtain these permissions, contact your SA administrator. See the *SA Administration Guide* for more information on permissions.

From a Server

When you create a new snapshot specification from a managed server, the snapshot specification will use the selected server as its source. You can choose several different server sources for the snapshot specification as you define the rules or choose no source at all and define your own custom rules. However, some rules require a source.



To take a snapshot of a managed server, the server must be reachable and you must have access to the server.

To create a snapshot specification from a server:

- 1 In the navigation pane, select **Devices** ► **Servers** ► **All Managed Servers**.
- 2 Select a server and then select **Actions** ► **Create Snapshot Specification**.

From the SA Library

If you want to create a new snapshot specification and set all your own rules, create the audit from the SA Client Library by performing the following steps:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Audit and Remediation**.
- 2 In the navigation pane, select snapshot specifications, and then select Windows or Unix.

Deleting a Snapshot Specification

To conserve disk space, you can delete snapshot specifications that you no longer need. You can choose to archive all snapshots generated from the snapshot specification, if you would like to keep a record of the results. Or, you can choose to delete the snapshot specification and all snapshots associated with it.

To delete a snapshot specification:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Audit and Remediation** ► **Snapshot Specifications**.
- 2 Select Windows or Unix.
- 3 Select one or more snapshot specifications and then select **Actions** ► **Delete**.
- 4 In the Confirmation Dialog, click **Yes** to delete this snapshot specification or click **No** if you do not want to delete it. You can also select the Archive Snapshots option, which will archive all snapshots generated from the snapshot. If you do not select the Archive option, all snapshots generated from the selected snapshot specification will be deleted.



When you delete a snapshot specification, all schedules associated with it are also deleted. See [Snapshot Jobs](#) on page 113.

Configuring a Snapshot Specification

The following tasks are required to configure a snapshot specification:

- Name and describe the snapshot specification, and decide if you want to perform an inventory.
- Choose target servers you want to take a snapshot of. You can choose to snapshot multiple servers or groups of servers.

- Configure your own custom rules, or choose settings from a source server to serve as the basis for the snapshot specification rules.
- Schedule the snapshot specification job to run once or on a recurring schedule.
- Set up email notifications to notify users when the snapshot specification job finishes successfully, if the job fails, or on both conditions.
- Save the snapshot specification.



If you take a snapshot of COM+ objects from a 32 bit Windows server and you attempt to remediate the results using copy to on to a Windows 64 bit server, this action might fail.



VMware ESXi servers cannot be the target of an audit or snapshot.

To configure a snapshot specification:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Audit and Remediation**.
- 2 In the navigation pane, select Snapshot Specifications, then either Windows or Unix.
- 3 From the **Actions** menu, select **New**.
- 4 In the Snapshot Specification window, enter the following information:
 - **Properties:** Enter a name and description for the snapshot specification. Also, for certain snapshot specification rules (Discovered Software, Internet Information Server, Local Security Settings, Packages and Patches, Windows and Unix Users and Groups), you can select the Perform Inventory option, which will capture all resources associated with the rule.
 - **Source:** Select a source for the snapshot specification. By default, the source server for the snapshot specification will be the managed server that you chose as the source for the snapshot specification. Browse the source server for values to populate the snapshot specification's rules. You can also choose a different source server as the basis of the snapshot specification for each rule category, or no source at all. If you choose no source, you must define your own rules, or choose to link to an audit policy in the rules section.
 - **Rules:** Choose a rule category from the list to begin configuring your snapshot specification's rules. Since each rule is unique and requires its own instructions, to configure specific rules see [Audit & Remediation Rules](#) on page 33.

If you want to use an audit policy to define the rules of your snapshot specification, click either **Link Policy** or **Import Policy**. When you link an audit policy, the snapshot specification maintains a direct connection with the audit policy, so if any changes are made to the policy, the snapshot specification will update it with the new changes. If you import an audit policy, the snapshot specification will use all the rules defined in the policy but will not maintain a link to the audit policy. For information on how to import or link to a snapshot specification, see [Ways to Link & Import Audit Policies](#) on page 81.

- **Targets:** Choose the Targets of the snapshot specification. These are servers or groups of servers that you want the configured snapshot specification rules to capture. To add a server or group of servers, click **Add**. To choose a source server to use to create the snapshot specification rules, click **Select**.
- **Schedule:** Choose to run the snapshot specification immediately, or on a recurring schedule. Choose whether you want to run it once, daily, weekly, monthly, or on a custom schedule. Parameters include:
 - **None:** No schedule will be set. To run the snapshot specification, select the snapshot specification, right-click, and select **Run snapshot specification**.

- **Daily:** Choose this option to run the snapshot specification on a daily basis.
- **Weekly:** Choose a day of the week to run the snapshot specification.
- **Monthly:** Choose the months to run the snapshot specification.
- **Custom:** In the Custom Crontab string field, enter a string that indicates a time schedule. The crontab string can include serial (1,2,3,4) and range (1-5) values. For example, the following crontab string will create the snapshot at midnight every weekday:

```
0 0 * * 1-5
```

An asterisk (*) in any of these fields represents all days of the month, all months of the year, all days of the week, and so on. For more information about crontab entry formats, consult the Unix man pages.

- **Time and Duration:** For each type of schedule, specify the hour and minute you want the daily schedule to start. Unless you specify an end time, the snapshot specification will keep running indefinitely. To choose an end date to end the snapshot specification schedule, select End, and from the calendar selector, choose a date. The Time Zone is set according to the time zone set in your user profile.
- **Notifications:** Enter the email addresses (separated by a comma or a space) of those you want to receive an email when the snapshot specification Job finishes running. You can choose to send the email notification on both success and the failure of the snapshot specification job (not the success of the audit rules). To add an email address, click **Add Notification Rule**.

5 When you have finished configuring the snapshot specification, from the **File** menu, select **Save**.



To prevent runaway processes, the snapshot process will time out if it exceeds 60 minutes or if the data that is collected from a managed server exceeds 1 gigabyte (GB). If you specify that you want to collect the full contents of files in the selection criteria, the data collected might exceed the maximum size that can be successfully recorded in a snapshot.

Configuring Snapshot Specification Rules

For information on how to configure specific snapshot specification rules, see [Audit & Remediation Rules](#) on page 33.

Saving a Snapshot Specification as an Audit Policy

You can save selection criteria used in a snapshot and save it as an audit policy. This can be useful if you would like to use the rules configured in a snapshot specification for other snapshot specifications or audits.



All audit policies you create must be saved in the SA Library in a folder. You must have permissions to write to the folder you want to save the audit policy to. For more information on folder permissions, see the *SA User Guide: Server Automation* or contact your SA Administrator.

To save your snapshot specification as an audit policy:

- 1 Launch the SA Client.
- 2 In the navigation pane, select **Library** ► **By Type** ► **Audit and Remediation**.
- 3 Select Snapshots Specification and then double-click a snapshot specification that you want to save as an audit policy.

- 4 In the Snapshot Specification window, select **File** ► **Save As**.
- 5 In the Save As window, enter a name and a brief description.
- 6 From the Type drop-down list, select Audit Policy.
- 7 Click **Save**. The selected snapshot specification has been saved as an audit policy.
- 8 To view the audit policy, from the navigation pane, select **Library** ► **By Type** ► **Audit and Remediation** ► **Audit Policies**. For more information about using audit policies, see [Audit Policy Management](#) on page 78.

Running a Snapshot Specification

When you run a snapshot specification, SA captures (from the target servers) all configuration parameters configured in the rules. After you run a snapshot specification, the results of the snapshot job become a snapshot and can be viewed inside the snapshot.

To run a snapshot specification:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Audit and Remediation**.
- 2 In the navigation pane, select Snapshot Specifications.
- 3 Select Windows or Unix.
- 4 Select a snapshot specification, right-click, and then select **Run**. In the Run Snapshot Specification window, step one shows you the name of the snapshot, the total number of rules defined, and all targets.
- 5 Click **View Rules Details** to view the rule definitions.
- 6 Click **Next**.
- 7 In the Scheduling window, choose whether you want the audit to run immediately or at a later date and time. To run the audit at a later time, select the second option and choose a date and time.
- 8 Click **Next**.
- 9 In the Notifications page, by default your user will have a notification email sent when the audit completes, whether or not the audit job is successful. To add an email notifier, click **Add Notifier** and enter an email address.
- 10 *(Optional)* You can specify if you want the email to be sent on success of the audit job () or failure of the audit job ().
- 11 *(Optional)* You can specify a Ticket Tracking ID in the Ticket ID field. The ticket ID field is only used when HP Professional Services has integrated SA with your change control systems. Otherwise, leave this field empty.
- 12 Click **Next**.
- 13 In the Job Status page, click **Start Job** to run the audit. When the audit has run, click **View Results** to view the results of the audit.

Snapshot Jobs

A snapshot specification job enables you to specify when you want the SA Client to create a snapshot (either once or on a recurring basis) and who you want to receive email notification about the status of the job. You can also view, edit, and delete existing snapshot specification schedules. When you delete a snapshot specification, all schedules associated with that snapshot specification will be deleted.

The SA Client lets you perform the following tasks to manage your snapshot jobs:

- [Scheduling a Recurring Snapshot Job](#) on page 113
- [Viewing and Editing a Snapshot Job Schedule](#) on page 114
- [Deleting a Snapshot Job Schedule](#) on page 115

Scheduling a Recurring Snapshot Job

After you have created, configured, and saved an snapshot specification, you can schedule snapshot specification a recurring snapshot job. After the schedule is set, you can edit the schedule according to your needs.

To schedule a recurring snapshot specification:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Audit and Remediation** ► **Snapshot Specifications**.
 - 2 Select either Windows or Unix.
 - 3 Select a snapshot and then double-click to open it.
 - 4 In the Snapshot Specification window Views pane, select Schedule.
 - 5 In the Schedule section, choose to run the snapshot job immediately or on a recurring schedule. Choose to run it once, daily, weekly, monthly, or on a custom schedule:
 - **None:** No schedule will be set. To run the snapshot job, select the snapshot specification, right-click, and select **Run Audit**.
 - **Daily:** Choose to run the snapshot job on a daily basis.
 - **Weekly:** Choose a day of the week to run the snapshot specification job.
 - **Monthly:** Choose the months to run the snapshot specification job.
 - **Custom:** In the Custom Crontab string field, enter a string the indicates a time schedule. The crontab string can include serial (1,2,3,4) and range (1-5) values. For example, the following crontab string will create the snapshot at midnight every weekday:

```
0 0 * * 1-5
```

An asterisk (*) in any of these fields represent all days of the month, all months of the year, all days of the week, and so on. For more information about crontab entry formats, consult the Unix man pages.
- In the Time and Duration section, for each type of schedule, specify the hour and minute you want the daily schedule to start. Unless you specify an end time, the snapshot specification job will keep running indefinitely. To choose an end date to end the audit schedule, select End, and then choose an end date. The Time Zone is set according to the time zone set in your user profile.
 - *(Optional)* Unselect the End option if you want the snapshot specification job to run indefinitely.

- 6 To save the snapshot specification job schedule, from the **File** menu select **Save**. The snapshot specification will now run according to the defined schedule.

Viewing and Editing a Snapshot Job Schedule

You can edit a snapshot specification schedule after you have created (or edited) and saved it.

To edit a scheduled snapshot specification:

- 1 In the navigation pane, select Jobs and Sessions.
 - 2 Select Recurring Schedules.
 - 3 From the drop-down list, select Create Snapshot. The list shows all scheduled snapshot specification jobs.
 - 4 To view a scheduled snapshot specification, double-click one.
 - 5 Select the Schedule object in the Views pane.
 - 6 To edit the snapshot specification job schedule, modify the following parameters:
 - **Schedule:** Choose to run the snapshot specification immediately, or on a recurring schedule. Choose to run it once, daily, weekly, monthly, or on a custom schedule. Parameters include:
 - **None:** No schedule will be set. To run the snapshot specification, select the snapshot specification, right-click, and select **Run snapshot specification**.
 - **Daily:** Choose to run the snapshot job on a daily basis.
 - **Weekly:** Choose the day of the week you want the snapshot job to run.
 - **Monthly:** Choose the months to run snapshot specification job.
 - **Custom:** In the Custom Crontab string field, enter a string that indicates a time schedule. The crontab string can include serial (1,2,3,4) and range (1-5) values. For example, the following crontab string will create the snapshot at midnight every weekday:

```
0 0 * * 1-5
```

An asterisk (*) in any of these fields represents all days of the month, all months of the year, all days of the week, and so on. For more information about crontab entry formats, consult the Unix man pages.
 - **Time and Duration:** For each type of schedule, specify the hour and minute, the day of the week (and month) you want the daily schedule to start. Unless you specify an end time, the snapshot specification job will keep running indefinitely. To choose a date to end the snapshot specification job schedule, select End and then choose a date. The Time Zone is set according to the time zone set in your user profile.
 - *(Optional)* Unselect the End option if you want the snapshot specification schedule to run indefinitely.
- 7 To save the snapshot specification schedule, from the **File** menu select **Save**. The snapshot job will now run according to the defined schedule.

