helpsystems

User Guide

Security Auditor

4.2.1

Copyright Terms and Conditions

201810221002

Welcome to Security Auditor 1
What is Security Auditor and Why Use It? 2
Getting Started 4
Starting Security Auditor on Windows 4
Starting Security Auditor on AIX or Linux 4
Launching the application from your browser 4
Stopping the Security Auditor web server 5
Web browser troubleshooting tips 5
Licensing 6
Current Version 6
Upgrading to the Current Version 6
Adding Security Auditor Users 7
Time out 8
Adding Servers to Manage 9
Adding a Windows Server 9
Adding a Non-Windows Server 11
Adding Multiple Servers 13
Server Groups 16
Adding, Monitoring, and Managing Cloud Services 18
Adding a Cloud Service Account 18
Defining and Validating Filters 19
Policy Overview 21
Group Policies and Private Policies 21
Initializing Policies 22
Copying Policies to Another Server and using the Export / Import Feature 26
Replace Template Options 27
Importing Policies 27
Managing S3 Bucket Policies 29
Enabling S3 Bucket Policies 29
Managing S3 Bucket Policies 29
Using Security Auditor 32
Configuration Values 33
Initializing 33
Using the Configuration Category 33
Running a compliance check 33
Running FixIt 34
Daemons 36
Initializing 36
Using the Daemon category 36
Running a compliance check 36
Discovering new daemons 37
Running FixIt 37
Exported Directories 39
Initializing 39
Running a compliance check 39
Running FixIt 39
Defining Templates 39
User Accounts 41
Files 50
Running a compliance check 52
Running a compliance check 54
Running FixIt 55
Scripts 56
Defining a Script Policy 56
Running a Compliance Check 57
Running FixIt 58
Return Codes 58
Exporting and Importing Script Packages 59

FixIt 60
FixIt in Test Mode 60
Running FixIt 60
FixIt Restrictions 60
Scheduling Security Auditor Jobs 61
Backing Up Security Auditor 62
Backup Scripts 62
Script location 62
Scripts 62
Running the Backup Scripts 63
Working with Reports 64
Documenting your Policy 64
Checking compliance 64
Documenting what FixIt Fixed 64
Generating and Viewing Reports 64
Report Formats 65
Emailing Reports 65
Removing Security Auditor from your Servers 65
Removing Security Auditor from the Console: 65
Reference 67
Add/Modify AWS Cloud Service Account 68
How to Get There 68
What it Does 68
Options 69
Add/Edit Filter 71
How to Get There 71
What it Does 71
Options 71
Managed Server Information 73
Installation Connection Information 74
Installation Configuration 74
Add Multiple Servers screen 76
How to get there 76
Server Information 77
Add/Modify Private Key 79
How to Get There 79
Options 79
Add/Modify Shared Bucket Policy 81
How to Get There 83
What it Does 83
Options 83
Properties 83
Permissions 89
Management 92
Add a New Server screen 93
How to get there 93
Server Information 94
Installation Information 95
Add/Modify Files Template screen 97
How to get there 97
What it Does 97
General tab 97
Selections tab 98
Policies tab 99
Compliance tab 102
Add a New Script Policy screen 103
How to Get There 103
What it Does 103
General tab 103

Return Codes tab 104

Add a New User Accounts Policy Template screen 106

How to get there 106

What it Does 106

General tab 106

Selections tab 107

Policies tab 108

Compliance tab 115

Add/Modify Scheduled Job 117

How to Get There 117

Options 117

General tab 117

Servers tab 118

Tasks tab 119

Bucket Policy Categories 121

How to Get There 121

What it Does 121

Options 121

Columns 122

Bucket Policy Category Details 123

How to Get There 123

What it Does 123

Options 123

Columns 124

CheckIt Screen 125

How to get there 125

Servers tab 125

Field Descriptions 126

Policies tab 126

Select Policy Categories 126

Consolidated Reports screen 127

How to get there 127

Servers tab 127

Policies tab 128

Options tab 128

Create AWS Account Reports screen 130

How to get there 130

Accounts tab 130

Select Accounts 130

Options tab 131

Create Reports screen 134

How to get there 134

Servers tab 134

Policies tab 135

Options tab 136

Export screen 139

How to get there 139

Export Server tab 139

Policies tab 139

File tab 140

Import Servers tab 140

Notes tab 140

Export Scripts Package 142

How to Get There 142

Servers tab 142

Scripts tab 142

Destinations tab 142

FixIt Screen 144

How to get there 144

Servers tab 144

Policies tab 145

Import screen 146

How to get there 146

Source tab 146

Servers tab 147

Policies tab 147

Import Scripts Package screen 148

How to get there 148

Source tab 148

Servers tab 148

Initialize Policies screen 150

How to get there 150

Servers tab 150

Policies tab 151

Manage AWS Cloud Service Accounts 152

How to get there 152

What it Does 152

Options 152

Column Descriptions 152

Manage Filters 154

How to Get There 154

What it Does 154

Options 155

Manage Licenses screen 156

How to get there 156

Installed Licenses 156

Upload Licenses 156

Manage Logging screen 158

How to get there 158

Application Tab 158

Log Files 158

Package logging levels 158

Field Descriptions 159

Syslog Tab 159

Manage Private Keys 160

How to Get There 160

Options 160

Field Descriptions 161

Manage Scheduled Jobs screen 162

How to get there 162

Options 162

Field Descriptions 162

Manage Shared Bucket Policy 164

How to get there 164

What it Does 164

Options 164

Column Descriptions 164

Manage Servers screen 166

How to get there 166

What it Does 166

Options 166

Manage Users screen 169

Field Descriptions 169

Modify Configuration Policy Attribute 171

How to get there 171

Field Descriptions 171

Modify Server screen 173

How to get there 173

Field Descriptions 173

Manage Scheduled Jobs screen 175

How to get there 175
Options 175
Field Descriptions 175
Modify Configuration Policy Attribute 177
How to get there 177
Field Descriptions 177
Modify Server screen 179
How to get there 179
Field Descriptions 179
Policy Values 181
Booleans 181
Integer 181
Dates 181
String 181
Backslashes, escapes, and quoting 186
Character Classes 186
Preferences screen 188
How to get there 188
General tab 188
Email Server tab 190
Cloud Services tab 191
Servers and Policies - Configuration 193
How to get there 193
What it Does 193
Servers and Policies - Daemons 216
How to get there 216
What it Does 216
Field Descriptions 217
Servers and Policies - Exported Directories 219
How to get there 219
What it Does 219
Table Options 220
Field Descriptions 220
/etc/exports 220
Directories 221
Servers and Policies - Files 222
How to get there 222
What it Does 222
Field Descriptions 223
Servers and Policies - Scripts 224
How to get there 224
What it Does 224
Field Descriptions 225
Servers and Policies - User Accounts 226
How to get there 226
What it Does 226
Field Descriptions 227
Upload a Script or Package to Console 228
How to get there 228
Upload shell script 228
Upload Script Policies zip file 228
Validate Filter screen 230
How to Get There 230
What it Does 230
Column Descriptions 230
View Daemon Details screen 232
How to get there 232
Field Descriptions 232
View Exported Directory Details screen 234
How to get there 234

Field Descriptions 234

View Reports screen 236

How to get there 236

Options 236

Field Descriptions 236

Appendix: Configuring Security Auditor for SSL Mode 238

Generating a Self-Signed Certificate 238

Enabling the Certificate 239

After You Are Done 240

Policy Values 241

Booleans 241

Integer 241

Dates 241

String 241

Backslashes, escapes, and quoting 246

Character Classes 246

Welcome to Security Auditor

Thank you for using Powertech Security Auditor. Security Auditor helps you with automating security administration as well as policy and security configuration management, compliance and monitoring. This manual provides information on how to use Security Auditor. If you can't find the answer to your question in this manual, see HelpSystems Support for additional resources and help.

What is Security Auditor and Why Use It?

Powertech Security Auditor is a product that automates security administration and policy compliance tasks and reporting. With Security Auditor you can:

- Check compliance and configuration of user accounts, directories, files, configuration settings, daemons, exported directories and more.
- Check compliance on a single server with a Private Policy, or check several servers against the same policy using a Group Policy.
- Monitor for changes to ownership, permissions and attributes for a specific set of files or directories.
- Deploy and run custom scripts to managed servers through the integrated cron function.
- Report the compliance status of running user-written scripts using the Security Auditor reporting function.
- Monitor for changes to the contents of critical application, configuration or server files.
- Use the Export/Import function to:
    - enforce the same policy requirements across multiple servers.
    - copy the required settings to new servers and configuring them using FixIt to set them to your required settings
- Email exception-based compliance reports, policy, FixIt or Message log reports to yourself and others.
- Document your security implementation with unique templates that reflect your security policy requirements.
- Use “Fix-It” to return out of compliance items to your security policy specifications.

Help for Managing your Compliance Requirements and your Servers

Security Auditor is a tool for to help you reduce the cost of attaining and staying in compliance with your security policy requirements. In addition, many organizations are using Security Auditor to address - not only compliance - but security administration issues as well. Here are some of the ways Security Auditor is being used:

> **NOTE:** Most of our clients performed many of the following processes “manually” before implementing Security Auditor to replace them. By automating such procedures, they reduced the time and resources it took them to ensure that their systems remain in compliance, resulting in measurable cost savings.

- Discover files with either the SUID or SGID bit set then monitor them for changes to their ownership, permissions or attributes.
- Discover when the sudoers file has been changed by using the checksum function.
- Ensure key system files are not world-writable.

- Schedule a cron job to run regular compliance checks on the daemons category to find when a daemon has been activated that shouldn't have been. Schedule the FixIt function to set the daemons to the appropriate value (turn them on or off as appropriate).
- Upload your user-written scripts to run customized compliance checks and FixIt scripts.
- Ensure all user accounts have been created - and remain - with the appropriate attributes.
- Discover new admin accounts.
- Discover user accounts with UID of 0 (root being the allowed exception, of course!)
- Discover user accounts with non-unique UIDs.
- Ensure all files for an application have the appropriate owner, group and permissions. Receive a detailed report specifying any files not figured correctly. Run FixIt to change the settings.
- Discover and manage inactive user accounts.
- Ensure that the exported directories that are required for your servers remain along with their appropriate settings.
- Aid with auditor and compliance requirements by ensuring password rules are set appropriately - both for the global settings and at the user level.
- Easily set-up new servers by defining file and user account templates, daemon and configuration settings, exporting the policies to the new server and running FixIt to set the configuration.
- Use the integrated cron function to setup regular compliance checks and immediate FixIt tasks to keep your servers in compliance.
- Document policy exceptions along with the policy then print the policy when the auditor appears - no more scrambling to find previous years' documentation or writing up the exception in the middle of your audit.

Getting Started

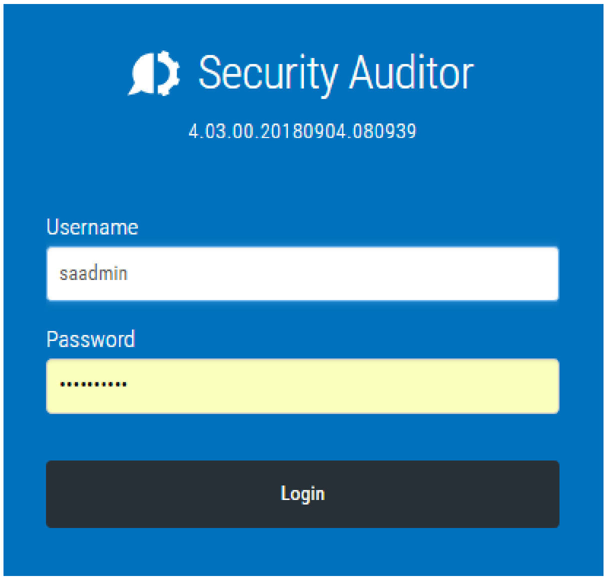
Follow the instructions for the operating system you are using to run the console.

Starting Security Auditor on Windows

On Windows, the Database and Tomcat start automatically during installation.

To start the application

1. Go to **Start** > **All Programs** > **Powertech Security Auditor** > **Security Auditor**. Your browser opens the Security Auditor login screen.



Security Auditor

4.03.00.20180904.080939

Username: saadmin

Password: ••••••••••

2. The first time you login, use user saadmin and password saadmin for your login credentials.

> **NOTE:** You can manually start and stop the Database and Tomcat, and configure their settings using additional shortcuts in the Windows Start menu.

Starting Security Auditor on AIX or Linux

Navigate to the directory where the console was installed and run the `startsa.sh` script.

> **TIP:** If `startsa.sh` fails, logout, login, then run the command again.

Launching the application from your browser

On Windows, the Start Menu shortcut opens Security Auditor using 'localhost.' Whether you are using Windows, Linux, or AIX, if you are launching your browser on the system on which the console is running, you can use the following 'localhost' URL to access the application:

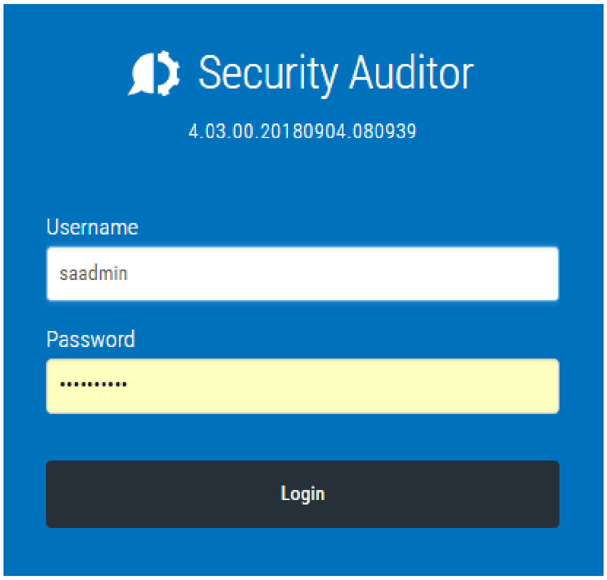
http://localhost:8080/securityauditor/

Otherwise, type the TCP/IP address or server name:

http://172.20.0.60:8080/securityauditor/

> **NOTE:** Both of the above URLs assume you have not changed the port the web server is listening on (the default is 8080). If you have changed the port, replace "8080" with the new port.

The Security Auditor login screen appears:



Security Auditor

4.03.00.20180904.080939

Username: saadmin

Password: ••••••••••

Sign on with the user saadmin and password saadmin. After this initial sign on you'll want to create your own user account to run the product. See the section, Adding Security Auditor Users later in this chapter for instructions.

Stopping the Security Auditor web server

To end Security Auditor on AIX or Linux

1. Log out of the application.
2. Close your browser.
3. To go the directory where the console was installed and run the stoppm.sh script.

To end Security Auditor on Windows

Close the browser. If you would like to stop the Security Auditor database and Tomcat services, you can do so under the Windows Start menu (**Start** > **Powertech Security Auditor** > **Stop Security Auditor**).

Web browser troubleshooting tips

- Make sure that the database is started.
- Make sure that Tomcat is started.
- On Windows, to start both the database and Tomcat go to **Start** > **Powertech Security Auditor** > **Start Security Auditor**.