Deleting a Snapshot Job Schedule

To delete a snapshot job schedule:

- 1 In the navigation pane, select Jobs and Sessions.
- 2 Select Recurring Schedules.
- 3 From the drop-down list, select Create Snapshot.
- 4 The content pane displays all snapshot specification jobs that have been run on this SA core. To display only snapshot specification jobs, from the drop-down list at the top of the content pane, select Run Snapshot Task. If you want to see only those snapshot specifications that you have scheduled or run, enter your user ID in the User ID field at the top of the content pane.
- 5 To delete the schedule, select it, right-click, and then select **Delete Schedule**.

4 Compliance in the SA Client

Overview

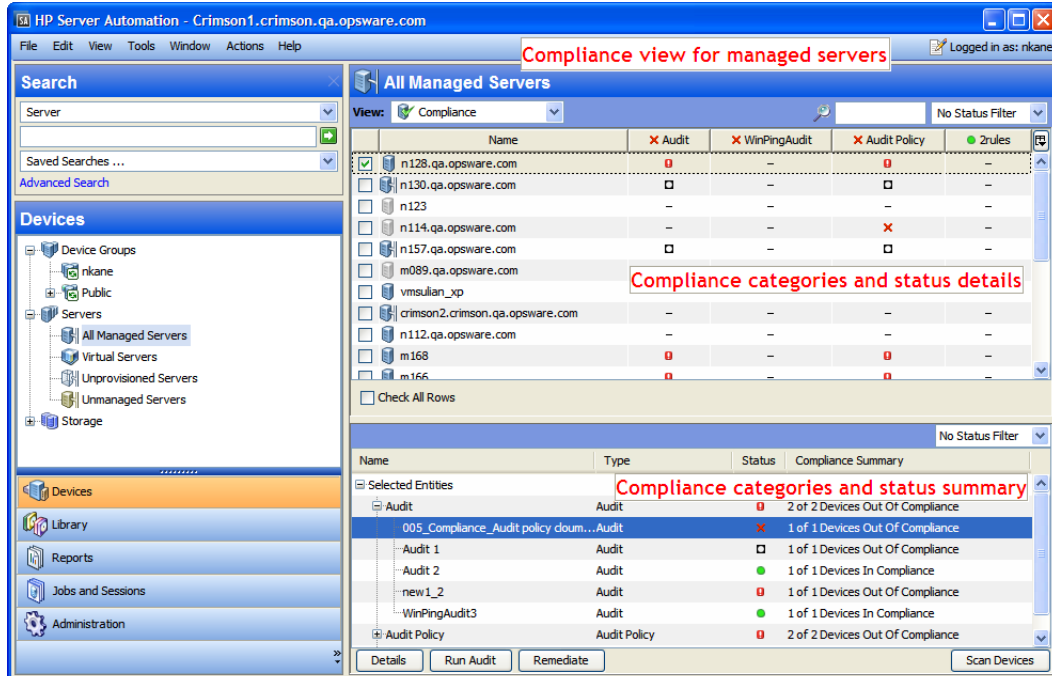
In the SA Client, the Compliance view allows you to see the overall compliance levels for all servers and groups of servers in your facility. From this view, which is commonly known as the *compliance dashboard*, you can remediate servers that are *out of compliance*. You can view compliance for an individual server, multiple servers, groups of servers, or for all servers under SA management.

The compliance dashboard displays the results of all compliance statuses on servers or groups of servers for audits, audit policies, software policies, patch policies, and application configurations. A server's compliance status is based on a *compliance policy*. A compliance policy defines unique server configuration settings or values to ensure that your IT environment is configured as it should be.

A compliance policy is typically created and defined by a *policy setter*. In some environments, a system administrator might be required to create an ad-hoc policy. The policy setter creates compliance policies and then attaches them to servers to ensure that servers are compliant with your organization's standards and policies. For example, a policy setter can create a software policy that defines a standard set of patches and packages that must be installed on a server. The policy setter can also define the manner in which certain application files must be configured on a server. A server or group of servers is considered *compliant* if its configuration matches the rules, defined by the policy setter, in the compliance policy.

The compliance dashboard allows you to determine whether the server's actual installed software, packages, patches, and configuration files settings match the configuration defined in the *software policy*. The Compliance view allows you to view compliance for groups of servers, showing a compliance status rollup for all members and sub-group members of a group. From the Compliance view, you can discover servers and groups of servers that are *out of compliance* and then remediate any problems. See [Figure 26](#) and [Figure 30](#).

Figure 26 Compliance View—Managed Servers



The information displayed in the compliance dashboard is as up-to-date as the last time the SA Client requested compliance information from the core. By default, the SA Client checks for new compliance information every 5 minutes. For information on how to change this time interval, see [Setting Automatic Compliance Check Frequency](#) on page 133.



Press **Ctrl + F5** to immediately retrieve the latest compliance information, instead of waiting for the default setting (5 minutes) to lapse.



Best Practice: Routinely review the compliance dashboard to assess server compliance levels and perform any necessary actions to fix problems. For example, use the Compliance view to determine the status of an individually scheduled audit that makes sure a Web application’s configuration, such as Apache’s http.conf file, meets the standards set by your group. You want to ensure that no one has changed the application’s configuration. To verify that no unwanted changes have been made, you should regularly check the Compliance view on this server’s Device Explorer to see if this scheduled audit’s compliance status has changed to Non-Compliant. If the status has changed to Non-Compliant, view the audit results and remediate the problem.



Best Practice: Use the compliance dashboard to help you answer a specific question or diagnose a specific problem. For example, create a scheduled audit that defines security standards for a group of servers in your facility. This audit example requires that all Windows 2003 servers contain a certain security patch. When Microsoft releases a new security patch, you need to identify your Windows 2003 servers that contain the new patch and those that do not. Update the audit to contain the new security patch and then browse the Windows 2003 servers in the device group’s Compliance view. Rerun the audit to find servers that require the patch and then remediate them by installing the new, required security patch.

Terminology

The following list defines key terms and concepts used in Server Automation server compliance:

- **Compliance:** The degree to which a server's configuration conforms to a check or test established in a collection of rules defined in an audit, a snapshot specification, or an audit policy. Compliance in Audit and Remediation is defined by the audit's or snapshot's rules that specify the values expected of the target servers. If the values on the target server are different than specified in the audit's rules, the server is considered Non-Compliant.
- **Compliance Category:** The Compliance view displays compliance statuses for the following compliance categories: Audit, Audit Policy, Software, Patch, Patch Policy, and Configuration (Application Configuration).
- **Compliance Policy:** The user-defined configuration that expresses the desired state for a server or device configuration or setting.

Examples:

A patch policy defines the specific patches that must be installed on a computer.

An audit policy might define that a certain Windows service must be disabled at all times.

An application configuration policy defines the way in which a configuration file must be configured.

- **Compliance Rule:** The content or setting inside of a policy that defines an ideal configuration for a server, such as a patch or package, a file configuration, software installation order, user and group membership and privileges, and so on.
- **Compliance Statuses:** Indicates the compliance status for a compliance category, reporting the differences between what should be (compliance policy) and what actually is (server configuration). For example, software compliance category in the Compliance view displays a status of Compliant if all configurations defined in the policy match the server configuration. Compliance calculation for groups is slightly different than individual servers.
- **Compliance Scan Results:** The results of a compliance scan. These results report the compliance status, details, and can also include remediate options.
- **Compliance Scan:** The mechanism that checks servers targeted by a compliance policy (audit, software, patch, and application configuration) and returns the results to the SA Client. A compliance scan could check to see what patches are installed on a computer targeted by a patch policy or software policy and return the results, or it can check a configuration file's contents and determine if it matches the rules defined in an application configuration. In the Compliance view, you can perform a compliance scan for the Software, Patch, and Configuration compliance categories. Audits do not have a scan feature; however, running an audit achieves the same results. Running an audit checks the servers targeted by the audit to determine if they are in compliance with an audit's rule definitions.
- **Compliance View:** Displays overall and individual compliance levels for all managed servers or groups of servers in your facility. This view is also known as the *compliance dashboard*.


Compliance Categories


The Compliance view for servers and groups of servers displays compliance for the following categories:

- **Audit:** Audit compliance represents an aggregate of all audits that run on a recurring schedule and indicates whether or not the rules defined in a scheduled audit match what is installed and configured on a target server or servers.
- **Audit Policy:** An audit policy is associated with a managed server via an audit. An audit links to an audit policy for the compliance rules and defines a list of servers and server groups for which to verify the rules. Optionally, the audit can define a recurring schedule. An audit policy can contain other audit policies.
- **Software:** Software compliance is determined by whether or not a software policy definition matches what is installed on a server. A software policy defines patches, packages, and application configurations, and scripts, including a host of other server objects, such as services, Windows registry, COM+, IIS Metabase, and so on. A software policy can also contain other software policies. See the *SA User Guide: Software Management* for more information.
- **Patch:** Patch compliance is determined by whether or not the patch policy definition matches the patches that are installed on a server or group of servers. The Compliance view displays compliance information for Windows patches only. See the *SA User Guide: Server Patching* for more information.
- **Configuration:** Configuration compliance is determined by whether or not the application configuration definition matches the configurations on a server or on a group of servers. An application configuration defines the configuration settings and values for application configuration files. Configuration compliance status is always an aggregation of all application configurations that are attached to the server. Individual status is not supported. See the *SA User Guide: Application Configuration* for more information. See also these sections:

Compliance Statuses

In general, a server or group of servers can be *Compliant* or *Non-Compliant*. This information is displayed in the Compliance View.

Compliant : The Compliance view displays this icon when a server is in compliance with the policy attached to it. A server is considered Compliant if the rules defined in the policy match the actual configuration on the server that the policy is attached to.

Non-Compliant : The Compliance view displays this icon when the server's actual configuration does not match the rules configured in a policy. For example, you can configure an audit to make sure that a Windows 2003 server has the Windows CIS recommended minimum password length of at least 8 characters. When the audit runs and checks the server's user password and discovers a user password that is only 4 characters, the Compliance view shows the server's audit policy as Non-Compliant.



Best Practice: Do not confuse *non-compliant rules* with *object differences*. A non-compliant rule can show more than one object difference. SA counts non-compliant rules—it does not count object differences. For example, when a directory rule includes many files (objects) in that directory and the audit finds that some objects are different, SA counts this as *one* difference. SA does not count this as *multiple* differences. In the SA Client, the Compliance view and the summary view in the Audit Results browser display a count for non-compliant rules. These views do not show a count for object differences.

When more than one policy is attached to a server, the aggregation column combines (rolls up) the status of all policies. If this server belongs to a device group of multiple servers, you can access the Compliance view for the group to see compliance status levels for all audits that run on all servers in the group, including servers in any sub-groups. The method used for determining compliance statuses for groups is based on a default calculation. The group of servers is considered Compliant if at least 95% of the servers that belong to the group have a status of Compliant. If less than 95% of the servers have a status of Compliant, the status of the group is shown as Partial Compliant.

You can customize the default compliance status threshold for groups of servers. See [Changing Device Group Compliance Settings](#) on page 124.



It is possible that actual server configurations, including policy information, might have changed from the last time you viewed compliance for a server or group in the Compliance view. To get the latest compliance data from the SA core, select **Refresh** from the **View** menu or press **Ctrl + F5**. You can also run a compliance scan on the server or group to determine the latest compliance status.

Compliance Status Definitions

Table 3 lists default compliance statuses for a policies, servers, and device groups.

Table 3 Compliance Status Icons







Icon	Compliance Status Description
	<p>Compliant</p> <ul style="list-style-type: none"> • Policy: All rules or items defined in the policy match the actual server configuration. • Servers: Compliance scan ran successfully and the server configuration matches <i>all</i> rules defined in <i>all</i> policies attached to the server. • Device Groups: Compliance scan ran successfully and the percentage of compliant servers is greater than the minimum threshold set in the Compliance Settings option in the Administration pane. By default, the threshold for a Compliant status is 95% of servers in the group. The compliance threshold definitions for Compliant can be modified.
	<p>Partial Compliance</p> <ul style="list-style-type: none"> • Policy: One or more rules or items defined in the policy does not match the actual server configuration, due to an exception applied to one of the rules. <i>This applies only to Windows Patch policies.</i> • Servers: Compliance scan ran successfully and the server configuration did not match at least one of the rules defined in any of the policies attached to the server, due to an exception applied to one of the rules. <i>This applies only to Windows Patch policies.</i> • Device Groups: Compliance scan ran successfully and enough servers in the group meet the threshold criteria for Non-Compliance set in the Compliance Settings in the Administration pane, while the rest of the servers in the group are Compliant. The compliance threshold definitions for Partial Compliance can be modified.
	<p>Non-Compliant</p> <ul style="list-style-type: none"> • Policy: One or more rules or items defined in the policy does not match the actual server configuration. • Servers: Compliance scan ran and the actual server configuration does not match at least one or more of the rules defined in the policy. • Device Groups: Compliance scan ran and enough servers in the group meet the threshold criteria for Non-Compliance set in the Compliance Settings option in the Administration pane to indicate the group is Non-Compliant. The compliance threshold definitions for Non-Compliance can be modified.
	<p>Scan Failure</p> <p>Compliance scan was unable to run.</p>

Table 3 Compliance Status Icons (cont'd)

Icon	Compliance Status Description
	Scan Needed Results undefined. This status can result if a compliance scan was never run (such as on a new installation) or the configuration on the server (or servers in the device group) changed since the last time information was reported to the SA Client.
	Scanning: The compliance scan is currently running.
—	No Tests Defined No compliance policies of this type are attached to the server or all servers in the device groups, including all servers in any sub-groups.

Compliance Status Thresholds—Policy, Server, & Server Group

Policy: Compliance status for a policy is based on all of the rules in the policy. If one of the rules in a policy is Non-Compliant (does not match the actual configuration on the managed server), the entire policy is considered Non-Compliant for a server.

Server & Server Group: Compliance status for a server is based on all of the policies attached to the server or that define the server as a target. If any one of the compliance categories has a compliance status of Non-Compliant, the server's overall compliance status is also considered Non-Compliant. All of the policies in all of the compliance categories must be Compliant for the server's overall compliance status to be Compliant.

Compliance Status Thresholds—Device Group

Whether or not a server is considered Compliant or Non-Compliant is important when viewing device group compliance in the Compliance view. This status is based on a default threshold calculation that you can configure and customize.

Non-Compliant: In the device group Compliance view, in order for a compliance category (Audit, Audit Policy, Software, Patch, or Configuration) to display a status of Non-Compliant, *more than 5% of all servers in a group must have the status of Non-Compliant for that category.* Another way to understand Non-Compliant for a device group is to remember that *when less than 95% of the servers are Compliant, a status of Non-Compliant will display.*

Partial-Compliant: In the device group Compliance view, in order for a compliance category (Audit, Audit Policy, Software, Patch, or Configuration) to display a status of Partial-Compliant, *more than 2% but less than or equal to 5% of all servers in a group must have the status of Non-Compliant for that category.* Another way to understand Partial-Compliant for a device group is to remember that *when less than 98% but at least 95% of the servers are Compliant, a status of Partial-Compliant will display.*

Compliant: In the device group Compliance view, in order for a compliance category (Audit, Software, Patch, or Configuration) to display a status of Compliant, *less than 2% of all servers in a group must have the status of Non-Compliant for that category.* Another way to understand Compliant for a device group is to remember that *at least 98% of the servers are Compliant.*

Device group status is calculated based on all policies (in all compliance categories) attached to all servers that belong to the group. This includes servers in all sub-groups that are children to the selected group.

You can change the default thresholds used to calculate compliance status. For example, you could configure that group compliance status be calculated non-recursively, which would exclude all sub-group server members from the compliance calculation.

Changing Device Group Compliance Settings

By default, the SA Client allows you to configure the manner in which compliance for a device group is determined.



In order to change device group compliance settings, you must be a member of a group that is assigned permission to the SA feature Model: Opsware. For more information on what type of permissions you have been granted, contact your SA Administrator.

To change the settings for device group compliance:

- 1 In the navigation pane, select **Administration ► Compliance Settings**.
- 2 In the Compliance Settings pane, in the Device Group Compliance section, click **Edit Settings**.
- 3 In the Device Group Compliance Settings window, configure the following settings:
 - **Display Device Group Rollup Compliance:** This option allows you to show or hide the icon that indicates compliance status of the parent group shown at the top of each compliance category column. This icon indicates a compliance status rollup for all members of a selected group.

For example, if this option is selected, when you select a group and then from the View drop-down list select Compliance, the top column heading for each compliance category column (Audit, Software, Patch, and Configuration) shows an icon that indicates the compliance status for all servers in the selected group. You can cursor-over this column heading to view compliance status for all devices in this category.
 - **Member Calculations:** This option allows you to choose whether or not you want to include servers that belong to sub-groups when calculating overall group compliance level for a compliance category. For example:
 - **Server and group members are considered:** This means that the compliance status for a device group will recursively check compliance for all servers in a group and for all servers in all sub-groups that belong to the selected device group.
 - **Only server members are considered:** This means that the compliance status for the selected device group will check compliance only for servers at the top level of the group and will exclude any servers that belong to any sub-group members.
 - **Thresholds:** Allows you to change the compliance threshold calculation percentage (%) that is used to determine device group compliance status for all compliance categories.

By default, a device group will display the following statuses:

 - Non-Compliant**—If more than 5% of its members are Non-Compliant.
 - Partial Compliance**—If more than 2% but less than 5% of its members are Non-Compliant.
 - Compliant**—If 2% or less of its members are Non-Compliant.
- 4 Click **OK** to save your settings.

The Compliance View

In the SA Client, you can view compliance for individual servers, for server groups, and for servers and server groups together:

- [Viewing Compliance for a Server](#)
- [Viewing Compliance for Multiple Servers](#)
- [Viewing Group Compliance](#)

When viewing compliance status for server groups, it is possible that there are servers in the group that your user does not have permission to see. In addition, your user account might not have permissions to view some of the policies (Audit, Software, and Patch) used to calculate the compliance status for a group of servers.

In these cases, even though you cannot see some servers and some policies, you will still be able to see overall compliance status for server groups that your user has access to view. You will also still be able to see compliance category rollups, even though some of the policies may be hidden from your view.

Viewing Compliance for a Server

To view compliance information for an individual server:

- 1 In the navigation pane, select **Devices** ► **All Managed Servers** or **Virtual Servers**.
- 2 In the content pane, select a server.
- 3 Right-click and select **Open** to display the Server browser.
- 4 In the Information pane, select **Management Policies**.
- 5 In the **Management Policies** pane, select **Compliance**.

The content pane displays a compliance summary pie chart of compliance statuses for each compliance category, including detailed status information for individual policies. See [Figure 27](#).

- 6 To perform an action on one of the compliance categories or on an individual policy in the categories, make a selection in the details list and click **Run Audit** (for audits only), **Remediate**, or **Scan Device**.



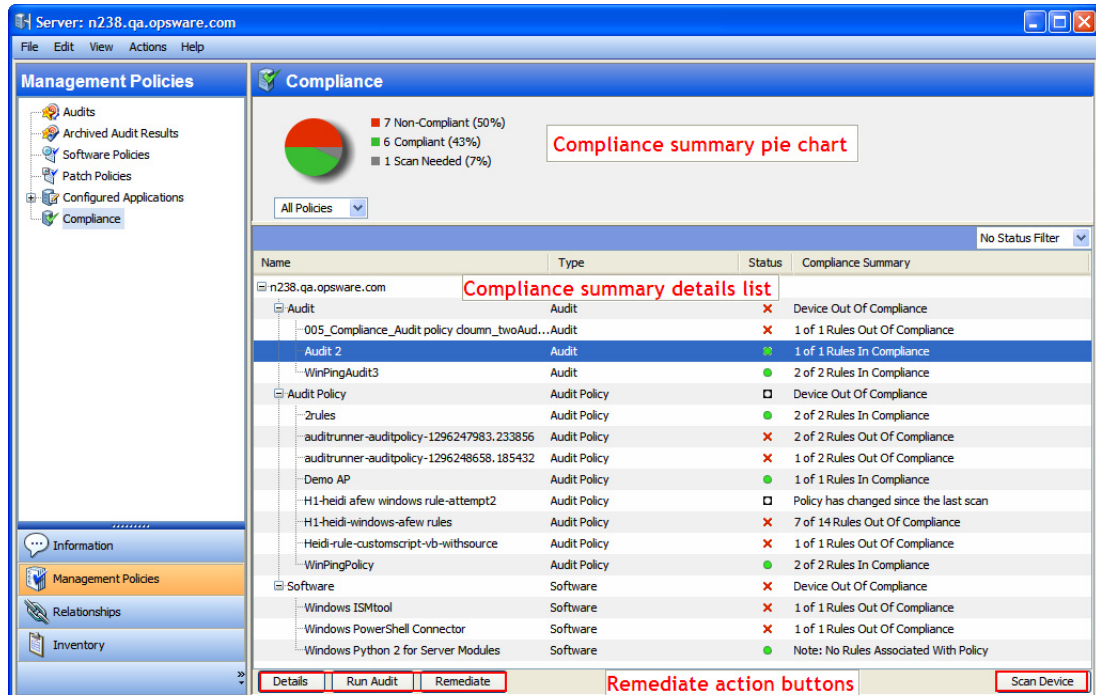
The ability to both view policies and perform remediation operations on them is determined by your user permissions. If you are not able to view a policy or perform an action on one, consult your SA Administrator.

Compliance Summary Pie Chart and Details

The Compliance view contains the following main sections:

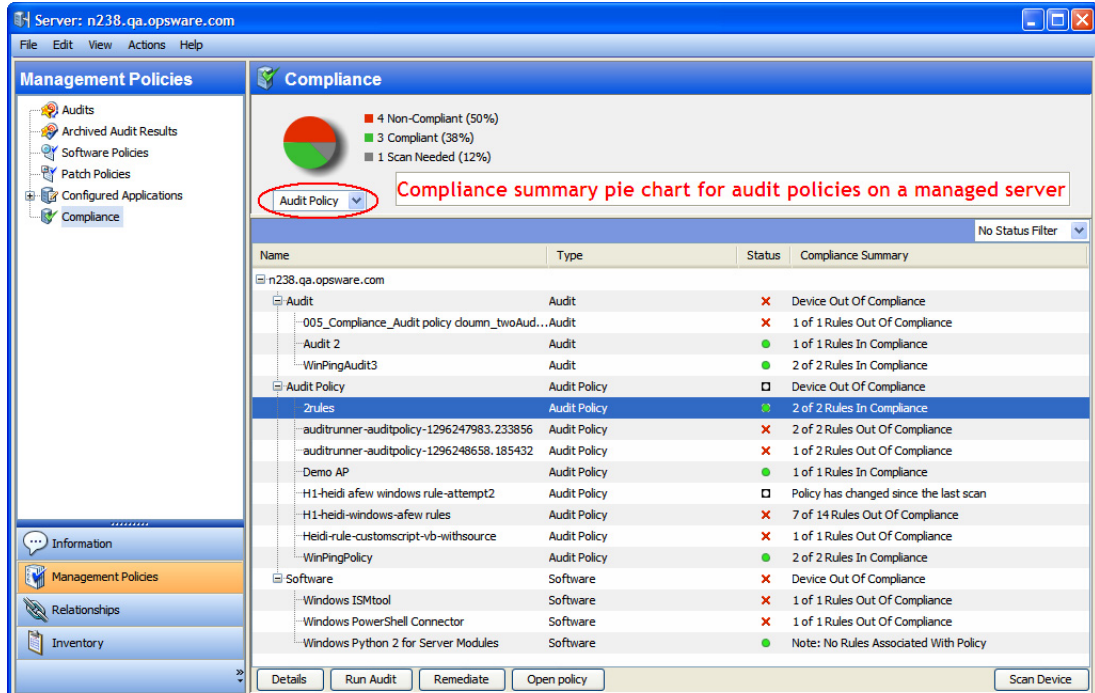
- The *compliance summary pie chart* provides a graphical display of the overall compliance status for all policies attached to the selected server. You can also filter this pie chart to show status only for a specific compliance category. See [Figure 27](#).
- The *compliance summary details list* allows you to drill down in each compliance category to see the overall compliance status, the policies contained in each category, the compliance status for each policy and a summary description for each. Depending on your selection, you can launch actions to remediate policies that are out of compliance, such as viewing details of a policy, running an audit, or scanning the device for compliance. See [Figure 27](#).