- If the web page is not displayed, make sure there are no local or network firewalls or routers blocking access.

Licensing

You will be given temporary licenses that you can use to manage some servers for a period of time. During this time Security Auditor is fully functional but it will stop working at the end of the temporary license period.

After purchasing Security Auditor, you will be provided with a file containing permanent licenses for the number of servers you are going to manage through Security Auditor. The managed server license file is imported to the console. Licenses are NOT entered on each server being managed. Licenses are not assigned to each managed server; therefore, you can choose which servers are managed through the console but the number cannot exceed the number of purchased licenses. If you run out of licenses, you must purchase more.

You can stop managing a server through the console and 'free up' the license, but to do so, you must delete the server from the console. Doing that removes all of the data for that system and you must start all over if you choose to manage it again in the future.

Uploading the License File

To upload the license file into the console, do the following:

1. Go to **Admin Tasks > Manage Licenses**.
2. You will see prompts for Customer name and Key. These should be entered EXACTLY as they were sent to you in an email. The easiest way to ensure they are entered correctly is to use the copy and paste feature.
3. Browse to the location of the license file sent to you.
4. Upload the file. Or, you can place the license file in the following directory (where Security Auditor was installed):

.../PowerTech/SecurityAuditor/tomcat/webapps/securityauditor/WEB-INF/license

Current Version

To determine what version of Security Auditor is installed on your console, go to **Help > About Security Auditor**. Choose **Help > Powertech Website** to open the Powertech website where you can find the current version.

Upgrading to the Current Version

If you already have Security Auditor installed, you will follow the same installation steps to upgrade the product as you did when first installing the product. First, you may want to export your policies to a file to back-up your work prior to the upgrade. (For more information, see the section on using the Export / Import feature earlier in this chapter.)

After backing up your policies, do the following:

To Upgrade on Windows

1. Go to **Start > All Programs > Powertech Security Auditor > Stop Security Auditor**.
2. Launch the executable that you've downloaded from the Powertech website and follow the instructions.

To Upgrade on AIX or Linux

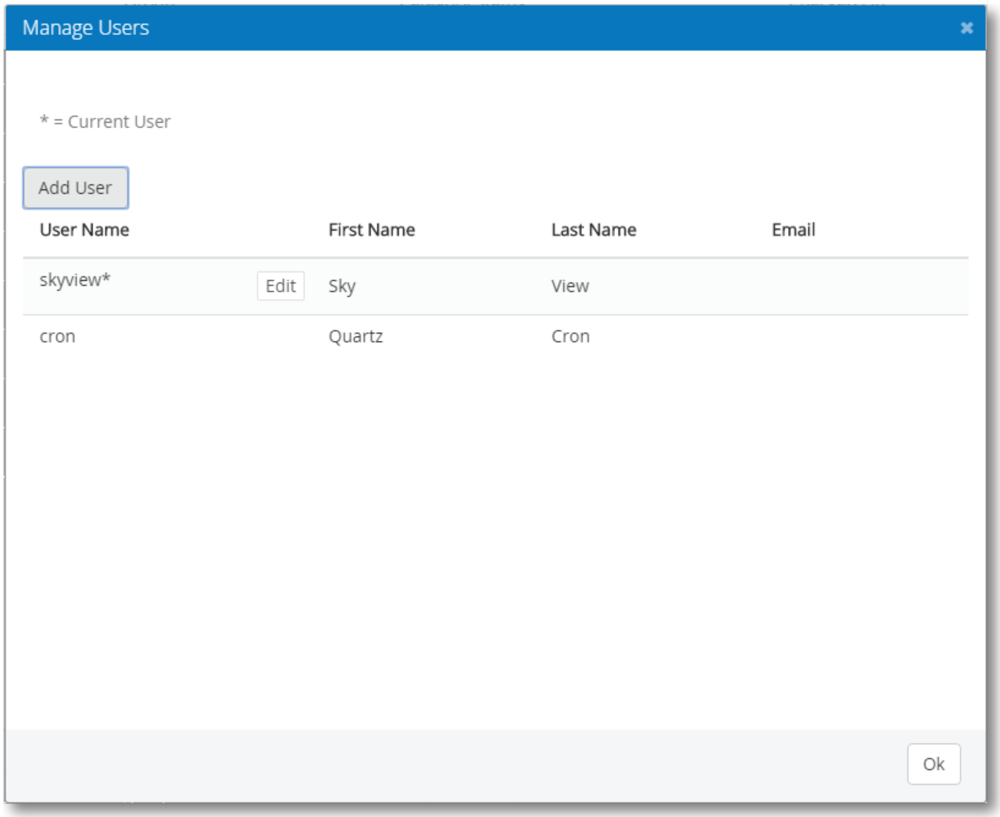
1. Navigate to where Security Auditor was installed and run the stoppm.sh script.
2. Follow the install instructions.

Adding Security Auditor Users

To get started, you'll sign on with the user saadmin and password saadmin. After this initial sign on you'll want to create your own user account to run the product. To create your own user account, do the following:

1. Go to the task bar and choose **Admin Tasks > Manage Users**.
2. Click **Add User**.
3. Complete the form and click **Add User**.

   Since many laws and regulations forbid the use of default passwords, we highly recommend that you change the password for the user; however, make sure you remember what it is because it's non-recoverable if you lose it. A safeguard would be to have another user defined so you can always sign on to the Security Auditor console.



* = Current User

User Name	First Name	Last Name	Email
skyview*	Sky	View	
cron	Quartz	Cron	

Time out

Security Auditor sessions time out after 15 minutes of inactivity. This is to ensure compliance with various laws and regulations and to ensure sessions are not left available for others to use. If you are in the middle of creating or modifying a template and you stop working on it for 15 minutes or more, your work will be lost.

Adding Servers to Manage

You can manage AIX, Linux, and Windows servers from the same Security Auditor console. The supported versions and distributions are:

- AIX 5.3, 6.1 and 7.1
- RHEL 6 & 7, Ubuntu 14 & 15, CentOS 6 & 7, Oracle Linux 6 & 7, and SLES 11 & 12
- Windows 7 or newer, Windows Server 2008 or newer (local User Account policies only)

> **NOTE:** sudo must be installed on the Linux server PRIOR to adding a Linux managed server.

Security Auditor can also monitor a cloud service, such as AWS, and enroll server instances automatically to be checked against a Group Policy. See Working with Cloud Server Instances.

Adding a Windows Server

> **NOTE:** Support for monitoring Windows servers is currently only available if the console is installed/run on Windows.

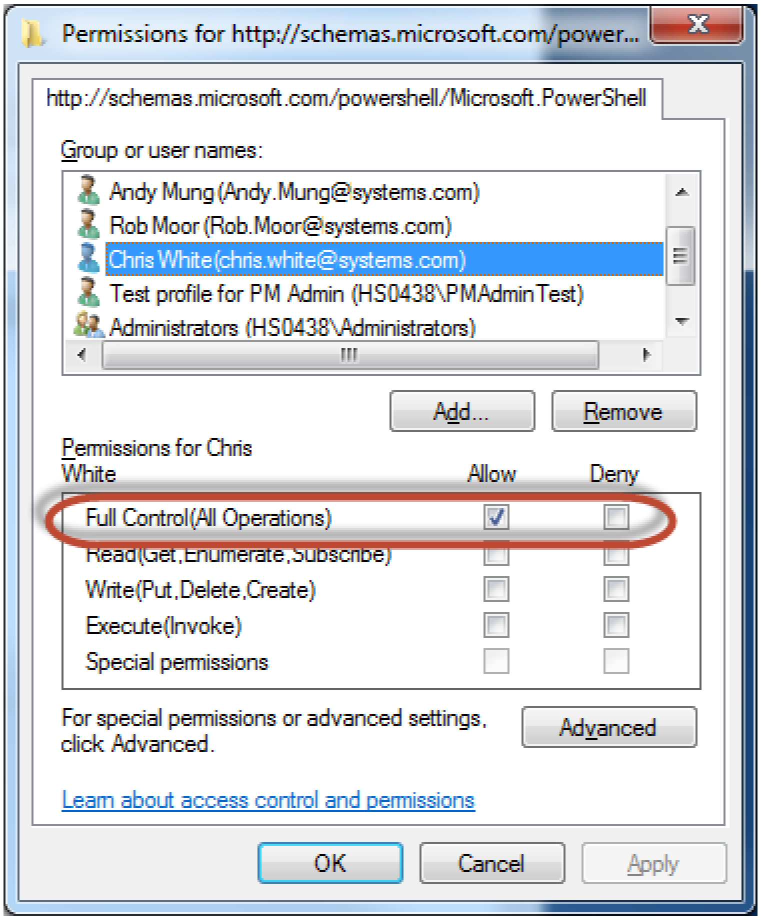
Security Auditor allows you to manage User Account policies for local users on Windows systems in your network. Do the following to add a Windows server:

1. On the remote computer, run the following Powershell commands:

   ```
   Enable-PSRemoting -Force

   Set-PSSessionConfiguration -ShowSecurityDescriptorUI -Name
   Microsoft.PowerShell -Force
   ```

   The second command launches the Permissions dialog box.



Permissions for http://schemas.microsoft.com/power...

http://schemas.microsoft.com/powershell/Microsoft.PowerShell

Group or user names:

- Andy Mung (Andy.Mung@systems.com)
- Rob Moor (Rob.Moor@systems.com)
- Chris White (chris.white@systems.com)
- Test profile for PM Admin (HS0438\PMAdminTest)
- Administrators (HS0438\Administrators)

Permissions for Chris White	Allow	Deny
Full Control(All Operations)	☑	☐
Read(Get,Enumerate,Subscribe)	☐	☐
Write(Put,Delete,Create)	☐	☐
Execute(Invoke)	☐	☐
Special permissions	☐	☐

For special permissions or advanced settings, click Advanced.

The connecting user must be given "Full Control" access on that dialog. The connecting user must also have sufficient access to run the commands.

2. To enable authentication, add the remote computer to the list of trusted hosts for both the console and managed endpoints. Enter the following Powershell commands to:

   a. List the current values.

   ```
   Get-Item -Path WSMan:\localhost\Client\TrustedHosts
   ```

   b. Add your new servers. Append servers to the end, separated by commas.

   ```
   Set-Item WSMan:\localhost\Client\TrustedHosts -Value
   'server1,server2'
   ```

> **NOTE:** As such, the Security Auditor console inserts managed endpoints here `-Value 'server1,server2'` and the managed endpoints put the Security Auditor console here –`Value 'server1,server2'`.

3. Open Security Auditor in your browser.
4. If you use the same administrator account to login to systems across your network, and would like to setup Security Auditor to use that account automatically when setting up new Windows servers to be managed, go to **Admin Tasks > Preferences**. Under "Windows User," enter the credentials for your administrator account and click **Save**.

5. Go to **Servers > Add a Server** or click **Add** on the Manage Servers page.
6. For Server Type, choose **Windows**, then enter a name, description, group and IP address.

   > **NOTE:** If you would like to create a new Group, check **New Group** and enter the name of the Group. If this Group should include a Shared Policy, check **New Group shares policy**. See Policy Overview for details. Also note that if you check 'New Group' and the Group already exists, Security Auditor will add the servers to the existing Group.

7. For Connection Option, choose **Default User and Password** to use the credentials you specified in the Preferences screen. Or, choose **Server Specific User and Password** to specify the credentials for this server individually.
8. Click **Save**. You are now ready to begin defining User Account policies. See User Accounts.

Adding a Non-Windows Server

1. Go to **Servers > Add a Server** or click Add on the Manage Servers page. The Add a New Server screen appears.
2. Fill in the dialog with the details of the server you want to manage through the Security Auditor console.
   - For Name, you can use the following variables:
     - {nameoripaddress}
     - {servertype}
     - {hostname}
   - For Description, you can use the following variables:
     - {name}
     - {nameoripaddress}
     - {servertype}
     - {hostname}
   - For Name or IP Address, you can use the variable {name}
3. For Group, you can select an existing group, or check **New Group** to create a new one. See Server Groups.

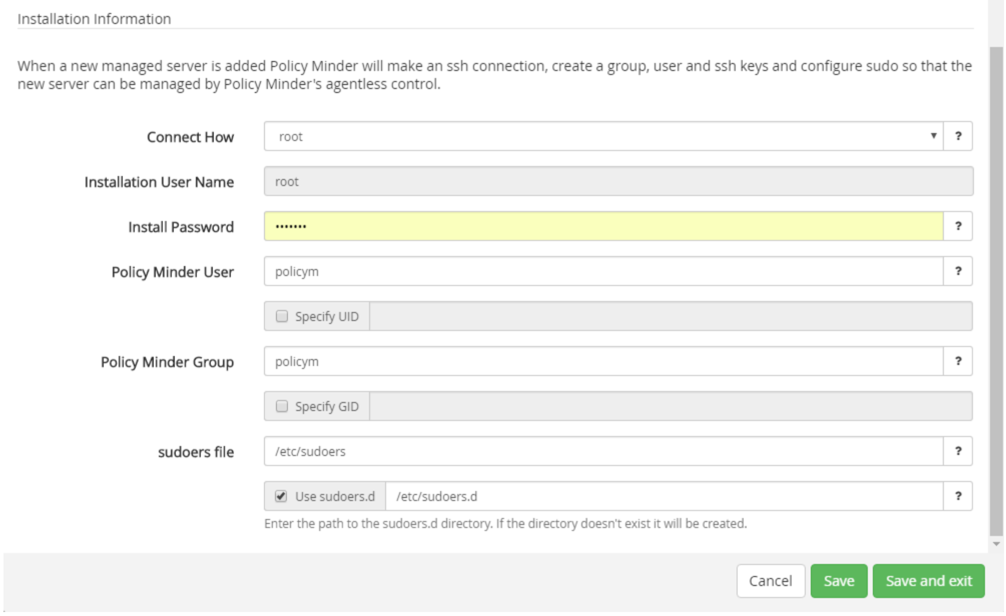
   > **NOTE:** When adding a new Group, if it should include a Shared Policy, check **New Group shares policy**. See Policy Overview for details. Also note that if you check 'New Group' and the Group already exists, Security Auditor will add the servers to the existing Group.

4. Specify the Installation Information:

   Options when adding a non-Windows server

   Option 1: If you take the default settings, you will need to provide root's password to make the initial connection. When the connection is made, the Security Auditor User policym and the Security Auditor Group policym will be created and the sudoer's file updated to provide the user policym with the ability to run the commands needed for the Security Auditor product.

Subsequent connections are made via SSH and use certificates, not user / password to establish the connection.



Installation Information

When a new managed server is added Policy Minder will make an ssh connection, create a group, user and ssh keys and configure sudo so that the new server can be managed by Policy Minder's agentless control.

Connect How	root
Installation User Name	root
Install Password	•••••••
Policy Minder User	policym
	□ Specify UID
Policy Minder Group	policym
	□ Specify GID
sudoers file	/etc/sudoers
	☑ Use sudoers.d /etc/sudoers.d

Enter the path to the sudoers.d directory. If the directory doesn't exist it will be created.