Figure 27 Compliance Summary for a Managed Server—All Policies



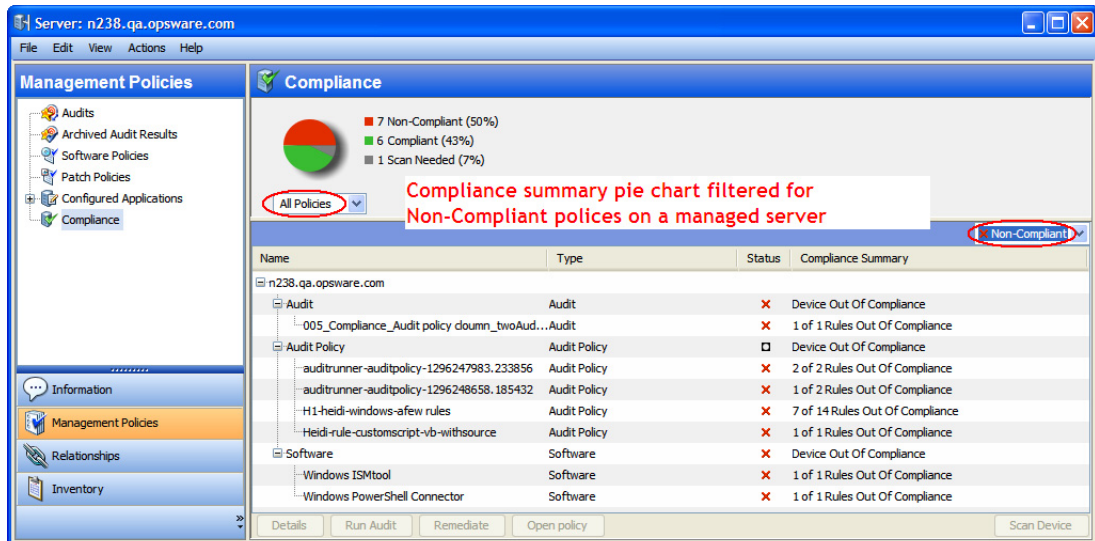
Select the drop-down list below the pie chart to view the pie chart filtered by each compliance test category, such as Audit Policy. See [Figure 28](#).

Figure 28 Compliance Summary for a Managed Server—Audit Policy



You can also choose to filter the compliance policy breakdowns in the details pane below the pie chart to see all compliance policies that contain a certain compliance status. For example, in Figure 29, the compliance view has been filtered to show only all compliance policies that are non-compliant.

Figure 29 Compliance Summary Filtered By Non-Compliant



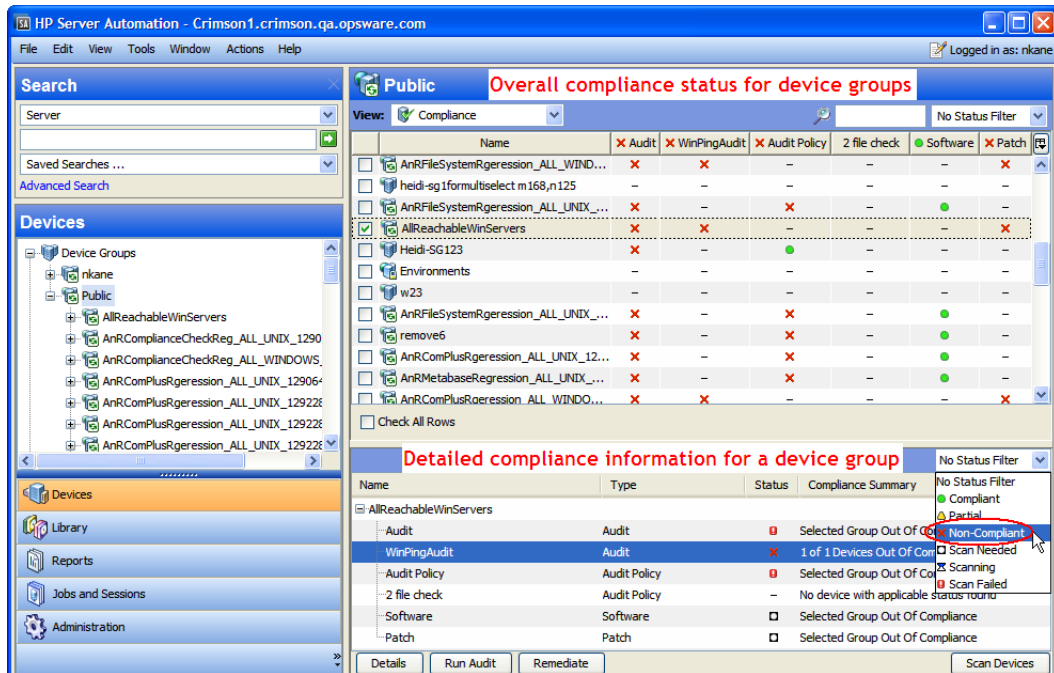
In the previous example, the Compliance view details pane shows all Non-Compliant policies attached to the server. A policy is considered Non-Compliant if at least one of the rules configured in the policy does not match the configuration on the server.

Viewing Compliance for Multiple Servers

To view compliance information for groups of servers:

- 1 In the navigation pane, select **Devices** ► **Device Groups**.
- 2 In the Device Groups tree, select Public or select your own user group list. The content pane displays the contents of all device groups in the list, either all public groups or all groups your user created.
- 3 From the View drop-down list, select Compliance.
- 4 For one or more of the device groups or any servers in the list, select the check box next to it to include it in the Compliance view details pane. The details pane displays compliance information for all servers in the selected group. See Figure 30.

Figure 30 Compliance View—Device Groups



- 5 (Optional) Use the status filter drop-down list to filter the view by compliance status. For example, you can choose to view only device groups that have a Non-Compliant ✗ status.
- 6 (Optional) In the details pane, select one of the categories. Depending on the category and your user permissions, click one of the action buttons at the bottom of the pane for more details, to run an audit, to remediate a software policy or a patch policy, or to run a compliance scan on all members of the group.

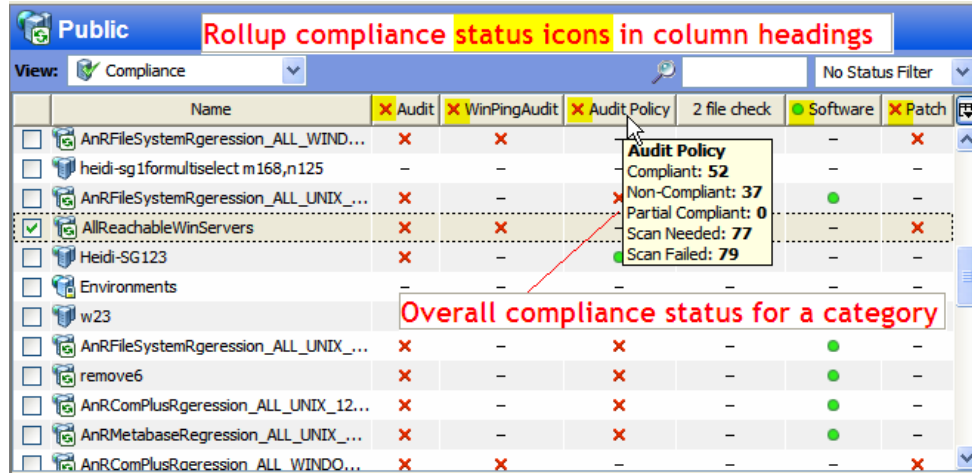
Device Group Compliance: Status Rollup

The device group content pane displays a summary of compliance status rollups for all group members and contents of groups that you selected in the navigation pane (**Devices** ► **Device Groups**).

Compliance status (Compliant, Non-Compliant, Partial, and so on) icons in the column heading at the top of the list indicate the rollup status for all groups in the list. To view the overall status for the compliance category for all visible groups, move the cursor over the column heading for a category.

In each row of the list, this view displays compliance status for each group in all compliance categories for each group in the list. These categories include Audit, Audit Policy, Software, Patch, and Configuration, including any individually scheduled audits that you choose to display in this view. In Figure 31, each compliance category displays a compliance status for all policies of each type that are attached to servers in the group.

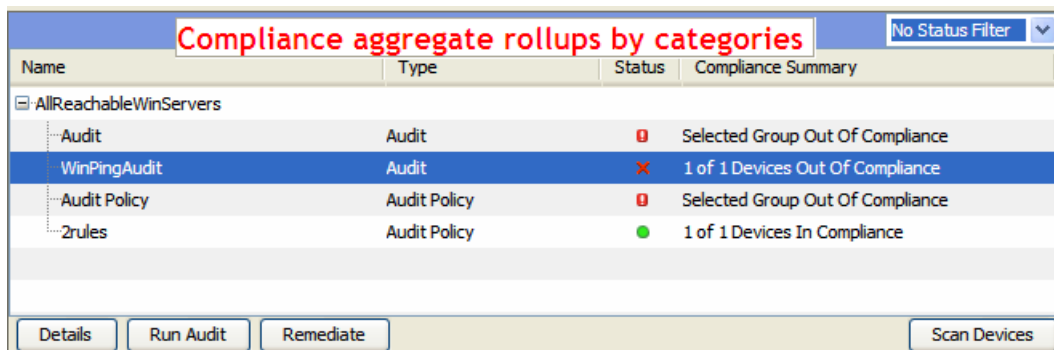
Figure 31 Compliance Rollups for Device Groups



Device Group Compliance: Aggregate Rollup

When you select one or more groups (or all of them) in the content pane, the details pane displays device compliance aggregate rollups in each column in the content pane for all members of the group. See Figure 32.

Figure 32 Compliance Aggregate Rollups for Device Groups




Use the status filter drop-down list to filter the view by compliance status. For example, you can choose to view only device groups that have a Non-Compliant ✗ status.

Depending on the category and your user permissions, click an action button for more details, to run an audit, to remediate a software policy or a patch policy, or to run a compliance scan on all members of the group.

Viewing Group Compliance

In the Group explorer, the Compliance view shows a rollup of compliance policy aggregates for each policy type for all members of the group as a whole, as opposed to compliance status for individual servers. This gives you a sense of whether or not the group is compliant for each policy type and for all servers in the group (and any sub-groups).

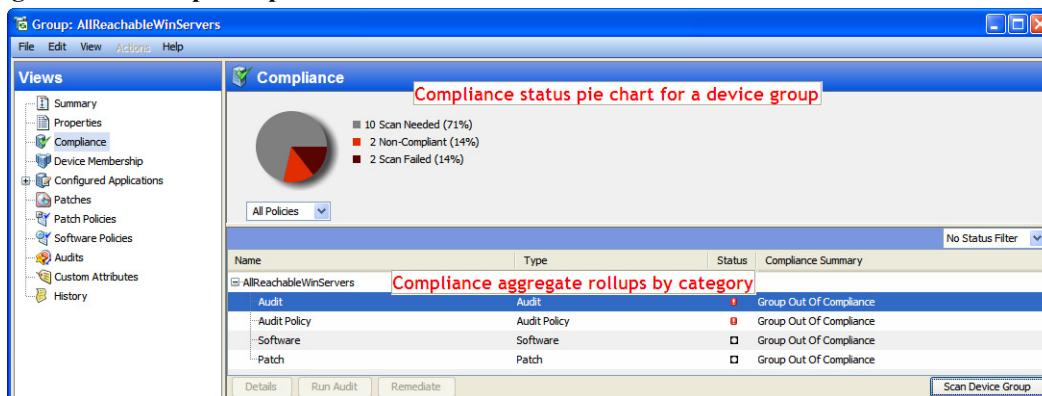
Use the status filter drop-down list to filter the view by compliance status. For example, you can choose to view only device groups that have a Non-Compliant  status.

Depending on the category and your user permissions, click an action button for more details, to run an audit, to remediate a software policy or a patch policy, or to run a compliance scan on all members of the group

To view a group of servers in the Device Group Explorer:

- 1 In the navigation pane, select **Devices** ► **Device Groups**.
- 2 In the Device Groups tree, select Public or select your own user group list. The content pane displays the contents of all device groups in the list, either all public groups or all groups your user created.
- 3 Select a server group.
- 4 Right-click and then select **Open**.
- 5 From the Views pane of the Group explorer, select Compliance. The Compliance view displays summary and rollup compliance status information about all servers in the group. See [Figure 33](#).