Alternative to Option 1: Some organizations do not allow root to make an SSH connection. In this case you can use su. Use the drop down box for Connect How and choose su. You will be prompted to enter root's password (so you can use SU on the server you're adding). You must also specify a user and password to make the initial connection. This user MUST be able to SU to root.

Another alternative to Option 1: Ubuntu doesn't have the concept of root so when adding an Ubuntu server, use the option to connect with sudo. To choose this option, use the drop down box for Connect How and choose sudo. The user specified in the Installation User Name field must be a user who can execute admin commands using sudo.

Option 2: By default a user and a group named policym will be created on each server. You may want to create a user and/or group by a different name than policym. Or you may want to specify the UID or GID for the user/group. To do so, name the user, group, and specify a UID and GID.

> **NOTE:** If the user or group do not already exist, they will be created with the UID / GID specified (if any).)

Option 3: By default, the commands required by Security Auditor will be added on the server being added in the /etc/sudoers.d file. If you uncheck this option, the commands will be added directly to the sudoers file. However, some organizations control how and by whom the sudoers file is updated. If this is the case, you can add the stanza to the sudoers file yourself. Add the Managed Server. In the Install log that is generated will be the stanza that needs to be added to the sudoers file. As part of adding the stanza to the sudoers file, be sure to change the host name to the server you're adding. Once that stanza is added (with the current host server name), run the Add Managed Server again. Security Auditor will detect that the commands have already been added and the install will complete successfully.

Option 4: If you would like to authenticate with the server using an SSH key for installation purposes, you can do so by specifying a private key. You might choose this option if you are installing on a cloud server instance (e.g. Amazon Web Services (AWS)). To do so:

1. Identify the private key used to communicate with the server. (This key is generally only available when the key pair is created.) If the same key is used for multiple servers, you may want to save a managed key in Security Auditor's Manage Private Keys screen for easy access.
2. When adding the server, in the Installation Authentication section of the Add a New Server or Add Multiple Servers screen, select one of the three Private Key options. Choose 'Private key (Copy/Paste)' to paste the key, choose 'Private key .pem file' to select a .pem file containing the key, or Managed Private Key to select a key you have loaded into Security Auditor's Manage Private Keys database.

5. When you click **Save** or **Save and exit**, a one-time SSH connection is made to the server that will configure the server based on the Installation Configuration. Installation will create the user and group specified, and create a different public/private key pair allowing the Security Auditor console SSH access as that user (e.g. the user policym will be created on the server you are adding). If using a Password, the initial connection does NOT have to be as root; however, it must have sufficient rights to modify the sudoers file on the server being added. If you use an SSH key for installation, the key is not used again or recorded by Security Auditor (unless it had been saved in Manage Private Keys).

Adding Multiple Servers

If you have many servers to manage you can add them quickly using the Add Multiple Servers screen.

1. Choose **Servers > Add Multiple Servers**. The Add Multiple Servers screen appears.
2. Specify the Server Type. All servers added must be of the same platform.
3. Specify the Server Names. You can specify the server names individually, separated by a semicolon or line feed. Names can be a server and DNS name (`MyServer` or `192.168.1.1`), or a server@DNS name combination (`MyServer@192.168.1.1` or `MyServer@DNSName.com`).

EXAMPLE:

```
Server1; Server2; 192.168.1.1; MyServer@MyDNSName.com
```

or

```
Server1
Server2
Server3
192.168.1.1
MyServer@MyDNSName.com
```

To expedite the process, tell Security Auditor to identify servers on your network using dynamic naming. For example, `Server[1-100]` will identify all servers named "Server" followed by an integer from 1-100 (e.g. `Server1; Server2; Server29; Server99`). `Server[001-100]` will identify servers similarly, but using the leading zeros (e.g. `Server001; Server002; Server029; Server099`). The syntax `Server[a,b,c,x,z]`, `Server[10,15-20, 35]`, and `MyServer@192.168.1.[1-10]` are also valid.

> **EXAMPLE:**
> `Server[1-400]; Server[001-400]; Server[a,b,c], Server[10-67]`

You can add the same server to Security Auditor more than once by specifying multiple names for the same IP address or DNS name.

> **EXAMPLE:**
> `MyAccountingServer1@192.168.1.1, MyAccountingServer2@192.168.1.1`

4. Use the available variables ({name}, {nameoripaddress}, {servertype}) to identify the desired Description.

   > **EXAMPLE:**
   > `Server: {name} DNSName: {nameoripaddress} ServerType: {servertype}`
   > Could yield
   > `Server: MyAccountingServer1 DNSName: 192.168.1.1 ServerType: AIX`

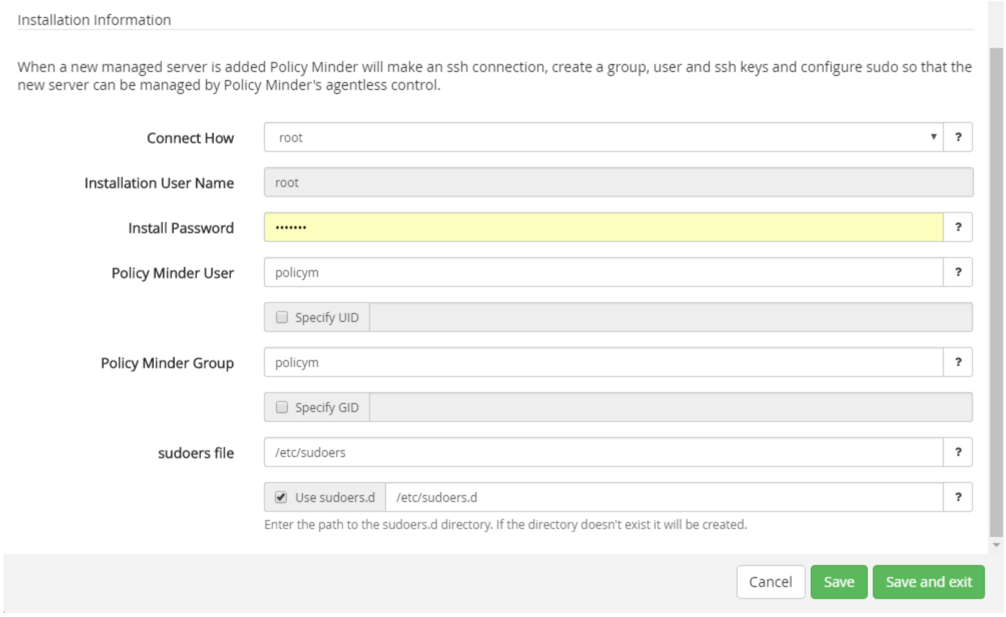
5. For Group, you can select an existing group, or check **New Group** to create a new one. See Server Groups.

   > **NOTE:** When adding a new Group, if it should include a Shared Policy, check **New Group shares policy**. See Policy Overview for details. Also note that if you check 'New Group' and the Group already exists, Security Auditor will add the servers to the existing Group.

6. Specify the Installation Information:

   Options when adding a non-Windows server

   Option 1: If you take the default settings, you will need to provide root's password to make the initial connection. When the connection is made, the Security Auditor User policym and the Security Auditor Group policym will be created and the sudoer's file updated to provide the user policym with the ability to run the commands needed for the Security Auditor product. Subsequent connections are made via SSH and use certificates, not user / password to establish the connection.



Installation Information

When a new managed server is added Policy Minder will make an ssh connection, create a group, user and ssh keys and configure sudo so that the new server can be managed by Policy Minder's agentless control.

Connect How	root
Installation User Name	root
Install Password	•••••••
Policy Minder User	policym
	□ Specify UID
Policy Minder Group	policym
	□ Specify GID
sudoers file	/etc/sudoers
	☑ Use sudoers.d /etc/sudoers.d

Enter the path to the sudoers.d directory. If the directory doesn't exist it will be created.

Alternative to Option 1: Some organizations do not allow root to make an SSH connection. In this case you can use su. Use the drop down box for Connect How and choose su. You will be prompted to enter root's password (so you can use SU on the server you're adding). You must also specify a user and password to make the initial connection. This user MUST be able to SU to root.

Another alternative to Option 1: Ubuntu doesn't have the concept of root so when adding an Ubuntu server, use the option to connect with sudo. To choose this option, use the drop down box for Connect How and choose sudo. The user specified in the Installation User Name field must be a user who can execute admin commands using sudo.

Option 2: By default a user and a group named policym will be created on each server. You may want to create a user and/or group by a different name than policym. Or you may want to specify the UID or GID for the user/group. To do so, name the user, group, and specify a UID and GID.

> **NOTE:** If the user or group do not already exist, they will be created with the UID / GID specified (if any).)

Option 3: By default, the commands required by Security Auditor will be added on the server being added in the /etc/sudoers.d file. If you uncheck this option, the commands will be added directly to the sudoers file. However, some organizations control how and by whom the sudoers file is updated. If this is the case, you can add the stanza to the sudoers file yourself. Add the Managed Server. In the Install log that is generated will be the stanza that needs to be added to the sudoers file. As part of adding the stanza to the sudoers file, be sure to change the host name to the server you're adding. Once that stanza is added (with the current host server name), run the Add Managed Server again. Security Auditor will detect that the commands have already been added and the install will complete successfully.

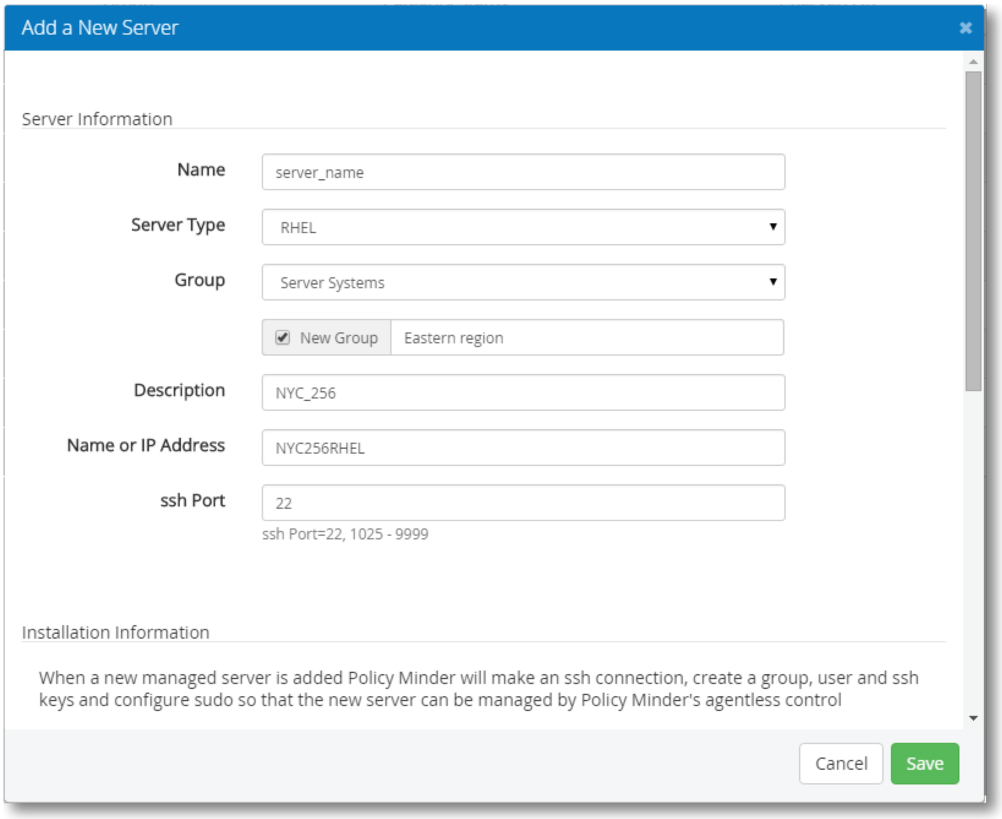
Option 4: If you would like to authenticate with the server using an SSH key for installation purposes, you can do so by specifying a private key. You might choose this option if you are installing on a cloud server instance (e.g. Amazon Web Services (AWS)). To do so:

   1. Identify the private key used to communicate with the server. (This key is generally only available when the key pair is created.) If the same key is used for multiple servers, you may want to save a managed key in Security Auditor's Manage Private Keys screen for easy access.
   2. When adding the server, in the Installation Authentication section of the Add a New Server or Add Multiple Servers screen, select one of the three Private Key options. Choose 'Private key (Copy/Paste)' to paste the key, choose 'Private key .pem file' to select a .pem file containing the key, or Managed Private Key to select a key you have loaded into Security Auditor's Manage Private Keys database.
7. When you click **Save** or **Save and exit**, a one-time SSH connection is made to the server that will configure the server based on the Installation Configuration. Installation will create the user and group specified, and create a different public/private key pair allowing the Security Auditor console SSH access as that user (e.g. the user saadmin will be created on the server you are adding). If using a Password, the initial connection does NOT have to be as root; however, it must have sufficient rights to modify the sudoers file on the server being added. If you use an SSH key for installation, the key is not used again or recorded by Security Auditor (unless it had been saved in Manage Private Keys).

Server Groups

You can create Server Groups to organize your servers for easier management, and in order to apply policies to multiple servers at once. You can create a new group when adding a new server. If you do nothing, all servers will be in the default group – Server Systems.

All servers in a Server Group must share the same operating system.



Add a New Server

Server Information

Name	server_name
Server Type	RHEL
Group	Server Systems
	☑ New Group · Eastern region
Description	NYC_256
Name or IP Address	NYC256RHEL
ssh Port	22

ssh Port=22, 1025 - 9999

Installation Information

When a new managed server is added Policy Minder will make an ssh connection, create a group, user and ssh keys and configure sudo so that the new server can be managed by Policy Minder's agentless control

Adding, Monitoring, and Managing Cloud Services

Security Auditor can check Security Policies on server instances of the Amazon Web Services (AWS) EC2 cloud service. These servers can be added individually or en masse just like servers on your local network, as described in Adding Servers to Manage. However, businesses often start new EC2 instances regularly, and manually adding a new Managed Server in Security Auditor for each new server instance can be time consuming.

Fortunately, Security Auditor can monitor your cloud service and use filters to automatically discover new server instances and map them to new Managed Servers, where they can be checked against an existing Group Policy. This process, called *polling*, allows Security Auditor to respond to deployment of new cloud server instances without any intervention from an administrator. (Servers that have been deleted from AWS can also be removed from Security Auditor automatically.)

The following instructions describe how to add a new cloud service, and begin monitoring and managing cloud server instances.

Adding a Cloud Service Account

1. Choose **AWS Accounts > Manage AWS Accounts**. The Manage AWS Cloud Service Accounts screen appears.
2. Click **Add** to open the Add AWS Cloud Service Account screen.
3. Add the requested information:
   - Enter a name (required) and description (optional) for the account.
   - The Type of account is currently limited to Amazon Web Services Elastic Compute Cloud.
   - Check Enable Discovery Polling if you would like to use filters to automatically discover and add server instances deployed by the service.
   - Enter your AWS Access Key ID and Secret Access Key.

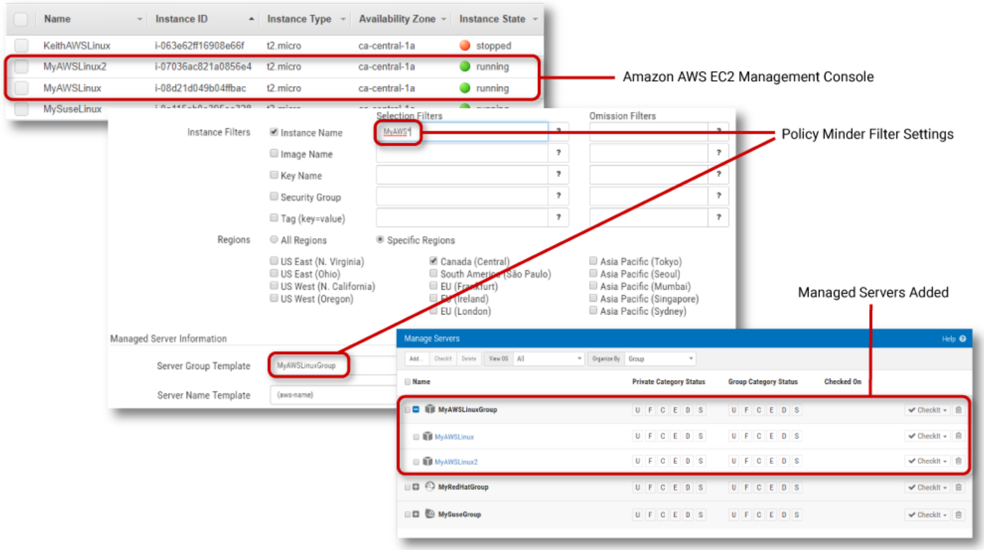
     > **NOTE:**
     > Amazon recommends against creating access keys for your AWS account and that you delete any that exist. Instead, create a user in AWS Identity and Access Management (IAM) and choose Programmatic access to create an access key for the user. For more information, see Lock away your AWS account root user access keys in the *IAM User Guide*.
     >
     > Credentials for a user with “AmazonEC2ReadOnlyAccess” policy at a minimum are required for accessing instance information in an Amazon AWS Account. The policy can be given to the user through Group membership, or it can be directly assigned to the user. There is also a “SecurityAudit” policy that includes “AmazonEC2ReadOnlyAccess” that can be used as a helpful alternative for users that have additional auditing requirements.
4. Click **Save**.

Defining and Validating Filters

In order to monitor for server instances, Security Auditor requires information about your cloud service account, which servers it should discover, and in which Groups the discovered servers' Managed Server definitions belong. Use the following general steps to configure Security Auditor's filters.

1. Choose **AWS Accounts > Manage AWS Accounts**. The Manage AWS Cloud Service Accounts screen appears.
2. Click **(Edit Filters)** for an existing cloud service account. The Manage Filters screen appears.
3. Click **New** to create a new filter definition. Note that multiple filters can be defined for the same cloud service account.
   a. Enter a name and description for the filter.
   b. Check the Instance Filters fields you wish to use and specify text and/or variables in those fields to indicate the server instances to discover. See Add Filter screen for more details regarding these fields.

   > **NOTE:** You can use the ? icons adjacent to the entry fields to identify the available variables.



Name	Instance ID	Instance Type	Availability Zone	Instance State
KeithAWSLinux	i-063e62ff16908e66f	t2.micro	ca-central-1a	stopped
MyAWSLinux2	i-07036ac821a0856e4	t2.micro	ca-central-1a	running
MyAWSLinux	i-08d21d049b04ffbac	t2.micro	ca-central-1a	running
MySuseLinux	[illegible]	[illegible]	[illegible]	[illegible]

Instance Filters — Selection Filters: ☑ Instance Name: MyAWS*; ☐ Image Name; ☐ Key Name; ☐ Security Group; ☐ Tag (key=value). Omission Filters: empty.

Regions: ○ All Regions ● Specific Regions

☐ US East (N. Virginia)
☐ US East (Ohio)
☐ US West (N. California)
☐ US West (Oregon)
☑ Canada (Central)
☐ South America (São Paulo)
☐ EU (Frankfurt)
☐ EU (Ireland)
☐ EU (London)
☐ Asia Pacific (Tokyo)
☐ Asia Pacific (Seoul)
☐ Asia Pacific (Mumbai)
☐ Asia Pacific (Singapore)
☐ Asia Pacific (Sydney)

Managed Server Information

Server Group Template: MyAWSLinuxGroup

Server Name Template: (aws-name)

Manage Servers — View OS: All; Organize By: Group

Name	Private Category Status	Group Category Status	Checked On
MyAWSLinuxGroup	U F C E D S	U F C E D S	
MyAWSLinux	U F C E D S	U F C E D S	
MyAWSLinux2	U F C E D S	U F C E D S	
MyRedHatGroup	U F C E D S	U F C E D S	
MySuseGroup	U F C E D S	U F C E D S	

   c. For Regions, choose All Regions to search your AWS account for server instances in all regions. Choose Specific Regions to identify the regions to be searched. Choose the minimum number of required regions for optimal performance.
   d. Enter the Managed Server Information. See Managed Server Information for a list of the available variables.
      - For Server Group Template, specify the Server Group discovered servers will be assigned to. All server instances discovered by this filter will be placed into one or more Groups. Servers that share a policy should be assigned to the same Group. Remember that only servers of the same Linux distribution can exist in any one Group. See Manage Servers screen for more details on Server Groups.

- For Server Name Template, specify how Security Auditor should name discovered server instances. Each server name must be unique.
- For Server Description Template, specify how the discovered server instances should be described.
- For Server IP Address/Name, specify whether you want to use a public or private IP address/DNS name.

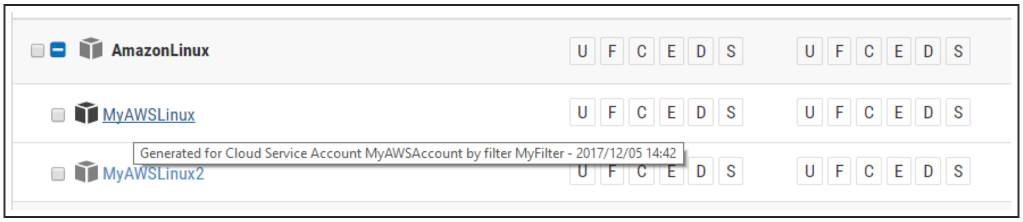
e. Enter the Installation Connection Information and Installation Configuration. See Installation Connection Information and Installation Configuration.

> **NOTE:**
> For Authenticate With, you can choose a Managed Key. See Manage Private Key screen for details.

4. Click **Save** to save your filter settings. You return to the Manage Filters screen.
5. Click ✓ **(Validate Filter)** next to the filter you have just defined to run the Filter. The results appear in the Validate Filter screen.
6. Click **Accept** to accept the results and begin polling (if polling is enabled). The Validate Filter button changes to View Filter ✓. You can click this button to view the Validate Filter screen with the list of server instances.

> **NOTE:** Polling is activated in the Cloud Services tab of the Preferences screen.

Click **Managed Servers** to return to the Managed Servers screen where you can review your servers and policies. Roll over a server instance with your mouse cursor to view more details.



AmazonLinux

MyAWSLinux

Generated for Cloud Service Account MyAWSAccount by filter MyFilter - 2017/12/05 14:42

MyAWSLinux2

Policy Overview

Group Policies and Private Policies

Security Auditor can check for compliance of many servers against a common Group Policy, or check for compliance of individual servers against their own Private Policies.

Each server can be checked against a Private Policy, a Group Policy, or both. For example, a Group Policy can be used for general settings that should be the same for all servers in the Group, then Private Policies can be defined for individual servers within the Group with more specific compliance standards that do not apply to other servers in the Group.

Group Policies

A *Group Policy* is a policy intended for comparison against all servers in a Server Group. Compliance with a Group Policy can be checked for individual servers in a Group, or for all servers in the Group at once.

> **NOTE:** To enable Shared Policies for a Group, the 'New Group shares policy' option must be checked when adding the group. See Add a New Server screen.

User Accounts, Files, and Scripts policy categories can be added and defined manually. Configuration, Exported Directories, and Daemons categories must be initialized for a server first. The initialization settings for that server become the compliance standard for the Group Policy.

To create a Group Policy for the User Accounts, Files, or Scripts Categories

1. Add servers to the desired Server Group (as they are added to Security Auditor).
2. Choose **Servers and Policies > Server Group** or **Servers and Policies > Server**. The Servers and Policies screen appears.
3. For Policy, choose **Group**.
4. Select the desired category (e.g. User Accounts).
5. Click **New**. You are prompted to define a Policy Template. See User Accounts, Daemons, and Scripts for details on defining Policies in these categories.

> **NOTE:** The operating system for all servers in a Group must be the same. Groups that share Configuration and/or Daemon policies should only include servers of the same OS *version*.

See To Initialize Group Policies below for information on creating Group Policies for Configuration, Exported Directories, and Daemons categories.

Private Policies

A *Private Policy* is a policy intended for a single server. While servers with Private Policies can be grouped together, and checked as a group, their compliance status is always a reflection of a comparison with their Private Policy.

To create a Private Policy for the User Accounts, Files, or Scripts Categories

1. Add the server to Security Auditor. It can be assigned to any Group, or the Default Group.
2. Choose **Servers and Policies > Server**. The Servers and Policies screen appears.
3. For Policy, choose **Private**.
4. Select the desired category (e.g. User Accounts).
5. Click **New**. You are prompted to define a Policy Template. See User Accounts, Daemons, and Scripts for details on defining Policies in these categories.

See To Initialize Private Policies below for information on creating Private Policies for Configuration, Exported Directories, and Daemons categories.

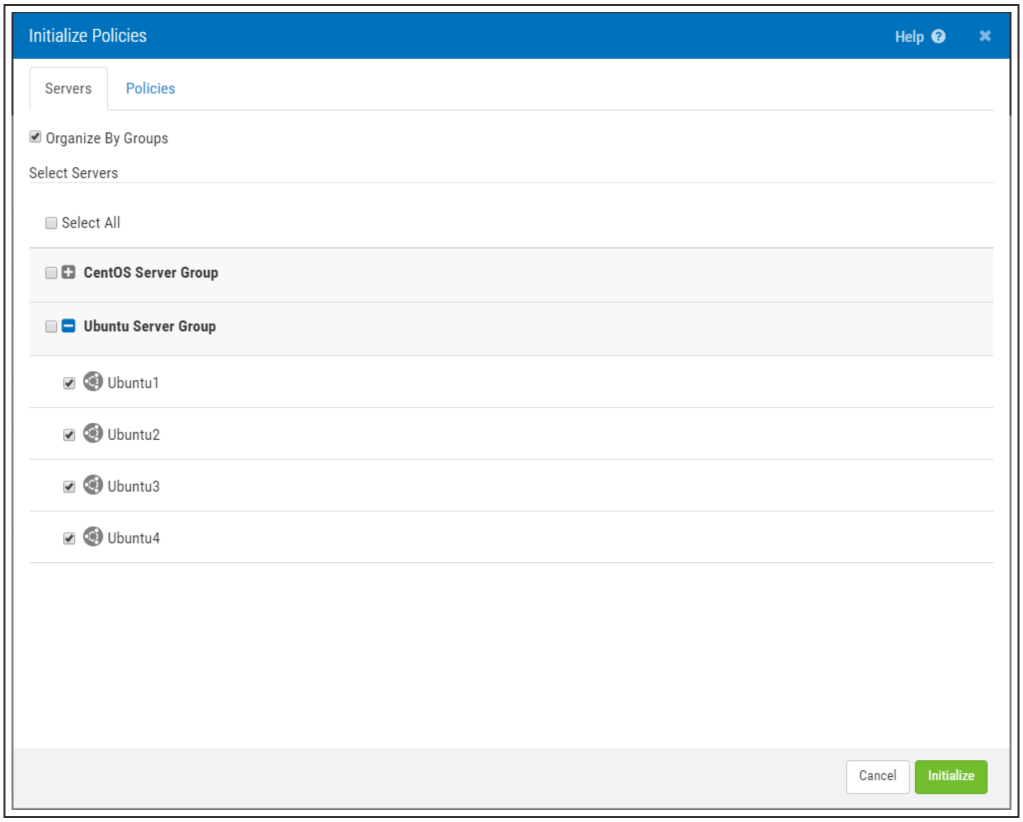
Initializing Policies

One quick way to get started using Security Auditor is to initialize your policies. When you initialize a category, Security Auditor retrieves the current settings for the category (or categories - Configuration, Exported Directories, and/or Scripts), and establishes that as the baseline policy for that category. The Private Policies for any number of servers can be initialized at the same time.

When you initialize a category for a Group Policy, on the other hand, Security Auditor retrieves the current settings *for a single server*, and establishes that as the baseline policy for that category for all servers in the Group.

To Initialize Private Policies for One or More Servers

1. Click on **Console Tasks > Initialize Policies**. The Initialize Policies screen appears. On the Servers tab, select one or more servers.



☑ Organize By Groups

Select Servers

□ Select All

□ CentOS Server Group

□ Ubuntu Server Group

☑ Ubuntu1

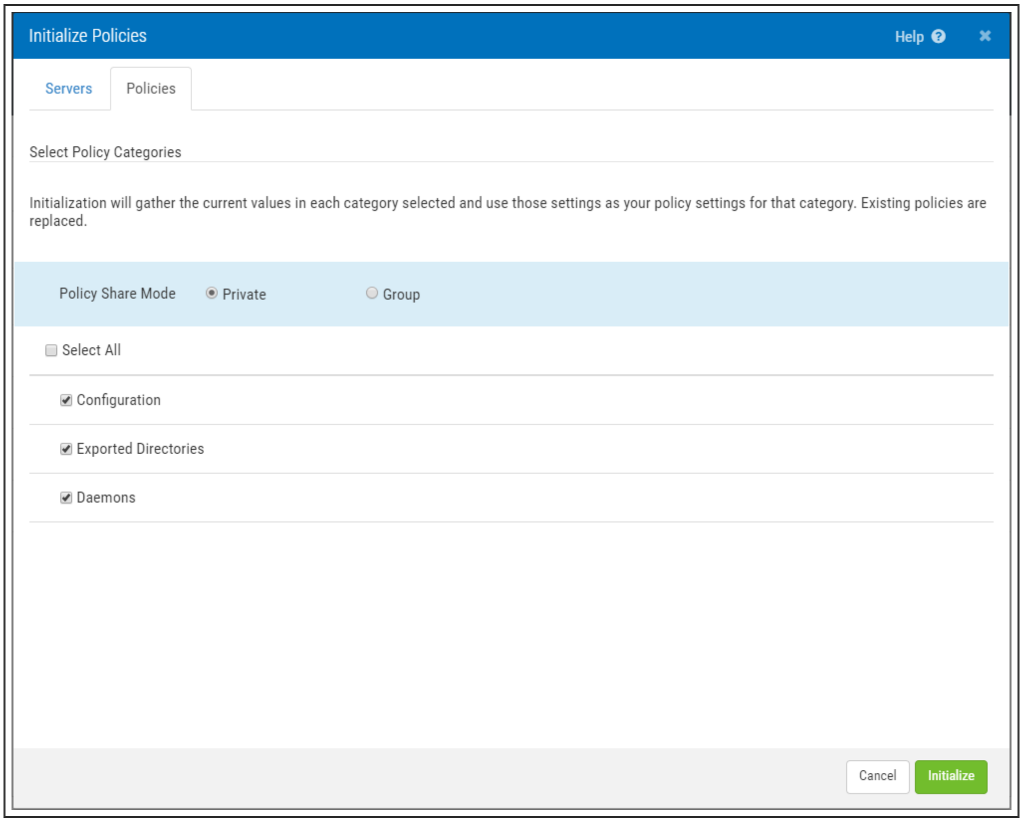
☑ Ubuntu2

☑ Ubuntu3

☑ Ubuntu4

2. Click the **Policies** tab.
3. For Policy Share Mode, choose **Private**.

4. Select the Categories to be initialized.



Select Policy Categories

Initialization will gather the current values in each category selected and use those settings as your policy settings for that category. Existing policies are replaced.