Figure 33 Group Compliance View



The compliance summary pie chart is a graphical display of the overall compliance status for all policies aggregates for all associated servers in the group. Sections in the pie chart show the compliance status and percentage of each status level by category, such as Compliant, Non-Compliant, Scan Needed, Scan Failed, and so on. You can also filter this pie chart to show status only for a certain compliance category.

The details pane displays device compliance aggregate rollups by compliance categories.

Depending on the category and your user permissions, click an action button for more details, to run an audit, to remediate a software policy or a patch policy, or to run a compliance scan on all members of the group.


Adding and Removing Compliance View Columns

When you view device groups in the Compliance view, by default, the following compliance categories display as columns in the content pane: Audit, Audit Policy, Software, Patch, and Configuration. You can show or hide any of these categories, and add or remove an individual policy in each category.

To add or remove device group compliance categories in the Compliance view:

- 1 In the navigation pane, select **Devices** ► **Device Groups**.
- 2 In Device Groups, expand your list of device groups or the Public list of device groups.
- 3 In the content pane, select a device group.
- 4 In the View drop-down list, select Compliance.

The content pane lists the following compliance categories: Audit, Audit Policy, Software, Patch, and Configuration. The content pane also indicates the statuses for each member of the device group.

- 5 Use the column selector  to add or remove a category.
- 6 In the Select Compliance View Columns window, the left side of the window displays tabs for each compliance category and all compliance policies in those categories that you have permissions to see. The right side of the window displays the currently visible policies in each category in the Compliance view. By default, the Compliance view displays the aggregate (rollup) of all policies in the category.
- 7 To add an individual policy as a column in the Compliance view, on the left side, select a compliance category tab and then a policy, and then click the plus (+) arrow button.
- 8 To remove an individual policy or an aggregate column from the Compliance view, select one on the right-side of the window and then click the minus (-) arrow button.
- 9 Click **OK** to save your changes.

Sorting the Compliance Category Display



Best Practice: It is useful to arrange the compliance categories in an ascending or descending order to customize your Compliance view display requirements.

To sort the columns in the Compliance view:

- 1 In the Compliance view, click inside a column heading.
The number “1” displays, superscripted adjacent to the compliance category name. This is the primary sort key for this table.
- 2 Click the UP or DOWN arrows inside the heading to indicate whether the data is sorted in ascending or descending order.
- 3 Press the **Ctrl** key and then click inside another column heading.
The number “2” displays, superscripted adjacent to the compliance category name. This is the secondary sort key for this table.
- 4 *(Optional)* Repeat step 3 as needed.
- 5 *(Optional)* Move the cursor over a column heading to display a rollup of the compliance statuses for a specific category.
- 6 To reset the sort keys, click on a column heading that is not annotated.

Filtering By Compliance Status

When you view compliance for individual managed servers and groups of servers in the Compliance view, you can filter the view to show only groups and servers that have at least one server that matches a specific compliance status for any of the displayed compliance categories. For example, when you select a group and then select Compliance view, you can use the status filter to only show members of the selected group (individual servers and those in any sub-groups) that have a Non-Compliant status for each of the compliance categories, such as Audit, Audit Policy, Patch, Software, and so on.

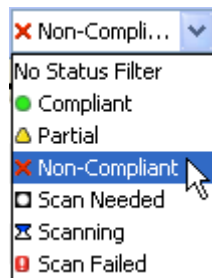
To filter the Compliance view by compliance status:

- 1 In the navigation pane, select **Devices** ► **Device Groups**.
- 2 In the Device Groups tree, navigate and select Public or select your own user group list.
- 3 In the Public pane, select a device group.

The content pane shows the Compliance view statuses for all members of the selected group.

- 4 To filter this view by compliance status, select one from the status filter drop-down list. See [Figure 34](#).

Figure 34 Compliance Status Filter



- 5 The Compliance view displays only those members of the group (individual servers and those in any sub-groups) that have a status of Non-Compliant **X**.
- 6 Select any of the servers or sub-groups in the group listed.

The details pane shows the compliance status information for those servers. You can filter information in the details pane by using the status filter in this pane.

Refreshing Compliance Information



Best Practice: It is useful to refresh the Compliance view to make sure you are looking at the latest compliance information in your core. To get the latest compliance information from the core, from the View menu, select Refresh or press **Ctrl + F5**.

When you first select the Compliance view, the information displayed shows the latest information reported from the SA core for each compliance category. It is possible that a server's configuration has changed since you last looked at the Compliance view. It is also possible that a policy has changed since you last viewed server and groups in the Compliance view. If this is the case, you might want to scan for compliance or rerun an audit to generate new data for the Compliance view display.

Setting Automatic Compliance Check Frequency

By default, the SA Client will check the core for new or changed compliance information every 5 minutes. You can change this time interval, using the Set Options window.



Press **Ctrl + F5** if you want the SA Client to immediately check for new compliance information in the core.

To change the automatic compliance check frequency setting:

- 1 In the SA Client, in the Tools menu, select Options.
- 2 In the Set Options window, in the Views pane, select General.
- 3 In the Cache section, in the “Check for updates every <xx> minute(s)” field, enter a time interval for how often you want the SA Client to check the core for new compliance information.

This check applies to all information accessed from the core by the SA Client, not just to compliance information. A longer interval increases the likelihood that the information you are viewing is out of date. A shorter interval increases network traffic flowing to and from your core—this means you are viewing more recent information.

- 4 (Optional) Click **Update Cache** to immediately check for new information from the core.
- 5 (Optional) Click **Reload Cache** to immediately reload (refresh) the cache.
- 6 Click **Save**.

Exporting Compliance View Information

If you want to view all information displayed in the Compliance view to a file, you can export the view to either .html or .csv.

To export Compliance view information to a file:

- 1 In the navigation pane, select **Devices > Device Groups**.
- 2 Select a group that you want to view compliance for, and from the **View** menu, select **Compliance**.
- 3 In the contents pane, select a server in the group.
- 4 Right-click, select **Export to**, and then select CSV or HTML.
- 5 In the Export Compliance View window:
 - a Enter a name for the file name.
 - b (Optional) Change the encoding if you want the saved file to use a specific encoding scheme.
 - c Click **Save**.

Compliance View Remediation

In addition to providing compliance status information for servers and groups, the Compliance view enables you to remediate server configurations that are not in compliance with your organization's standards, as defined by your audit, software, patch, and application configuration compliance policies.

By definition, the action of remediating a server or group of servers means finding how and where a server or server group is out of compliance (Non-Compliant), and then making sure that a server's actual configuration conforms to your compliance policies.

From the Compliance view for a server or a group of servers, you can perform the following actions:

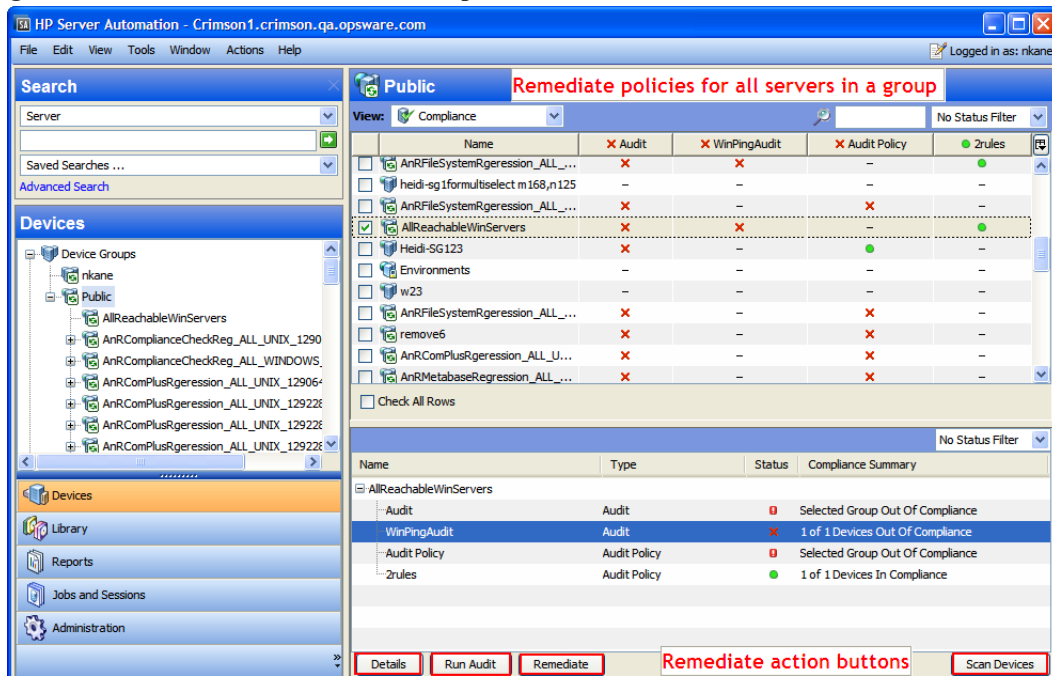
- Remediate a patch policy or a software policy.
- Run, view, and remediate audit results.
- Push an application configuration to a server.
- Run a compliance scan for patches, software, or application configurations to get the latest compliance information for your servers.

When you select a server or group of servers in the Compliance view, or view them in the Device or Device Group Explorer, the details pane provides action buttons for operations that help you discover and remediate out of compliance policies. The type of actions available are based on the type of policy, whether you select a single managed server or group of servers, and whether or not you select an individual policy, multiple policies, or the rollup of a compliance category in the details pane.

Compliance View Remediate—Server Group

Figure 35 shows how the Compliance view enables the remediate action for a server group.

Figure 35 Remediate for a Server Group



The details pane for the selected group shows a summary of all policies attached to all servers in the group (and all servers in any sub-groups) arranged by a compliance category—Audit, Audit Policy, Software, Patch, and Configuration. When you select a group, you can only remediate an entire category of policies, such as all software policies or all patch policies attached to all servers in the group that are out of

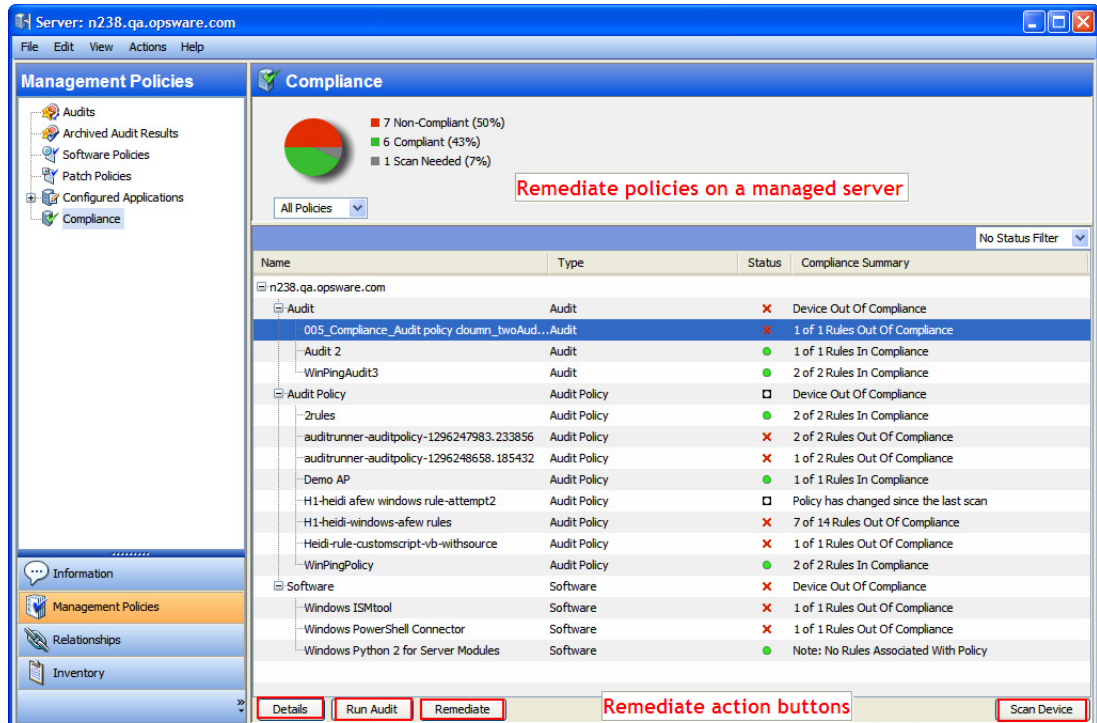
compliance. If you select the Software category in the details pane, the **Remediate** button is enabled. When you click **Remediate**, the SA Client launches the Remediate wizard. Complete the steps in this wizard to remediate any out-of-compliance policy configurations for all servers in the group.