Policy Share Mode ● Private ○ Group

□ Select All

☑ Configuration

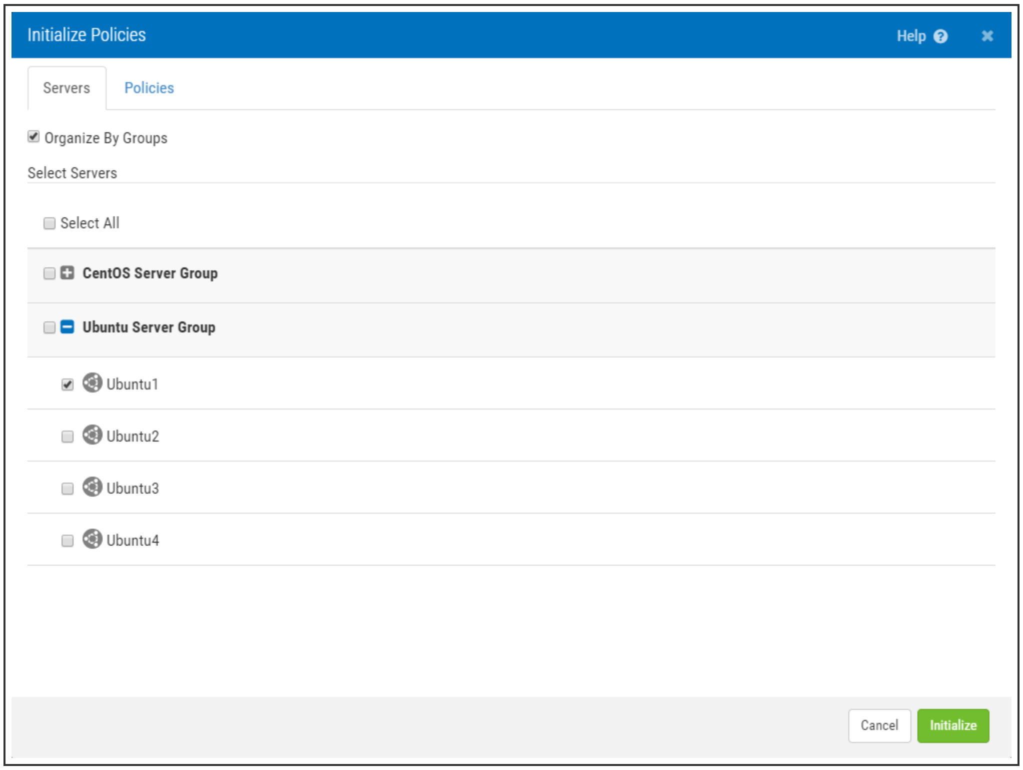
☑ Exported Directories

☑ Daemons

5. Click **Initialize**.

To Initialize Policies for a Group

1. Click on **Console Tasks > Initialize Policies**. The Initialize Policies screen appears. On the Servers tab, select the server whose settings you would like to use for the Policy standard. (Only one Group can be initialized at a time.)



☑ Organize By Groups

Select Servers

□ Select All

□ CentOS Server Group

□ Ubuntu Server Group

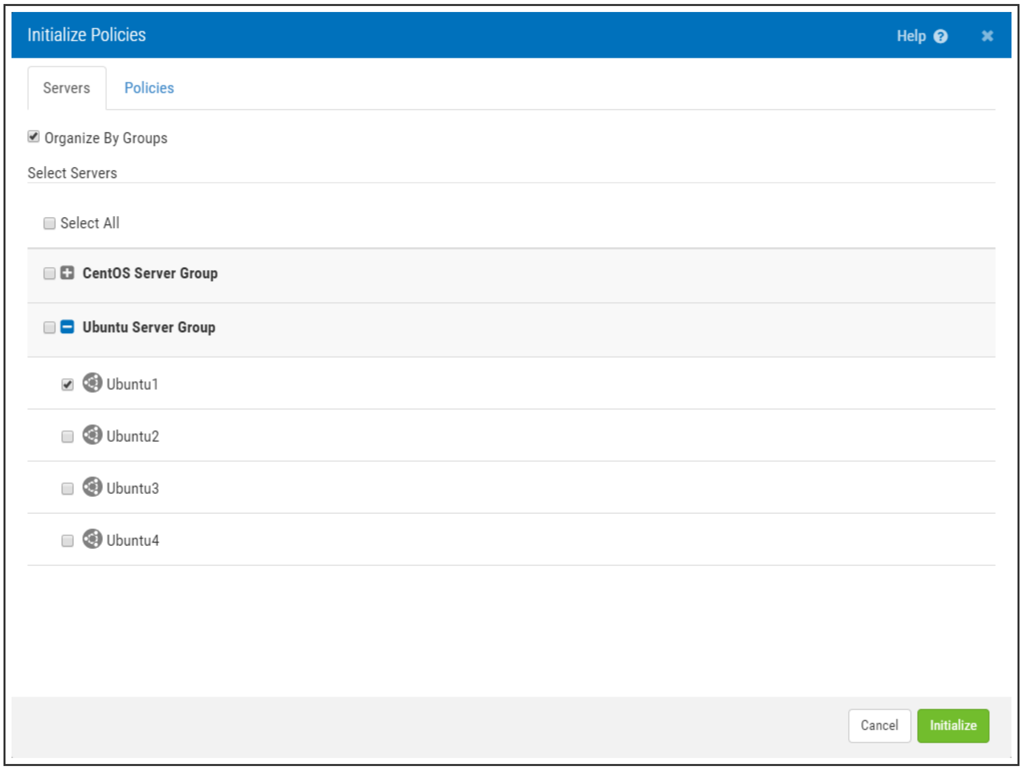
☑ Ubuntu1

□ Ubuntu2

□ Ubuntu3

□ Ubuntu4

2. Click the **Policies** tab.
3. For Policy Share Mode, choose **Group**.
4. Select the Category to be initialized.



☑ Organize By Groups

Select Servers

□ Select All

□ CentOS Server Group

□ Ubuntu Server Group

☑ Ubuntu1

□ Ubuntu2

□ Ubuntu3

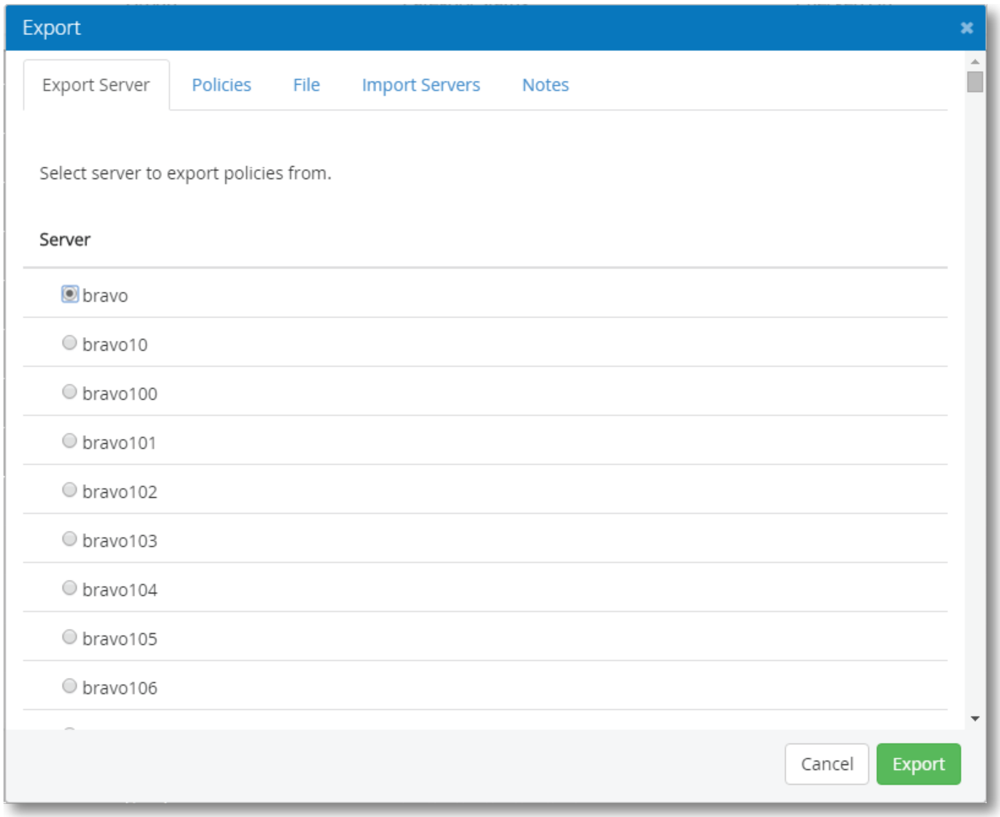
□ Ubuntu4

5. Click **Initialize**.

Copying Policies to Another Server and using the Export / Import Feature

Once you have defined policies on one of your servers, you can use the export/import function to copy the policies from one server to another. You might want to use this feature when configuring/setting up a server ensuring the settings are the set properly on the new server, to propagate user account policies to all servers to ensure consistent policy compliance, to ensure settings on QA servers are consistent with production, etc.

Before you can copy a policy to another server, you must first Export it. Go to **Console tasks > Export**. You'll see the following dialog:



Export

Select server to export policies from.

Server
● bravo
○ bravo10
○ bravo100
○ bravo101
○ bravo102
○ bravo103
○ bravo104
○ bravo105
○ bravo106

Do the following:

1. On the Servers tab specify which server you are exporting from (you can only specify one server.)
2. On the Policies tab specify whether it is a Private or Group Policy, then select the policies you want to export.
3. On the Destinations tab, specify the servers you want to import (or copy) policies to.

> **NOTE:** Exporting a file provides the option to create an .xml file of the exported policies. If the server you are importing (copying policies) to is managed by this console, you can simply choose the option to copy the policy to the server(s) and avoid having to import via the exported file.

Replace Template Options

- By default, policies defined on the target system are over-laid if they also exist on the server to which they are being imported.
- When specifying Replace and a template exists on the target system with the same name as a template on the master system, the master system template will be imported and will have a number added to the end of the name.

Importing Policies

You may want to import a policy file from another console or one that you have acquired elsewhere.

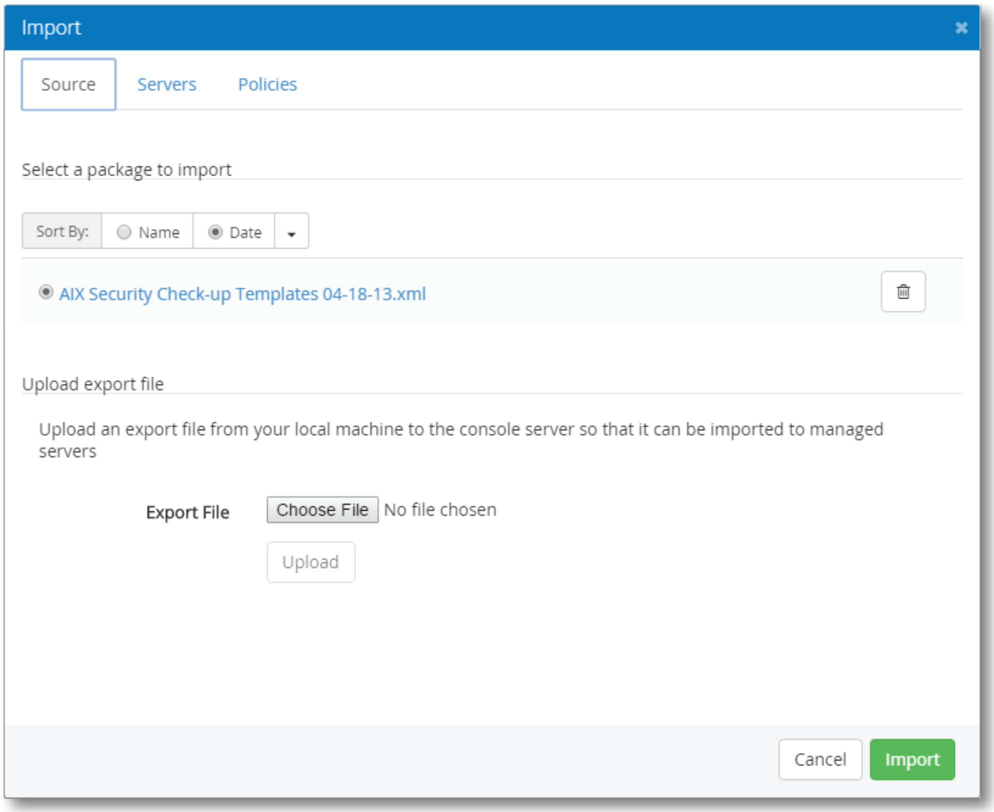
To import a policy file, go to **Console tasks > Import**:

- For consoles running on Windows you can Browse to find the policy file and upload it.
- For consoles running on AIX or Linux, place the .xml file in the following directory (where Security Auditor was installed).

.../Powertech/SecurityAuditor/tomcat/webapps/securityauditor/exports

(this also works for Windows consoles)

Once you have uploaded the policy file or placed it in the proper directory, it will be listed as one of the files available to be imported. In the example below, the AIX Security Check-up file is available for import.


Import

Source | Servers | Policies

Select a package to import

Sort By: ○ Name ● Date

● AIX Security Check-up Templates 04-18-13.xml

Upload export file

Upload an export file from your local machine to the console server so that it can be imported to managed servers

Export File: No file chosen

The next chapters will explain how to define policies and templates as well as what to expect when and using the CheckIt and FixIt functions.

Managing S3 Bucket Policies

Security Auditor allows you to monitor your AWS S3 bucket settings across many buckets at once using a *Shared Bucket Policy*, with exceptions to Shared Bucket Policy settings specified for individual Buckets using *Private Bucket Policies* (For brevity, these are also referred to as simply *Shared Policies* and *Private Policies*).

For information on setting up a new AWS account with Security Auditor, see Adding, Monitoring, and Managing Cloud Service Accounts.

Enabling S3 Bucket Policies

1. Choose **AWS Accounts** > **Manage AWS Accounts**. The Manage AWS Cloud Service Accounts screen appears.
2. Click the name of an AWS account to open the Modify AWS Cloud Service Account screen. Or, click **Add** to add an account.
3. Under AWS S3 Policy, check **Enable AWS S3 Policy**. Here, you can specify whether to allow new or deleted buckets in your policy, and specify a Shared Bucket Policy. Security Auditor includes the *DEFAULT policy, which is configured to match the AWS S3 default settings.
4. Click **Save**.

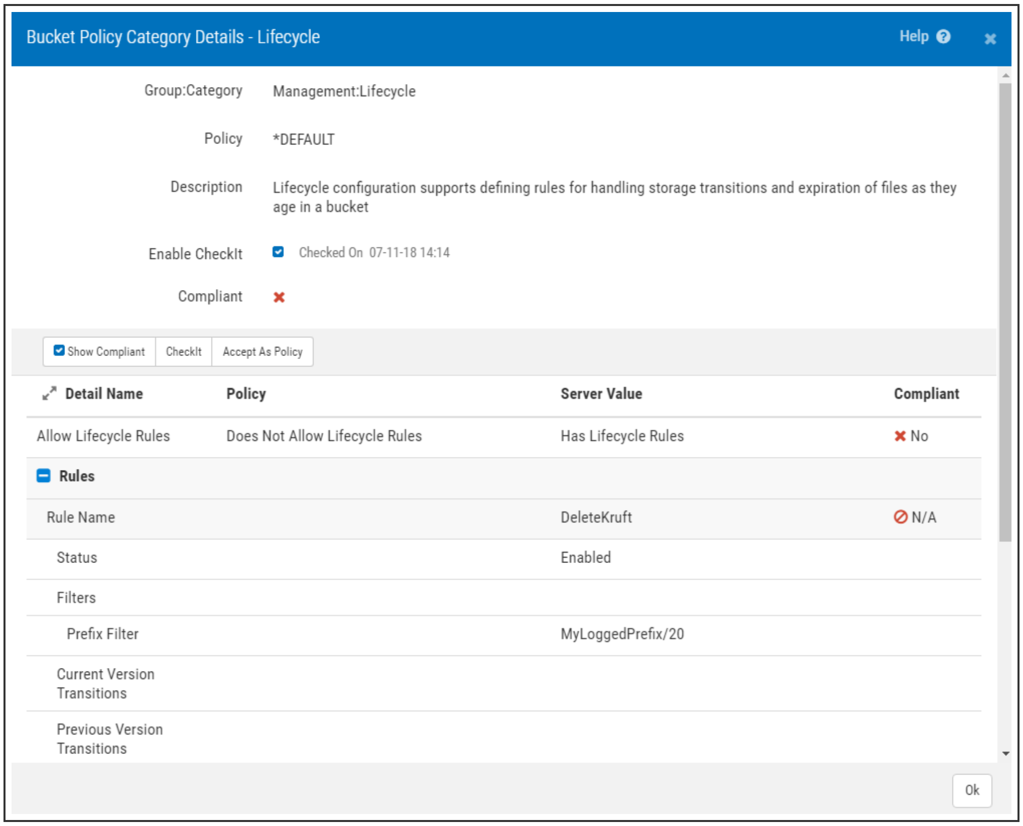
> **NOTE:** To add a new Shared Bucket Policy, choose **AWS Accounts** > **Manage Shared Bucket Policy** and click **Add**. The Add Shared Bucket Policy screen appears, where you can create a Shared Bucket Policy.

Managing S3 Bucket Policies

1. Choose **AWS Accounts** > **Manage AWS Accounts** to open the Manage AWS Cloud Service Accounts screen.
2. Click ✓ for an account. If an AWS S3 policy has been enabled, and Security Auditor finds Buckets in the account, B appears for the account under the Policy column.

   > **NOTE:** The color of the "B" button depends on the status of the Buckets in the account.
   >
   > B = Not Checked
   >
   > B = Not Compliant
   >
   > B = Compliant

3. Click B to open the Manage Service Buckets screen. This screen lists each bucket in the AWS account, along with its status: Not checked ✱, Not Compliant ✖ , or Compliant ✔. Here, you can:
   - Click ✓ to run CheckIt to check for compliance.
   - Click 👍 to accept the non-compliant values as part of the Policy. Accepted values are marked with an * (asterisk) in the Bucket Policy Categories screen to indicate they are overridden by a Private Policy.
   - Click ● to enable/disable CheckIt for the Bucket.
4. Click a Bucket Name to open the Bucket Policy Categories screen for that Bucket. This screen lists the Bucket Policy Categories for the account, along with their status: Not checked ✱, Not Compliant ✖ , or Compliant ✔. Categories marked with an * (asterisk) are overridden with a Private Policy. Here, you can:
   - Click ● to enable/disable CheckIt for the Bucket.
   - Click 👍 to accept the non-compliant values as part of the Policy. Accepted values are marked with an * (asterisk) in the Bucket Policy Categories screen to indicate they are overridden by a Private Policy.
   - Click ✓ to run CheckIt to check the Category for compliance.
   - Click ↺ to revert back to the Shared Policy.
5. Click a non-compliant Category to open the Bucket Policy Category Details screen where you can identify more details about the non-compliant values. In the following example, the policy does not allow Lifecycle Rules, but the server has Lifecycle Rules.
6. You can click ⊞ Rules to expand the details list, which shows the specific non-compliant server values.



Bucket Policy Category Details - Lifecycle

Group:Category: Management:Lifecycle

Policy: *DEFAULT

Description: Lifecycle configuration supports defining rules for handling storage transitions and expiration of files as they age in a bucket

Enable CheckIt: ☑ Checked On 07-11-18 14:14

Compliant: ✗

Detail Name	Policy	Server Value	Compliant
Allow Lifecycle Rules	Does Not Allow Lifecycle Rules	Has Lifecycle Rules	✗ No
Rules			
Rule Name		DeleteKruft	⊘ N/A
Status		Enabled	
Filters			
Prefix Filter		MyLoggedPrefix/20	
Current Version Transitions			
Previous Version Transitions			

Using Security Auditor

Defining Policies, Running Compliance Checks, and Using FixIt

The previous chapter provided instructions for starting to use Security Auditor. This chapter describes each category in depth.

Configuration Values

Security Auditor allows you to define your policy for global configuration settings.

Initializing

Many administrators are comfortable with the current settings for these configuration settings and want to make sure that they remain set that way. The way to use Security Auditor to ensure they remain the same is to start by initializing the Security Auditor Configuration category.

1. Go to **Servers > Initialize Policies**.
2. Select the server or servers you would like to initialize for Private policies. To initialize a Group Policy, select a single server, which will be the Group Policy's benchmark for these categories (see Policy Overview for details).
3. Select the **Policies** tab.
4. Choose whether this is a Private or Group policy.
5. Choose the Configuration category.
6. Click **Initialize**.

Using the Configuration Category

If you are not familiar with all of the attributes listed in this category, simply click on the attribute name and a description will be displayed. You'll notice that for an AIX managed server, some attributes, such as the minlen attribute as defined in the User Account Creation – Password category have a value of "No Entry Policy." This means that, when a user account is created, there is no entry for minlen in the /etc/security/user file. (If there's an entry at the user level, it overrides (takes precedence over) the global value.) Instead, the value for minlen is to come from the minlen global setting. This value is defined in Security Auditor in the User Account Default – Password minlen attribute. The "No Entry Policy" is not applicable for this attribute since this is the global (highest level) attribute.

Running a compliance check

You may want to check all of the values listed in the Configuration category. Or, because only some of them are meaningful for your organization you only want to check a few. If this is the case, you can change the policy value to be "Any value". This means that it doesn't matter what the value is and it will never be checked during a compliance check or identified as out of compliance.

When a compliance check is run against the Configuration category, the values you specify for your policy will be compared against the actual value of the configuration item. The item will be in compliance if the actual value is the same as the value you have defined in the policy. If the actual setting is different than the value defined in the policy, the value will be flagged as "out of compliance".

To run a compliance check, do one of the following:

- On the Manage Servers screen, click ✓ CheckIt ▾ and choose whether you want to check the Private Policy, Group Policy, or both for the server (or Server Group).
- On the Servers and Policies screen, click ✓ for the Attribute under the Action column.
- On the Manage Servers screen, click C next to a server to open the server's Configuration policies. Check **Attribute** to select all Attributes and click **CheckIt** in the upper right. This will run a compliance check on all of the attributes in the Configuration category.
- Choose **Servers > CheckIt**. Choose the server(s) and then the category, then click **CheckIt**.
- Schedule a regular compliance check. Choose **Admin tasks > Manage Scheduled Jobs**.

Running FixIt

If an item is identified as Out of compliance (✖), you can have Security Auditor change the value to make it match the policy by running the Security Auditor FixIt function. By default, FixIt is not enabled. You must enable FixIt.

> **NOTE:** You must first run a compliance check to identify what is out of compliance before you can run FixIt.

Once a compliance check has been run and FixIt is enabled, do one of the following:

- On the Servers and Policies screen, click 🔧 for the setting under the Action column.
- Check the individual item or all items and then click FixIt and choose **Servers > FixIt**. Choose the server and then the category, then click FixIt
- Schedule a regular compliance check and FixIt. Choose **Admin Tasks > Manage Scheduled Jobs**.

> **NOTE:** FixIt cannot be used for all AIX configuration settings. Obviously, prior to using FixIt, all changes should be reviewed carefully; however, some settings seemed as those they had significant chance of causing disruption if changed. Therefore, these values cannot be changed through FixIt:

- auth_type
- pwd_algorithm
- auth1
- auth2
- SYSTEM
- default_roles
- roles
- auditclasses
- dictionlist
- pwdchecks

- account_locked
- rlogin

These settings are also noted in the Configuration category with an ‘*’. These items will be identified as out of compliance but FixIt will not modify their values.

Daemons

Security Auditor allows you to define your policy for daemons regardless of whether they should be required to be running, restricted from running, or whether it doesn't matter whether they are running or not.

Initializing

Initializing this category will result in a list of the daemons currently on the server.

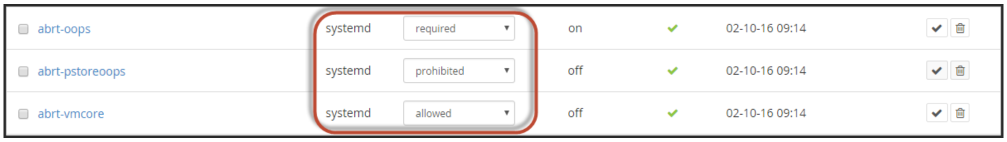
To initialize the Security Auditor Daemon category:

1. Go to **Servers > Initialize Policies**.
2. Select the server or servers you would like to initialize for Private policies. To initialize a shared policy, select a single server.
3. Select the **Policies** tab.
4. Choose whether this is a Private or Group policy.
5. Choose the Daemon category.
6. Click **Initialize**.

- Daemons currently running will be set to a policy value of **Required**.
- Daemons not running will be set to a policy value of **Prohibited**.

Using the Daemon category

Once initialized, you can alter the daemon settings to indicate whether they are Required (must be running), Prohibited (cannot be running) or Allowed (can be running or stopped.)



□ abrt-oops	systemd	required ▾	on	✓	02-10-16 09:14	✓ 🗑
□ abrt-pstoreoops	systemd	prohibited ▾	off	✓	02-10-16 09:14	✓ 🗑
□ abrt-vmcore	systemd	allowed ▾	off	✓	02-10-16 09:14	✓ 🗑

You can delete a daemon from the category. This does NOT delete the daemon from the server – only from the policy and subsequent compliance checks.

Running a compliance check

When a compliance check is run against the Daemon category, the values specified in the policy will be compared against the setting of the daemon on the server. The daemon will be in compliance if the server setting is the same as the Policy Value (or if the Policy Value is set to allowed). If the current setting is different than the value defined in the policy, the value will be flagged as "out of compliance."

To run a compliance check, do one of the following:

- On the Manage Servers screen, click ✓ CheckIt ▾ and choose whether you want to check the Private Policy, Group Policy, or both for the server (or Server Group).

- On the Manage Servers screen, click D next to a server to open the server's Daemon policies.
  - Click ✓ for the Daemon under the Action column. Or,
  - Select one or more Daemons and click **CheckIt**. This will run a compliance check on all the selected daemons in the Daemon category.
- Choose **Servers** > **CheckIt**. Choose the server from the Servers tab and then Daemons' from the Policies tab, then click **CheckIt**.
- Schedule a regular compliance check. Go to **Admin tasks** > **Manage Scheduled Jobs**.

Discovering new daemons

As mentioned earlier, you can remove a daemon from the category. Deleting a daemon does not remove it from the server. If you wish to include the daemon again or discover other daemons that may be running on the server, do the following:

- Run a compliance check on the category and resolve any compliance issues (if any).
- Go to **Servers** > **Initialize Policies** and initialize the policy for the Daemon category. This will bring in the daemons currently on the partition, including any daemons previous deleted from the category.

Running FixIt

If an item is identified as Out of compliance (✖), you can have Security Auditor change the value to make it match the policy by running the Security Auditor FixIt function. By default, FixIt is not enabled. You must enable FixIt.

> **NOTE:** You must first run a compliance check to identify what is out of compliance before you can run FixIt.
> FixIt will start or stop the daemon based on the setting defined in the policy. FixIt will not take any action on daemons whose setting is Allowed.

Once a compliance check has been run and FixIt is enabled, do one of the following:

- Check the individual daemon or all daemons and then click **FixIt**.
- Choose **Servers** > **FixIt**. Choose the server and then the category, then click **FixIt**.
- Schedule a regular compliance check and FixIt. Choose **Admin Tasks** > **Manage Scheduled Jobs**.

> **NOTE:** FixIt cannot be used for all daemons. Changing some daemons could be catastrophic; therefore, FixIt is not allowed for the following:

- biod
- cron
- ctrmc
- IBM AuditRM

- IBM.CSMAgentRM
- IBM.DMSRM
- IBM.DRM
- IBM.ERRM
- IBM.HostRm
- IBM.HWCTRLRM
- IBM.LPRM
- IBM.SensorRM
- IBM.ServiceRM
- inetd
- nfsd
- portmap
- qdaemon
- rpc.lockd
- rpc.statd
- sshd
- syslogd
- xntpd

These daemons will also be noted in the Daemons category with an ‘*’. These items will be identified as out of compliance but FixIt will not modify their values.

Exported Directories

Security Auditor allows you to define your policy for exported directories.

Initializing

Initializing this category will create a list of the exported directories on the server. To initialize the Security Auditor Exported Directories category, go to **Servers > Initialize Policies** and choose to initialize the Exported Directories category.

> **NOTE:** The initialize will read the exports file and compare it to what's configured on the server. It also looks for errant spaces and the setting of the no_root_squash flag. If you don't want this analysis performed on the exported directories, simply uncheck the appropriate box(es).

Running a compliance check

When a compliance check is run against the Exported Directories category, the values specified in the policy will be compared against the settings of each Exported Directory. The directory will be in compliance if the setting is the same as the value you have defined in the policy. If the settings are different than the values defined in the policy for the exported directories, the directory will be flagged as "out of compliance."