You can view this same information and access these option by selecting the group, and from the Actions menu select **Open**. This action launches the Group explorer and displays the same details pane for the group, along with the action buttons in the details pane.

Compliance View Remediate—Server

Figure 36 shows how the Compliance view enables the remediate action for an individual server.

Figure 36 Remediate for a Server



For a server group, remediate actions always apply to all members of the group. For an individual managed server, you can remediate either all or selected policies that are attached to the server. For example, you can launch a server and, from the server's Device Explorer, select **Management Policies** ► **Compliance** to view all compliance policies attached to the server.

In the details pane, select an audit or a software policy to view the audit. Use an action button to run the audit, remediate the software policy, or scan the device for compliance.

Compliance Scans

In the Compliance view, you can perform a compliance scan for the Audit, Audit Policy, Software, Patch, or Configuration compliance categories. When you scan for compliance, you scan servers targeted by a compliance policy to determine whether target server configurations match the policy's rule definitions. For example, a compliance scan can check to see what patches are installed on a computer, compare that with a patch or software policy, and then return the results to the Compliance view. Or, a compliance scan can check the contents of a configuration file on a server in order to determine whether it matches the rules defined in an application configuration.


Audits do not have a scan feature; however, running an audit produces the same results. For an audit, when you run an audit, SA checks the target server configuration to determine the extent to which it matches the audit's rule definitions.

The following actions occur when scanning the compliance categories:

- **Software Compliance Scan:** Compares configuration files on a server to determine whether they match the values stored in the software policies attached to the server or server group. The results of this scan show servers that are in compliance (have all required software policy items installed) and servers that are out of compliance (do not have all required software policy items installed). Scanning for software compliance applies to HP-UX, Unix, and Solaris patch management.
- **Patch Compliance Scan:** Compares patches that are installed on a server with patch policies and patch policy exceptions that are attached to that server. The results of this scan show servers that are in compliance (have all required patches installed) and servers that are out of compliance (do not have all required patches installed). Scanning for patch compliance applies only to Windows patch management.
- **Configuration Compliance Scan:** Compares configuration files on a server with the template-defined application configurations that are attached to that server. The results of this scan show servers that are in compliance (configuration file definitions match the configuration templates) and servers that are out of compliance (configuration file definitions do not match the configuration templates). See for more information about Configuration compliance.

Patch Compliance

In Server Automation, patch management enables you to identify, install, and remove patches on managed servers and groups of servers. Using Windows patch management, you can identify and install patches for the Windows 2000 SP 4, Windows 2003, and Windows 2008, and operating systems, including Service Packs, Update Rollups, and hotfixes.


In the Compliance view, you can review the compliance status for patch policies to see whether your servers have the correct patches installed on them. During a patch compliance scan, Server Automation checks managed servers and public device groups to determine whether all patches in a policy and a policy exception were installed successfully. If the patches installed (or not installed) on the server do not match the patch policy definitions, the Compliance view displays the server's patch policies as Non-Compliant .

Compliance scans can be run on a one-time basis or they can be scheduled on a recurring basis. You can remediate a patch policy to a server to ensure a server's or server group's patch compliance.

See the *SA User Guide: Server Patching* for more information.


Patch Compliance Status Criteria


Patch compliance status is determined by the following criteria:


- **Patch Compliance—Single Server:** If at least one item in a patch policy does not match what is discovered (or does not exist) on the server the policy is attached to, the server's patch compliance status is Non-Compliant . The details pane of a server's Device explorer window shows the Patch category as Non-Compliant and the summary column indicates how many rules (patch policy items) are Non-Compliant out of the total number of rules.

For example, if a patch policy contains 10 items and 6 of the items are Non-Compliant, the patch policy's status is Non-Compliant and the summary description reads: "6 of 10 Rules Out of Compliance."

If more than one patch policy targets a single server and if at least one of those policies is Non-Compliant, then the aggregate compliance status for Patch is also displayed as Non-Compliant as well. You can expand the Patch category of the details pane to see which of the policies are not in compliance, including a breakdown of how many rules in each policy are either in or out of compliance.

- **Patch Policy—Rule Exception:** If a rule exception is applied to one of the patch policy items, the server's Patch compliance displays a compliance status of Partial-Compliant . *Patch is the only compliance category that allows rule exceptions at the policy level.*

Patch Compliance—Device Groups: A patch policy attached to a group of servers is considered Compliant if more than 5% of the servers in the group attached to the policy have a status of Non-Compliant . If this is the case, the aggregate compliance for patch policy displays as Non-Compliant. Another way to understand Non-Compliant for a device group is to remember that when less than 95% of the servers are Compliant, a status of Non-Compliant will display.

However, if more than 2%, but less than or equal to 5%, of all servers in a group have the status of Non-Compliant for that category, then the status is Partial-Compliant . Another way to understand Partial-Compliant for a device group is to remember that when less than 98% but at least 95% of the servers are Compliant, a status of Partial-Compliant will display.

If less than 2% of all servers in a group have a Patch Policy status of Non-Compliant for that category, then the overall status is Compliant. Another way to understand Compliant for a device group is to remember that at least 98% of the servers are Compliant.

The details pane for a group of servers in the Compliance view shows whether the patch policies are compliant or not. This information does not expand to show a breakdown of individual servers and policies.

You can modify the thresholds used to determine compliance for groups of servers.

Remediating Patch Compliance for Servers

When you remediate patch compliance for a single server or for multiple servers, you can choose to remediate either all of the policies attached to the servers or choose to remediate individual policies. You can remediate patch policies for a single server by viewing the server's Device explorer or you can remediate patch policies for multiple servers by selecting the policies in the Device Groups list.

To remediate patch policies on single or multiple servers:

- 1 To remediate patch policies for a single server in the Device Explorer, in the navigation pane, select **Devices > Servers > All Managed Servers**.
- 2 Select a server in the content pane.
- 3 Right-click and then select **Open** to open the Server browser.
- 4 In the navigation pane, select **Management Policies > Compliance**.
- 5 In the details pane of the Compliance view, expand the Patch category and select an individual policy or the top level Patch category. This selection enables you to remediate all patch policies attached to the server).
- 6 Click **Remediate** and then complete the steps in the Remediate wizard.

Or

- 1 To remediate patch policies for multiple servers, in the navigation pane, select **Devices > Device Groups** and then select a group.
- 2 From the View drop-down list, select Compliance.
- 3 In the details pane of the Compliance view, expand the Patch category and select a patch policy that is attached to the selected servers. Or, select the top level Patch category if you want to remediate all of the patch policies attached to the selected servers.
- 4 Click one of the following buttons to remediate patch policies:
 - **Remediate**: Launches the Remediate wizard that allows you to remediate the selected patch policy or policies against the selected server or servers.
 - **Scan Device**: Displays the Scan for Compliance window where you first select the types of policies you want scanned and then click **Scan** to launch the job. This processes scans the selected servers for all Audit, Audit Policy, Software, Patch, and Configuration policies attached to the servers. When you include Configuration in your policy selection, a Scan Configuration Compliance window displays the status of the scan. This action does not have any effect on the audits that target this server.

Remediating Patch Compliance for Groups


When you remediate patch policies for a single group of servers or for multiple groups of servers, you can remediate all the policies attached to all servers in the single group or in multiple groups. However, when you select a group or multiple groups, you can only remediate *all* patch policies attached to *all* servers in the group and any sub-groups.

To remediate patch policies for a single group of servers or for multiple groups of servers:

- 1 To remediate patch policies for a single server in the Device Explorer, from the navigation pane, select **Devices ► Servers ► All Managed Servers**.
 - 2 Select a server in the content pane.
 - 3 Right-click and then select **Open** to open the Server browser.
 - 4 In the navigation pane, select **Management Policies ► Compliance**.
 - 5 In the details pane of the Compliance view, expand the Patch category and select an individual patch policy or the top level Patch category. This selection enables you to remediate all patch policies attached to the server.
 - 6 Click **Remediate** and then complete the steps in the Remediate wizard.
- Or
- 1 To remediate patch policies for multiple servers, from the navigation pane, select **Devices ► Device Groups**, and then select a group.
 - 2 From the View drop-down list, select Compliance.
 - 3 In the details pane of the Compliance view, expand the Patch category and select a policy that is attached to the selected servers. Or, select the top level Patch category if you want to remediate all of the policies attached to the selected servers.
 - 4 Click **Remediate** and then complete the steps in the Remediate wizard.

Audit Compliance


In Server Automation, audit and remediation allows you to define server configuration policies in an *audit*. An *audit* helps you make sure that the servers in your facilities meet your audit policy standards. An audit consists of a collection of rules that you can define to model those standards. For example, an audit can consist of Windows COM+ configurations, registry settings, services, file system settings, hardware configuration, user and group password settings, software installation, packages, storage settings, and so on, that define an *ideal server configuration*. Or, the audit might represent a *negative server configuration* that enables you to determine the way a server should *not* be configured.

Audit compliance determines whether the rules defined in a recurring audit match the actual server configuration for all servers targeted by the audit. The Compliance view allows you to see both the aggregate and individual compliance status of all audits that run on a recurring schedule on a server or group of servers. If any of the audits are Non-Compliant , you can remediate any differences found between the audit and the audit's target server or servers.

The Compliance view derives audit compliance servers and groups of servers from regularly scheduled audits.


Audit Compliance Status Criteria

Audit compliance status is determined by the following criteria:


- **Audit Compliance—Single Server:** If a single rule in an audit does not match the target server's configuration, the server's audit compliance status is Non-Compliant . The details pane in a server's Device explorer shows the Audit category as Non-Compliant and the summary column indicates how many rules are Non-Compliant out of the total number of rules.

For example, if an audit has 10 rules and 4 of the rules are Non-Compliant, the audit's status is listed as Non-Compliant and the summary description displays: "4 of 10 Rules Out of Compliance."

If more than one audit targets the server and if at least one of those audits is Non-Compliant, the aggregate compliance status for audits is also displayed as Non-Compliant. You can expand the Audit category of the details pane to see which of the audits are not in compliance, including a breakdown of how many rules in each audit are in compliance or out of compliance.

- **Audit Compliance—Device Groups:** An audit that targets a group of servers (and all servers in all sub-groups) is considered Compliant if at least 95% of the servers in the group that are targeted by the audit have a compliance status of Compliant .

If more than 5% of the servers in the group targeted by an audit have a status of Non-Compliant, the aggregate compliance for audits displays as Non-Compliant. Another way to understand Non-Compliant for a device group is to remember that *when less than 95% of the servers are Compliant*, a status of Non-Compliant will display.

However, if more than 2%, but less than or equal to 5%, of all servers in a group have the status of Non-Compliant for that category, the status is Partial compliant . Another way to understand Partial-Compliant for a device group is to remember that *when less than 98% but at least 95% of the servers are Compliant*, a status of Partial-Compliant will display.

If less than 2% of all servers in a group have an Audit status of Non-Compliant for that category, the overall status is Compliant. Another way to understand Compliant for a device group is to remember that *at least 98% of the servers are Compliant*.

The details pane for a group of servers in the Compliance view shows whether all of the audits are compliant. This information does not expand to show a breakdown of individual servers and audits.

Audit Compliance Remediation

The Compliance view allows you to view all audits that target a server or group of servers and to remediate those results that are out of compliance. This ensures that a server's configuration complies with the rules defined in an audit.

For each audit rule that is out of compliance on the target server (the server's configuration either did not match the rule definition or simply did not exist), remediation copies the rule object to the target server so it matches the rule. Or, in the case of a value-based audit rule, remediation changes the target server's configuration to match the rule.

Example: You have an audit that checks a group of Windows servers to make sure that they contain certain registry keys and ACLs. After the audit runs against a Windows server, it is possible that several of the rules are out of compliance. This means the Registry keys specified in the audit rules were not found on the target servers. When you remediate, the audit feature copies the Registry keys specified in the audit rule to the target servers. This ensures that the servers have the specific keys and associated ACLs. For a group of servers, remediation has the same results—where only the remediation operation applies to all servers in the group, including all servers contained in any sub-groups.

Remediating Audits Attached to Servers

You can remediate an audit that is attached to a single server or an audit that is attached to multiple servers. You can only remediate individual audits. You cannot aggregate audits at the top level. For any group that is selected, all direct server children in that group are the subject of the remediation.

When the **Remediate** button is not enabled in the Compliance view, even though a single policy is selected in the detail pane and one or more servers are selected in the summary pane, it typically means that there is no audit result for that policy to remediate.

You cannot run an audit on a group of servers from the Compliance view. However, you can create an audit that runs against a group of servers and remediate those audit results for a group of servers from the Audit Results window.