To run a compliance check, do one of the following:

- On the Manage Servers screen, click E next to a server to open the server's Exported Directories policies. Then click **CheckIt**. This will run a compliance check on all of the exported directories in the category.
- Choose **Servers > CheckIt**. Choose the server and then the category, then click **CheckIt**.
- Schedule a regular compliance check. Choose **Admin tasks > Manage Scheduled Jobs**.

Running FixIt

FixIt is not available for the Exported Directories category.

Defining Templates

The User Account and Files categories use templates to select what is going to be examined and the attributes to analyze.

Template Tips:

- When you define a template, the first tab allows you define what items – user accounts, directories or files you want to select to be examined when a compliance check is run on this template. You can include or omit items using specific or generic names. The Policies tab allows you to define the attributes that will be examined during a compliance check.

- You can specify a value for each attribute or you can leave the value as the default of ‘any’ value. ‘Any’ value means that it doesn’t matter what the value is, this particular attribute will always be in compliance. In other words, this attribute is ignored when a compliance check is run for the template.

User Accounts

Security Auditor supports User Account policies for AIX, Linux, and Windows servers.

What user account attributes need to be checked and the requirements for user profile compliance will vary from organization to organization. Some of the common user account templates we see configured are used to check for:

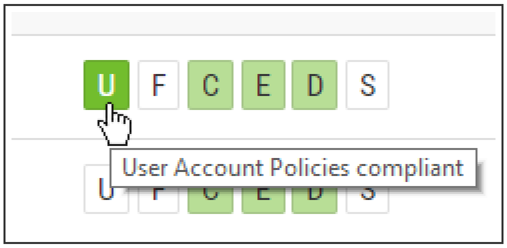
- New admin accounts
- Inactive accounts
- Members of a particular group to be configured with specific settings such as logon and audit settings.
- Accounts with UID of 0 (other than root)
- Multiple accounts with the same UID

Example – Detecting New Admin Accounts on AIX

The following steps are essentially the same regardless of the platform of the server being managed.

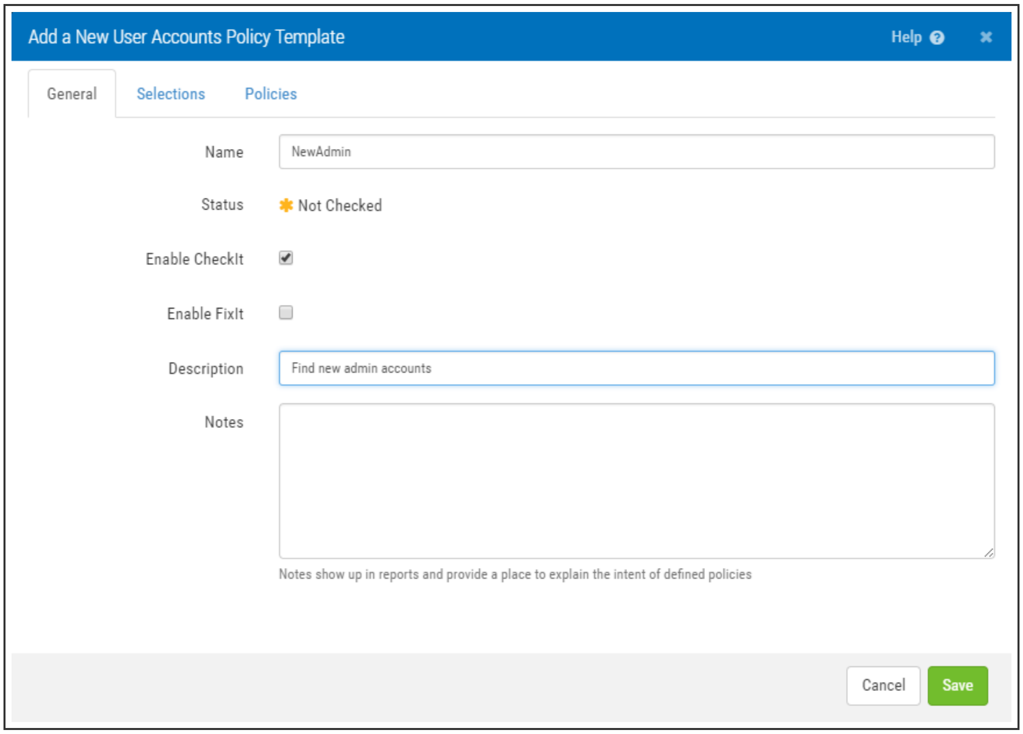
Defining the template

1. To get to the User Account category, on the Manage Servers screen, click the U category for the Private or Group Policy in the row of the desired server.



Or go to **Servers and Policies > [server name]**. In the drop-down lists, select whether this should be a Private or Group Policy, then select **User Accounts**.

2. Click **New**. The Add a New User Accounts Policy Template screen appears.
3. Fill out the General tab – example below.



Add a New User Accounts Policy Template

Name: NewAdmin

Status: ✱ Not Checked

Enable CheckIt ☑

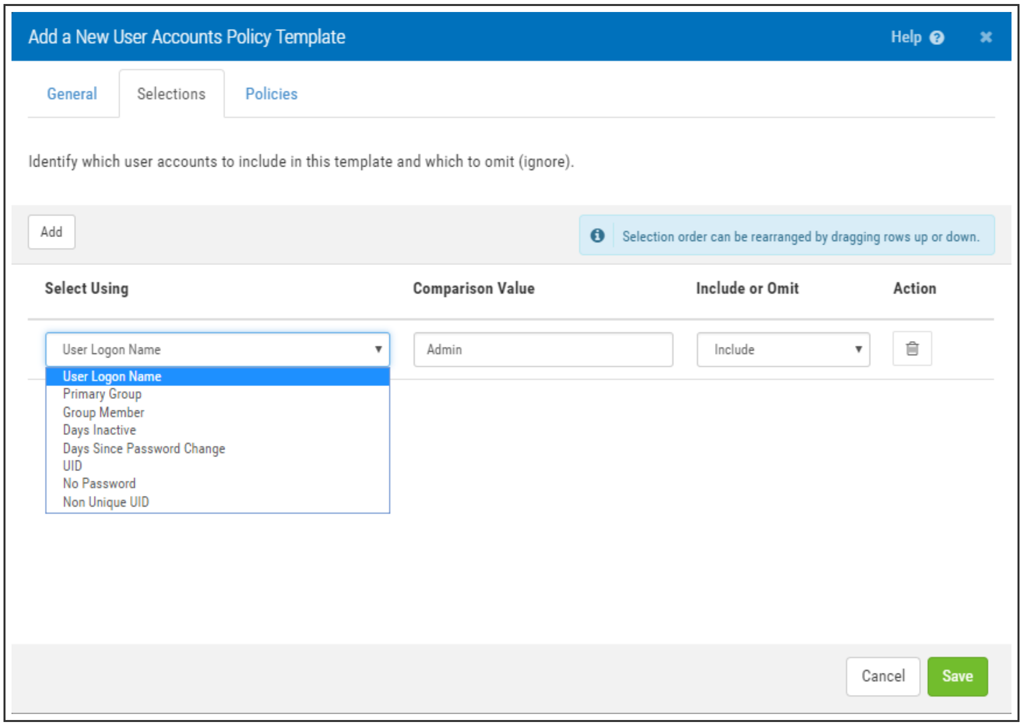
Enable FixIt ☐

Description: Find new admin accounts

Notes

Notes show up in reports and provide a place to explain the intent of defined policies

4. Click on the **Selections** tab, then click on **Add** to choose the user accounts that will be examined during a compliance check. For this example we're selecting Admin but you can select users based on, for example:
   - User account name (using the full name or a generic (as in bob*))
   - Accounts that have a specific primary group
   - Members of a specific group
   - Number of days the account has been inactive
   - Number of days since the last password change
   - UID (to check for accounts with UID of 0 – in addition to root, for example)
   - Non-unique UIDs



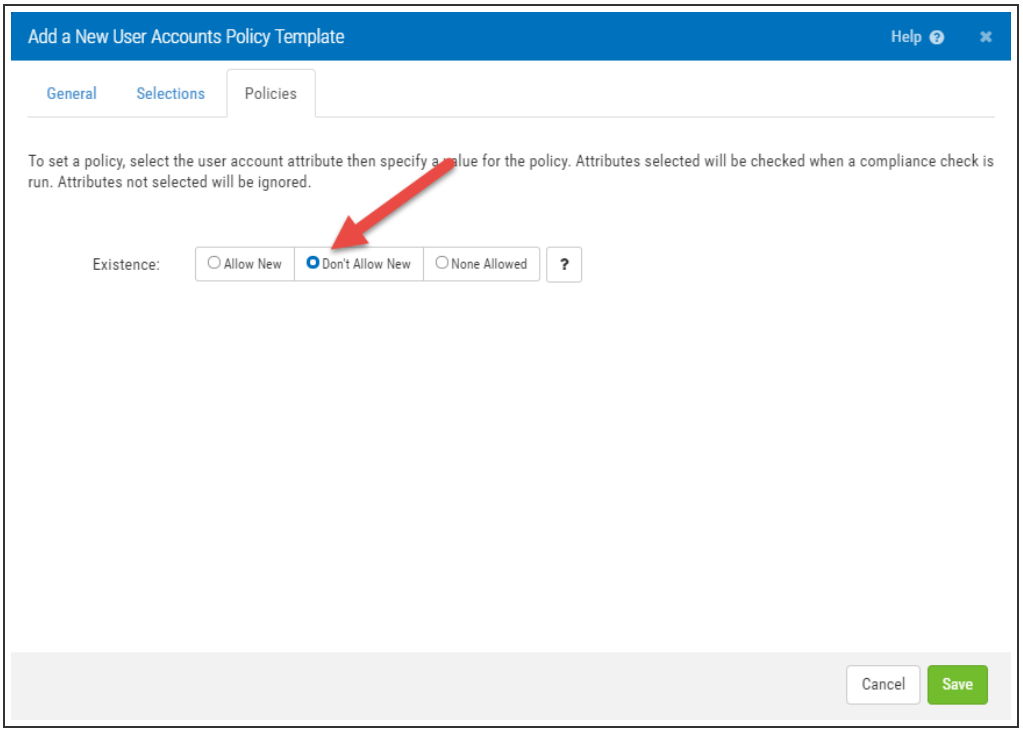
Add a New User Accounts Policy Template

Identify which user accounts to include in this template and which to omit (ignore).

Selection order can be rearranged by dragging rows up or down.

Select Using	Comparison Value	Include or Omit	Action
User Logon Name	Admin	Include	

5. Click on the **Policies** tab. This is where you specify what user account attributes will be checked when a compliance check is run. For this example, we're not going to select any user account attributes. Rather, we are going to disallow new accounts. To do so, select the **Don't Allow New** radio button.



Add a New User Accounts Policy Template

To set a policy, select the user account attribute then specify a value for the policy. Attributes selected will be checked when a compliance check is run. Attributes not selected will be ignored.

Existence: ○ Allow New ● Don't Allow New ○ None Allowed ?

6. Click **Save**.

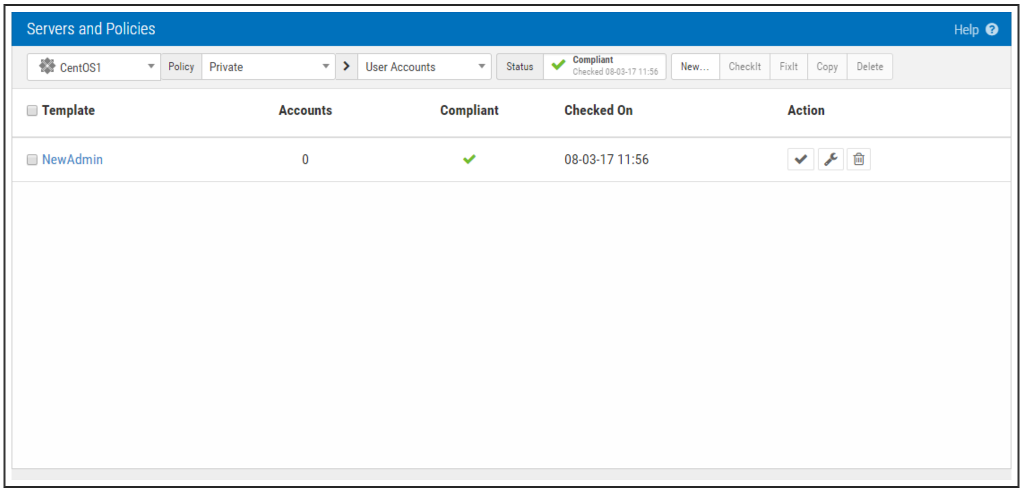
Run a compliance check

The first time a compliance check is run on this template, a baseline of all of the current admin accounts is established. On subsequent compliance checks, if new admin accounts are created or accounts are changed to be an admin, the compliance check will identify any account not in the baseline as out of compliance.

To run a compliance check, do one of the following

- On the Manage Servers screen, click U next to a server to open the server's Files policies.
    - Click ✓ for the Template under the Action column. Or,
    - Select one or more Templates and click **CheckIt**. This will run a compliance check on all the selected user account Templates.
- Choose **Servers > CheckIt**. Choose the server from the Servers tab and then user account Templates from the Policies tab, then click **CheckIt**.
- Schedule a regular compliance check. Go to **Admin tasks > Manage Scheduled Jobs**.

The first time a compliance check is run on this template all accounts will be in compliance.



□ Template	Accounts	Compliant	Checked On	Action
□ NewAdmin	0	✓	08-03-17 11:56	✓ 🔧 🗑

If the template is out of compliance, then a new admin account has been discovered. Click on the template name and then the Compliance tab to determine the new admin account name. In the example below, the Show Compliant box has been unchecked to only show the non-compliant accounts. In this case, the markj account is out of compliance.

If you click on the user account name, you'll see that the account is out of compliance because it's New. Some organizations grant admin rights to individuals temporarily for a special project. Leaving the account out of compliance will serve as a reminder to remove the admin rights once the project is complete.

The 'Allow new accounts' policy attribute is not limited to finding new admin accounts. You can use the 'Allow new accounts' for other templates - perhaps to track new members of a particular group.

Example – Managing Inactive Accounts

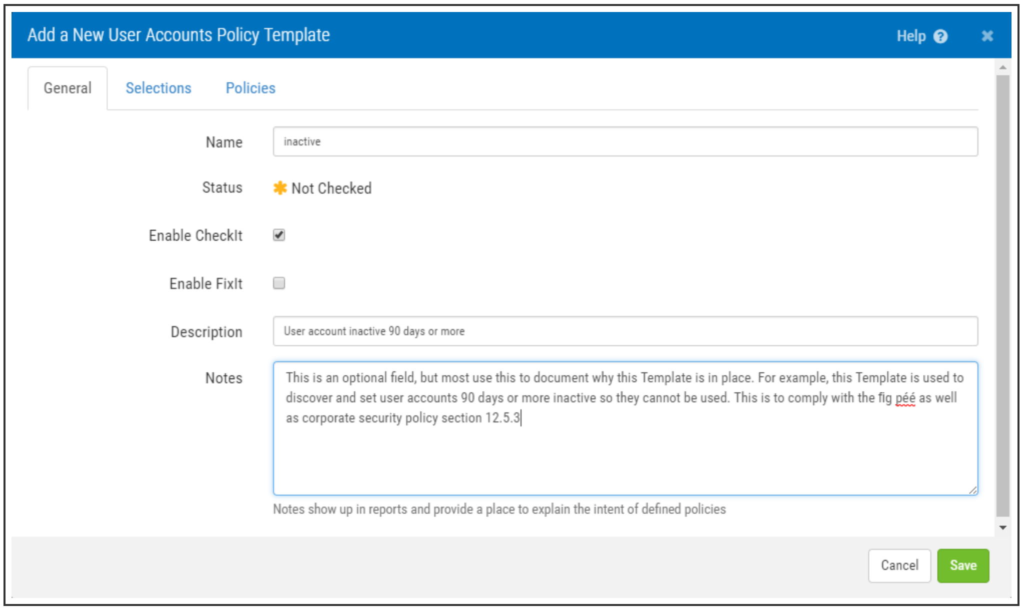
Ensuring user accounts are unable to be used when they are no longer active is both a good security practice as well as required by many laws and regulations. Let's see how you can automate this process:

Define the template

1. To get to the User Account category, on the Manage Servers screen, click the U category for the Private or Group Policy in the row of the desired server.