To remediate an individual audit on a single server:

- 1 In the navigation pane, select **Devices > Servers > All Managed Servers**.
- 2 In the content pane, select a server.
- 3 Right-click and then select **Open** to open the Server explorer.
- 4 In the navigation pane, select **Management Policies > Compliance**.
- 5 In the details pane of the Compliance view, expand the Audit category and then select an individual policy.
- 6 Click **Remediate** and then complete the steps in the Remediate wizard.

To remediate an individual audit on multiple servers:

- 1 In the navigation pane, select **Devices > Device Groups**, and then select a group.
- 2 From the View drop-down list, select Compliance.
- 3 Select multiple servers by selecting the check boxes next to each server.
- 4 In the details pane of the Compliance view, expand the Audit category and select an individual audit that is targeting all of the selected servers.
- 5 Click one of the following buttons to perform a type of remediation for an audit on a single server or on multiple servers:

- **Details:** Displays the Audit Result window that shows all differences found between the audit and the target, and allows you to remediate the differences by rule or by server. Click the **View Rules Details** link to open the Rules window and view the audit rules. Select a server and click **Run Partial Audit** to launch the Audit Servers wizard.
- **Run Audit:** Launches the Audit Servers wizard and allows you to run the audit immediately or schedule to run the audit at a later time. The audit will run against all servers targeted by the audit.
- **Remediate:** Launches the Remediate wizard, which allows you to remediate target server configurations that are out of compliance with the audit rules. You can remediate differences by rule or by server. If none of the selected servers have remediate results for the selected policy, a **No Results Found to Remediate!** message will display.
- **Scan Devices:** Displays the Scan for Compliance dialog where you first select the types of policies you want scanned and then click **Scan** to launch the job. This processes scans the selected servers for all Audit, Audit Policy, Software, Patch, and Configuration policies attached to the servers. When you include Configuration in your policy selection, a Scan Configuration Compliance job window displays the status of the scan. This action does not have any effect on the audits that target this server.

Audit Policy Compliance

You can add an audit that has a recurring schedule to the Compliance view. The Compliance view displays the result of the latest run of that audit. The audit can directly contain audit rules or it can inherit audit rules from the source snapshot or source snapshot specification. In the Compliance view, you should display the Audit column to confirm associated audit rules. See [Figure 37](#).

Figure 37 Compliance View with Audit & Audit Policy.

Name	Audit	WinPingAudit	Audit Policy	2 file check	Software	Patch
crimson1.crimson.qa.opsware.com	-	-	-	-	-	-
m103.qa.opsware.com	×	-	●	-	-	-
n156.qa.opsware.com	●	-	●	-	●	-
n238.qa.opsware.com	×	-	□	-	□	-
m176.qa.opsware.com	-	-	×	-	-	-
m179.qa.opsware.com	□	×	□	-	□	□
m021.qa.opsware.com	●	-	●	-	-	-
n114.qa.opsware.com	-	-	×	-	□	-
n123	-	-	-	-	-	-
n157.qa.opsware.com	●	-	□	-	-	-
n130.qa.opsware.com	□	-	□	-	-	×

Name	Type	Status	Compliance Summary
n238.qa.opsware.com			
Audit	Audit	×	Selected Device Out Of Compliance
-005_Compliance_Audit.policy cloumn_twoAudits...	Audit	×	1 of 1 Rules Out Of Compliance
Audit 2	Audit	●	1 of 1 Rules In Compliance
WinPingAudit3	Audit	●	2 of 2 Rules In Compliance
Audit Policy	Audit Policy	□	Selected Device Out Of Compliance
2rules	Audit Policy	●	2 of 2 Rules In Compliance
auditranner-auditpolicy-1296247983.233856	Audit Policy	×	2 of 2 Rules Out Of Compliance
auditranner-auditpolicy-1296248658.185432	Audit Policy	×	1 of 2 Rules Out Of Compliance



Best Practice: You should link your audits to audit policies for the audit rules. This is a common and recommended use case. This structure allows for several audits to be linked to the same audit policy. Each audit can include a different set of servers or server groups that have different recurring schedules. In the Compliance view, in the Audit Policy column, all compliance results for each audit linked to the policy are displayed.

If there is more than one audit with an overlapping set of servers, the Audit Policy column shows the status of the most recent result for each server, regardless of which audit ran last. To view the most recent audit result for a given operation, select an audit and then click **Details**, **Run Audit**, or **Remediate** in the Compliance view. See [Figure 37](#).

An audit policy can be hierarchical. That is, an audit policy can link to other audit policies.

Example:

Policy A links to Policy B. Policy B links to Policy C.

- When an audit is created and linked to Policy A, the audit will run using a flattened list of compliance rules that belong to Policy A, Policy B, and Policy C.
- If you add the Audit Policy column in the Compliance view for Policy A, the compliance status shows the result of the audit with all rules from Policy A, Policy B, and Policy C.
- If there are no audits directly linked to Policy B or Policy C, there are no individual results available for these policies. If you add the Audit Policy column in the Compliance view for these policies, a dash (-) indicates that there are no results to display.




Another difference between the Audit and Audit Policy columns in the Compliance view is that only audits with recurring schedules are available for display. However, any audit policy can be a column, just as it applies to software and patch policies.

The compliance categories (columns) that are selectable for the Compliance view are configurable.

- The default setting includes Audit Policy, Software, Patch, and Configuration.
- For new installations, the Audit category is not listed.

Software Compliance

In Server Automation, software management allows you to create *software policies* that enable you to install software and configure applications simultaneously. A *software policy* can contain several different items, such as packages, RPM packages, patches, application configurations, and other software policies. After creating a software policy, you can attach it to servers or groups of servers.


Software compliance indicates whether items in a software policy are compliant with the actual server configuration. If the actual server configuration does not match the software policy definitions, the server's software policies are Non-Compliant .

The Compliance view derives software compliance information for software policies when you scan a server or group for software compliance.

See the *SA User Guide: Software Management* for more information.

Software Compliance Status Criteria

Software compliance status is determined by the following criteria:

- **Software Compliance—Single Server:** If at least one item in a software policy does not match what is discovered (or does not exist) on the server the policy is attached to, the server's software compliance status is Non-Compliant . The details pane of a server's Device explorer shows the Software category as Non-Compliant and the summary column indicates how many rules (software policy items) are Non-Compliant, out of the total number of rules.

For example, if a software policy contains 10 items and 6 of the items are Non-Compliant, the software policy's status is listed as Non-Compliant and the summary description reads: "6 of 10 Rules Out of Compliance."

If more than one software policy targets a single server and if at least one of those policies is Non-Compliant, the aggregate compliance status for Software is also displayed as Non-Compliant. You can expand the Software category of the details pane to see which of the policies are not in compliance, including a breakdown of how many rules in each policy are either in or out of compliance.

- **Software Compliance—Device Groups:** A software policy attached to a group of servers is considered Compliant *if more than 5% of the servers in the group attached to the policy have a status of Non-Compliant* ❌. If this is the case, the aggregate compliance for software policy displays as Non-Compliant. Another way to understand Non-Compliant for a device group is to remember that *when less than 95% of the servers are Compliant*, a status of Non-Compliant will display.

However, if more than 2%, but less than or equal to 5%, of all servers in a group have the status of Non-Compliant for that category, the status is Partial-Compliant ⚠️. Another way to understand Partial-Compliant for a device group is to remember that *when less than 98% but at least 95% of the servers are Compliant*, a status of Partial-Compliant will display.

If less than 2% of all servers in a group have a Software Policy status of Non-Compliant for that category, the overall status is Compliant. Another way to understand Compliant is to remember that *at least 98% of the servers are Compliant*.

The details pane for a group of servers in the Compliance view shows whether the software policies are compliant or not. This information does not expand to show a breakdown of individual servers and policies.

You can modify the thresholds used to determine compliance for groups of servers.

Software Compliance Remediation

The Compliance view allows you to view all software policies attached to a server or to groups of servers, and to remediate those servers that are out of compliance. This enables you to ensure that a server's software configuration complies with the software policy definition.

For each software policy item—such as software, packages, patches, scripts, and application configurations—software remediation installs (or for a script, executes) those items on the target server. If the items do not exist on the server, they get installed. If the items existed but did not match the policy, they get updated with the correct version.

For example, you have a software policy that consists of several packages, patches, scripts, and an application configuration, all organized in the order in which they are to be installed and executed. First, you remediate the software the policy on a server to make sure the server is in compliance with your company's software installation standards. Over time, some of the items in the software policy get updated—such as a new set of packages gets added—and, for whatever reason, a software item on the server was uninstalled.

When you perform a software compliance scan, the scan determines the server's compliance status by comparing the software policy contents with the actual software installed on the server. Even if only one software item attached to one of the servers is not in compliance with the policy, the server will have a software compliance status of Non-Compliant ❌.

When you remediate a server or group of servers, the patches, packages, and application configurations specified in the policy are installed and applied in the order specified in the policy. For a group of servers, remediation has the same results, only the remediation operation applies to all servers in the group, including all servers contained in any sub-groups.

Remediating Software Compliance for Servers

When you remediate software compliance for a single server or for multiple servers, you can choose to remediate all of the policies attached to the servers or choose to remediate individual policies.

You can select the Software Aggregate policy, which remediates all software policies for all servers selected. If a group is selected, it remediates against all direct server children in that group. If a single software policy is selected in the details pane, the entities selected in the summary pane have that policy remediated.

To remediate software policies on a single server:

- 1 In the navigation pane, select **Devices ► Servers ► All Managed Servers**.
- 2 Select a server in the content pane.
- 3 Right-click and then select **Open** to open the Server browser.
- 4 In the navigation pane, select **Management Policies ► Compliance**.
- 5 In the details pane of the Compliance view, expand the Software category and select an individual software policy or the top level Software category. This selection enables you to remediate policies that are attached to the server.
- 6 Click **Remediate** and then complete the steps in the Remediate wizard. If SA does not find devices to remediate, a warning dialog displays.

To remediate software policies on multiple servers:

- 1 In the navigation pane, select **Devices ► Device Groups**, and then select a group.
- 2 From the View drop-down list, select Compliance.
- 3 In the content pane, select servers.
- 4 In the details pane of the Compliance View, expand the Software category and select a software policy that is attached to the selected servers. Or, select the top level Software category if you want to remediate all of the software policies attached to the selected servers.
- 5 Click one of the following buttons to remediate software policies:
 - **Remediate**: Launches the Remediate wizard that allows you to remediate the selected software policy or policies against the selected server or servers.
 - **Scan Device**: Displays the Scan for Compliance window where you first select the types of policies you want scanned and then click **Scan** to launch the job. This processes scans the selected servers for all Audit, Audit Policy, Software, Patch, and Configuration policies attached to the servers. When you include Configuration in your policy selection, a Scan Configuration Compliance window displays the status of the scan. This action does not have any effect on the audits that target this server.

Remediating Software Compliance for Groups

When you remediate software policies for a single group of servers or for multiple groups of servers, you can remediate all policies attached to all servers in the single group or in multiple groups. However, when you select a group or multiple groups, you can only remediate *all* software policies attached to *all* servers in the group and any sub-groups.

To remediate software policies for a single group of servers or for multiple groups of servers:

- 1 To remediate software policies for a single server in the Device Explorer, in the navigation pane, select **Devices > Servers > All Managed Servers**.
- 2 In the content pane, select a server.
- 3 Right-click and then select **Open** to open the Device browser.
- 4 In the navigation pane, select **Management Policies > Compliance**.
- 5 In the details pane of the Compliance view, expand the Software category and select an individual software policy or the top level Software category. This selection enables you to remediate all policies attached to the server.
- 6 Click **Remediate** and then complete the steps in the Remediate wizard.

Or

- 7 In the content pane that shows a list of servers that belong to the group, select multiple servers by selecting the check box next to each server. (*Optional*) Select **Check All Rows** to select all servers.
- 8 To remediate software policies for multiple servers, in the navigation pane, select **Devices > Device Groups**, and then select a group.
- 9 From the View drop-down list, select Compliance.
- 10 In the details pane of the Compliance view, expand the Software category and select a software policy that is attached to the selected servers. Or, select the top level Software category if you want to remediate all of the software policies attached to the selected servers.
- 11 Click one of the following buttons to remediate software policies:
 - **Remediate**: Launches the Remediate wizard that allows you to remediate the selected software policy or policies against the selected server or servers.
 - **Scan Device**: Displays the Scan for Compliance window where you first select the types of policies you want scanned and then click **Scan** to launch the job. This processes scans the selected servers for all Audit, Audit Policy, Software, Patch, and Configuration policies attached to the servers. When you include Configuration in your policy selection, a Scan Configuration Compliance window displays the status of the scan. This action does not have any effect on the audits that target this server.

Configuration Compliance

In Server Automation, an *application configuration* manages configuration files on a managed server. An application configuration can manage one or several configuration files for an individual server or for group of servers. Each application configuration includes one or more templates that model an ideal configuration state for the fields. These templates help you manage configuration values (*key-value pairs*) for specific files on a server.

For example, you can create an application configuration that manages the hosts file for servers in your data center. You can define the IP address-hostname key-value pairs for a standard Unix hosts file and then attach the application configuration to several servers or to a group of servers that contain the file. The *application configuration* serves as *the policy that helps ensure that the hosts files on the target servers have the correct IP address-hostname definitions*.

Application configuration compliance indicates whether all of the application configurations (policies) attached to a server are compliant with the actual application configuration files on the managed server. In the hosts file example, if the information inside the hosts file in a server configuration does not match the values defined in the application configuration, the server's Configuration is Non-Compliant ✘. If more than one application configuration is attached to a server and any one of the actual configuration files targeted by the application configuration is different, the entire server is shown as Non-Compliant in the Compliance view.

Conversely, if there are no differences found between the application configuration and the files on a server, the Configuration compliance status is Compliant ●. All application configurations must be 100% compliant for the server's Configuration compliance status to display as Compliant in the Compliance view.

To check the latest state of a configuration file targeted by an application configuration, you can perform an application configuration compliance scan to determine whether there are any differences between the application configuration and the actual configuration files on the server.

See the *SA User Guide: Application Configuration* for more information.

Configuration Compliance Status Criteria

Configuration compliance status is determined by the following criteria:

- **Configuration Compliance—Single Server:** If any differences are discovered between the application configuration and the actual configuration file on the target server, the server's Configuration compliance status is Non-Compliant ❌. The details pane of a server's Device explorer shows the Configuration category as Non-Compliant. If the server has several application configurations attached to it and any one of the actual configuration files targeted by the application configuration is different than the application configuration, the entire server is considered Non-Compliant in the Compliance view.
- **Configuration Compliance—Device Groups:** An application configuration attached to a group of servers is considered Compliant *if more than 5% of the servers in the group attached to the application configuration have a status of Non-Compliant* ❌. If this is the case, the aggregate compliance for Configuration displays as Non-Compliant. Another way to understand Non-Compliant for a device group is to remember that *when less than 95% of the servers are Compliant*, a status of Non-Compliant will display.

However, *if more than 2%, but less than or equal to 5%, of all servers in a group have the status of Non-Compliant for that category*, the status is Partial-Compliant ⚠️. Another way to understand Partial-Compliant for a device group is to remember that *when less than 98% but at least 95% of the servers are Compliant*, a status of Partial-Compliant will display.

If less than 2% of all servers in a group have a Configuration status of Non-Compliant for that category, the overall status is Compliant. Another way to understand Compliant is to remember that *at least 98% of the servers are Compliant*.

The details pane for a group of servers in the Compliance view shows whether the application configurations are compliant or not. This information does not expand to show a breakdown of individual servers and policies.

You can modify the thresholds used to determine compliance for groups of servers.

Remediating Configuration Compliance—Servers and Groups

Remediation for an application configuration is slightly different than the other compliance category types. Rather than remediating a policy on a server (as you can with Audit Policy, Software, or Patch), to remediate an application configuration, you select an application configuration in the Device explorer or Group explorer. You then use the *push* function to push the values defined in the application to the actual configuration files on the server or group of servers. When you push an application configuration, all values defined in the application configuration templates are added to or replace those on the target configuration files.

The manner in which a value in an application configuration get pushed, such as sequences of lists and scalars, depends on how those values have been set in the application configuration inheritance hierarchy and what sequence merge modes have been configured in the configuration template.

To remediate application configurations on a server or on a group of servers:

- 1 To remediate an application configuration for a single server in the Device Explorer, in the navigation pane, select **Devices** ► **Servers** ► **All Managed Servers**, and then select a server.
Or
- 2 To remediate an application configuration for a group of servers, in the navigation pane, select **Devices** ► **Device Groups**, and then select a group.
- 3 Right-click and then select **Open** to open the Device browser.
- 4 In the Information pane, select **Management Policies** ► **Configured Applications**. See the *SA User Guide: Application Configuration* to continue. See also:

Index

Symbols

/etc/passwd file, 51

A

ACL. See Windows Access Control List., 46

ad hoc audit, running, 22

Anonymous Authentication, 55

AppConfig templates, 51

application configuration
definition of, 147
example policy, 119

archived audit result, 12

archived snapshot, 12

audit

auditing process, 17

audit results

viewing and remediating, 93

audits and the Compliance view, 16

configuring, overview, 27

definition of, 12, 15, 16, 140

elements of, 18

re-running from audit results, 23

results, value based remediation, 92

running from the SA Library, 21

running on a server, 22

saving as audit policy, 83

scheduling, 84

scheduling recurring, 24

searching for, 97, 106

selection criteria

inclusions/exclusions, 69

snapshot used in, 101

sources, server or snapshot, 28

viewing completed audit job, 25

ways to create, 19

creating from a server, 20

from a group of servers, 20

from an audit policy, 21

from a snapshot, 21

from the SA Library, 20

Audit and Remediation

audit policies, 78

audit process overview, 17

audit results, 84

capturing golden server configuration, 14

creating an audit policy, 79

deleting

snapshot specification, 109

examples (use cases), 14

exceptions, 76

adding to an audit, 77

editing, 77

rules that cannot have exceptions, 76

linking and importing audit policies, 81

rules

configuring, application configuration, 36

configuring, COM+, 40

configuring, compliance checks, 64

configuring, custom script, 41

configuring, file system, 45

configuring, hardware, 52

configuring, IIS Metabase, 53

configuring, operating system, 58

configuring, users and groups, 60

configuring, Windows Registry, 61

configuring, Windows services, 62

server objects, 31

scheduling audits, 24

selection criteria

inclusions/exclusions, 69

terms and concepts, 12

viewing

and remediating audit results, 93

ways to create an audit, 19

audit compliance, definition of, 140

audit job, definition of, 12

audit policy

creating, 79

definition of, 12, 15, 78

example of, 119

exporting to HTML or CSV, 84

linking and importing, 81

locating in the SA library, 84

saving, 83

audit result, definition of, 12

audit rule type, definition of, 12

Audit Servers wizard, 142

B

best practice

- archiving audit results, 97
- BSA Essentials Subscription Services, 11
- deleting audit results, 96
- environment variable in pathnames, 75, 81, 83, 96, 97
- how to use an audit policy, 15
- linked rule, 50
- linking an audit policy or snapshot specification, 78
- linking an audit policy to an audit or snapshot specification, 81
- linking audit rules to audit policies, 14
- sources for a file rule, 50

BSA Essentials Subscription Services, 11, 13, 14, 66, 68

C

Center for Internet Security, 11

check. See rule., 13

checksum, 46

CIS. See Center for Internet Security., 11

COM+, 17

COM+ object

- configuring Audit and Remediation rule, 40

Common Vulnerabilities and Exposures, 14

compliance

- application configuration, 147
- patch, 137
- software, 143

compliance, definition of, 13, 119

compliance category, definition of, 119

Compliance Check Editor, 66, 67, 68

compliance checks

- configuring Audit and Remediation rule, 64
- creating custom categories, 68
- editing properties, 67
- managing, 66
- restoring to defaults, 68

Compliance Dashboard. See Compliance view., 117

Compliance dashboard. See Compliance view., 119

compliance dashboard. See Compliance view., 16

compliance policy, 117

- definition of, 119

compliance rule, definition of, 119

compliance scan

- definition of, 119
- examples of, 136

compliance scan results, definition of, 119

compliance statuses, definition of, 119

compliance status for Compliance view, 120

compliance summary details list, 126

compliance summary pie chart, 126

Compliance view, 16

- application configuration, 147
- audit, 140
- compliance statuses, 120
- definition of, 119
- general categories, 136
- overview, 117
- patch, 137
- refreshing, 132
- remediation overview, 136
- software, 143
- terms and concepts, 125

compliant, definition of, 117

Configuration Compliance Scan, 136

copying

- objects to a server from a snapshot, 107

creating

- audit policy, 79
- custom compliance checks categories, 68
- snapshot specification, 109
- snapshot specification from library, 109

custom script

- configuring Audit and Remediation rule, 41

CVE. See Common Vulnerabilities and Exposures., 14

D

deleting

- snapshot, 96, 106
- snapshot job schedule, 115
- snapshot specification, 109

Discovered Software rule, 33

E

editing

- audit rule exceptions, 77
- audit schedule, 25
- compliance checks properties, 67
- snapshot job schedule, 114

exception, definition of, 12

exceptions

- about, 76
- adding to an audit, 77
- considerations, 76
- rules that cannot have exceptions, 76

exporting
audit policy, 84

F

Federal Information Security Management Act, 11
File System
configuration Audit and Remediation rule, 45
FISMA. See Federal Information Security Management Act., 11, 13

G

golden server, 12, 14, 16, 51

H

hardware, configuring Audit & Remediation rule, 52
Hardware rule, 33
hosts file, managing, 147
HP Live Network, 11
HPLN. See HP Live Network., 11

I

IIS Metabase, 15, 16
configuring Audit and Remediation rule, 53
importing
audit policy rules, 83
IP address-hostname key-value pairs, Unix hosts file, 147

K

key-value pairs, application configuration, 147

L

linked rule, 50
linking an audit policy to audit or snapshot specification, 81
locating audit policies in the SA Client library, 84

M

master audit policy, 82

N

negative server configuration, 140
Non-Compliant, definition of, 127

O

object differences, 120
OpenSolaris, security vulnerabilities, 14

operating systems
configuring Audit and Remediation rule, 58

P

parameterized checks, 75
passwd.tpl, 51
patch compliance, 137
patch compliance scan, 136
patch policy, example of, 119
patch policy exceptions, 136
Payment Card Industry, 11
PCI. See Payment Card Industry., 11
policy setter, 13, 117
PPD File Manager, 14
ppdmgr. See PPD File Manager., 14
push, application configuration, 149

R

reflexive auditing, 30
Remediate wizard, 138, 139, 142, 145, 146
remediation, definition of, 134
remediation value, 33, 34
restoring compliance checks to defaults, 68
rule
definition of, 13
linked, 50
server-based, 13
unlinked, 50
user-defined, 13
rule exception. See exception., 12
rule exceptions
adding to an audit, 77
rules
non-compliant, 120
Rules window, 142
running
ad hoc audit, 22
audit from server, 22
audit from the SA Library, 21
snapshot specification, 112

S

Sarbanes-Oxley, 11, 13
saving
audit or snapshot specification as audit policy, 83
snapshot specification as policy, 111

- scalars, application configuration, 149
- scheduling
 - audit, 84
 - audit, recurring, 24
 - snapshot job, 113
- search
 - audit, 97, 106
- server-based rule, 13
- Server Object, 34
- server object, definition of, 13
- server objects, 31
- snapshot
 - copying objects to server from, 107
 - definition of, 13, 16
 - deleting, 96, 106
 - template, 109
 - deleting job schedule, 115
 - difference between snapshot specification, 100
 - editing job schedule, 114
 - locating, 103
 - locating in SA Client, 115
 - process, 99
 - scheduling, 113
 - used in an audit, 101
 - used with audit policies, 108
 - viewing contents of, 104
- snapshot specification, 108
 - and audit policies, 108
 - configuring rules for, 111
 - creating from library, 109
 - creating from server, 109
 - definition of, 13
 - deleting, 109
 - elements of, 101
 - relationship to snapshots, 100
 - running, 112
 - selection criteria
 - inclusions/exclusions, 69
- snapshot specification job, definition of, 13
- software compliance
 - compliance remediate options, 144
 - Compliance view, 143
- Software compliance scan, 136
- software policy, 117
 - definition of, 143
- Subscription Services. See BSA Essentials Subscription Services., 11
- Sun Solaris 10, security vulnerabilities, 14

T

- target, definition of, 13
- Target Value, 34

U

- unlinked rule, 50
- user-defined rule, 13
- users and groups, configuring, 60

V

- viewing
 - audit results, 93
 - audit server usage, 21
 - completed audit job, 25
 - Compliance view, 125
 - snapshot contents, 104

W

- Windows Access Control List, 46
- Windows CIS, 120
- Windows Registry
 - configuring rule, 61
- Windows services
 - configuring Audit and Remediation rule, 62