   Or, go to **Servers and Policies > [server name]**. In the drop-down lists, select whether this should be a Private or Group Policy, then select **User Accounts**.

2. Click **New**. The Add a New User Accounts Policy Template screen appears.
3. Fill in the General tab – see below:



Name: inactive

Status: Not Checked

Enable CheckIt ☑

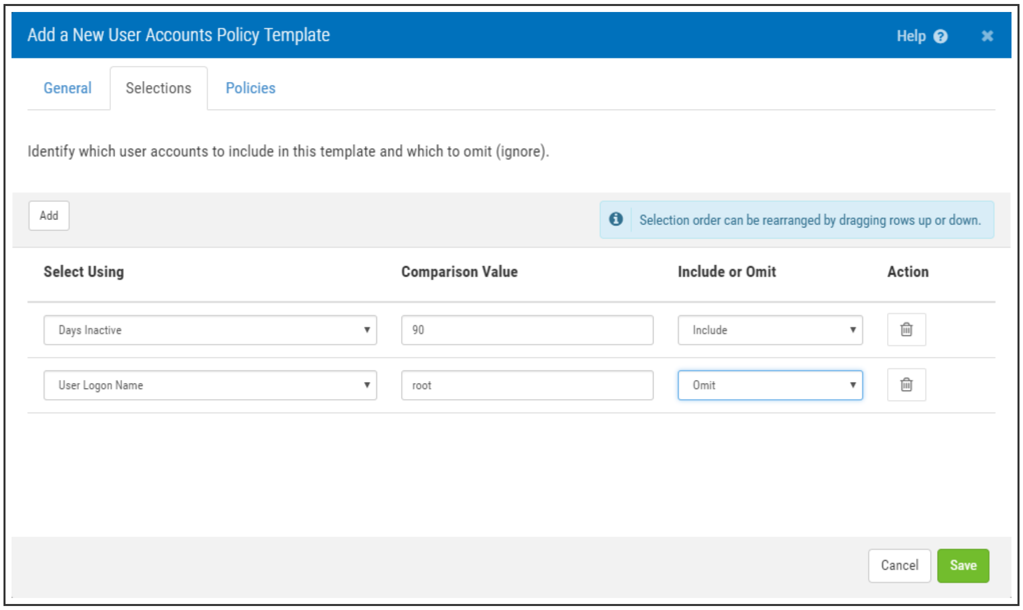
Enable FixIt ☐

Description: User account inactive 90 days or more

Notes: This is an optional field, but most use this to document why this Template is in place. For example, this Template is used to discover and set user accounts 90 days or more inactive so they cannot be used. This is to comply with the fig péé as well as corporate security policy section 12.5.3

Notes show up in reports and provide a place to explain the intent of defined policies

4. Click on the **Selections** tab, click **Add**, and then click on the drop down and choose **Days Inactive**.
5. Enter the number of days inactive you want to select on.
6. Click **Add** if you want to, for example, omit any accounts from being examined during the compliance check.



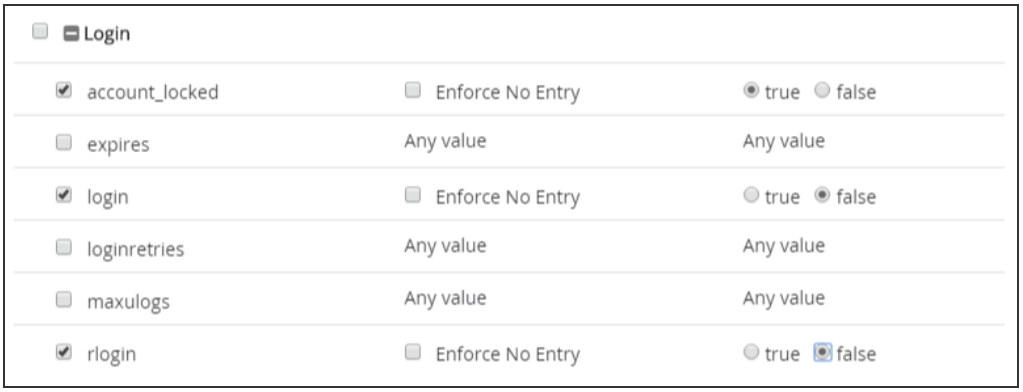
Add a New User Accounts Policy Template

Identify which user accounts to include in this template and which to omit (ignore).

Selection order can be rearranged by dragging rows up or down.

Select Using	Comparison Value	Include or Omit	Action
Days Inactive	90	Include	
User Logon Name	root	Omit	

7. Click the **Policies** tab. In this example we've opened up the Login category so that we can specify what the values should be for the account_locked, login and rlogin attributes. These will be compared to the user account settings during a compliance check. **Notice** the "Enforce No Entry" field in the middle column. There are times, when you want to force values to come from the user account global settings – for example, you typically want this to occur for the password attributes so that you can manage password composition rules on a global basis, rather than an individual basis. But in this case, we don't want these settings to come from the global value. We actually want them to be set in the entry for the inactive user accounts.



□ Login

☑ account_locked	□ Enforce No Entry	● true ○ false
□ expires	Any value	Any value
☑ login	□ Enforce No Entry	○ true ● false
□ loginretries	Any value	Any value
□ maxulogs	Any value	Any value
☑ rlogin	□ Enforce No Entry	○ true ● false

8. Click **Save**.

Run a compliance check

When you run a compliance check on this template any user account inactive 90 days or more will be examined. The accountlocked attribute must be true and login and rlogin must be false. If any attributes do not match these rules, the user account will be identified as out of compliance.

To run a compliance check, do one of the following:

- Click ✓ next to the template name and then click **CheckIt**.
- Go to **Servers > CheckIt**, choose the server.

  > **NOTE:** This runs a compliance check against all templates in the User account category.

- Create a cron job to run the compliance check. Go to **Admin tasks > Manage Scheduled Jobs** (creating scheduled jobs is discussed later).

If the template is out of compliance (indicated by a ✖ in the Compliant column), click on the template name and then the Compliance tab to determine the accounts out of compliance. Click on the account name to see the details of why it's out of compliance.

Run FixIt

FixIt changes the settings of the user account to match the policy (as defined by the template.) To run FixIt, you must first enable it for this template. To enable FixIt, click on the template name then, on the General tab, check the Enable FixIt box. Once you have enabled FixIt, you can run it on the individual user account that is out of compliance or run it on the entire category by selecting the user or template and clicking the FixIt button.

Example – Checking for UID of 0

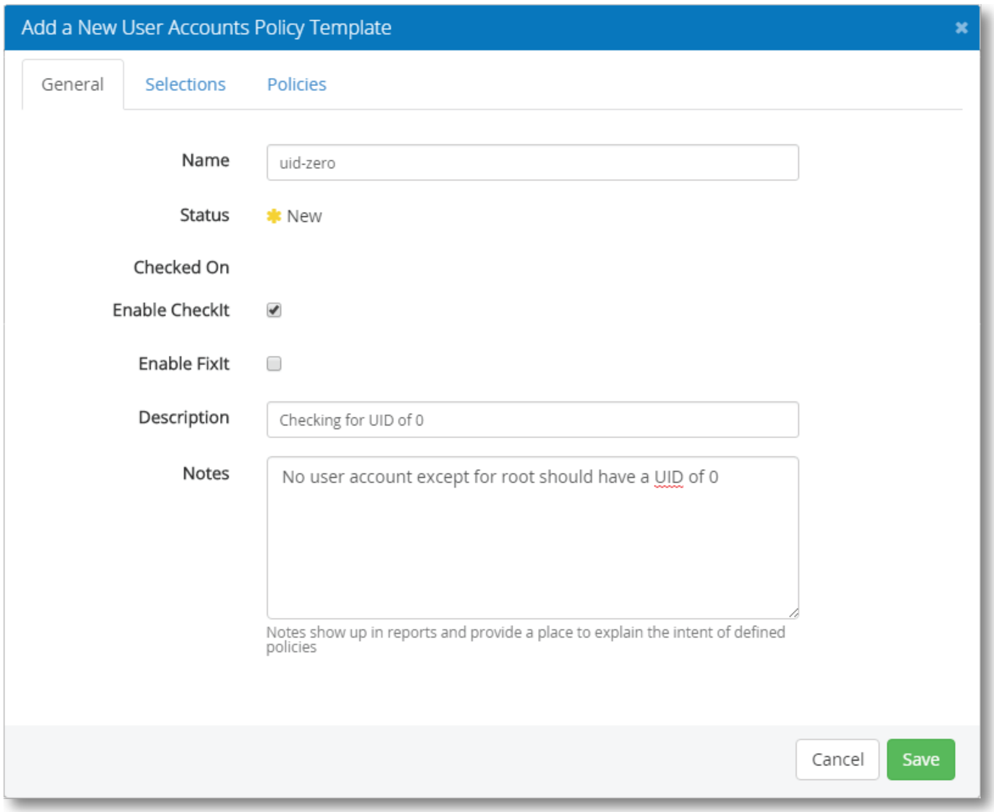
Making sure there are no other user accounts besides root with UID of 0 is a routine request of many auditors. Here's how you'd configure that template:

Define the template

1. To get to the User Account category, on the Manage Servers screen, click the U category for the Private or Group Policy in the row of the desired server.

   Or, go to **Servers and Policies > [server name]**. In the drop-down lists, select whether this should be a Private or Group Policy, then select **User Accounts**.

2. Click **New**.
3. Fill in the General tab – see next example:



Add a New User Accounts Policy Template

Name: uid-zero

Status: New

Checked On

Enable CheckIt: ☑

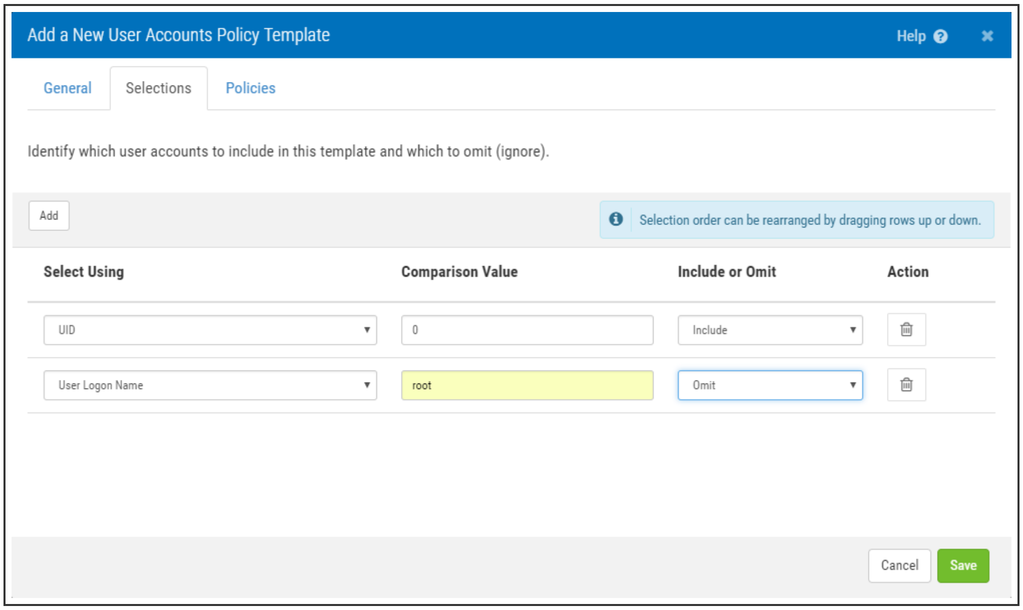
Enable FixIt: □

Description: Checking for UID of 0

Notes: No user account except for root should have a UID of 0

Notes show up in reports and provide a place to explain the intent of defined policies

4. Click on the **Selections** tab and click **Add**.
5. Choose **UID** from the drop-down and specify **0** for the Comparison value.
6. Click **Add** again and omit User Logon Name root from being examined (we know that root should have UID of 0).



Add a New User Accounts Policy Template

Identify which user accounts to include in this template and which to omit (ignore).

Selection order can be rearranged by dragging rows up or down.

Select Using	Comparison Value	Include or Omit	Action
UID	0	Include	🗑
User Logon Name	root	Omit	🗑

7. Click **Save**.

Run a compliance check

When you run a compliance check on this template any user account that has a UID of 0 – with the exception of root, will be identified as being out of compliance.

To run a compliance check, do one of the following:

- Click ✓ next to the template name (under the Action column).
- Check the box next to the template name and then click **CheckIt**.
- Go to **Servers > CheckIt**, choose the server.

> **NOTE:** This runs a compliance check against all templates in the User account category.

- Create a cron job to run the compliance check. Go to **Admin tasks > Manage Scheduled Jobs** (creating scheduled jobs is discussed later).

If the template is out of compliance (indicated by a ✖ in the Compliant column), click on the template name and then the Compliance tab to determine the accounts out of compliance. (In this case, the accounts with UID of 0.)

Files

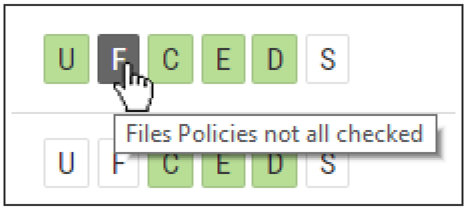
You can create templates to regularly check the permissions, ownership and other attributes of directories and files. You can also use templates to find new files that didn’t exist during the last compliance check - for example, a new executable with the SUID bit set. Or you can monitor a set of files for ownership or group changes. Use your imagination and there are some very powerful administration and compliance tasks that can be automated. Let’s take a look at some examples.

Example 1 – Finding all files with the SUID bit and Monitor Ownership

You may have an application or set of files configured to run with the permission of the owner (i.e., the SUID bit is on). If one of these files’ owner changes, you’d obviously want to know that so that the application doesn’t fail or users aren’t gaining more permissions than they need. Finding those files and then monitoring to make sure the ownership doesn’t change may be something you’ve always wanted to do but didn’t have the time to write the script or just didn’t have the resources to get it done. This is a very easy scenario for Security Auditor.

Defining the template

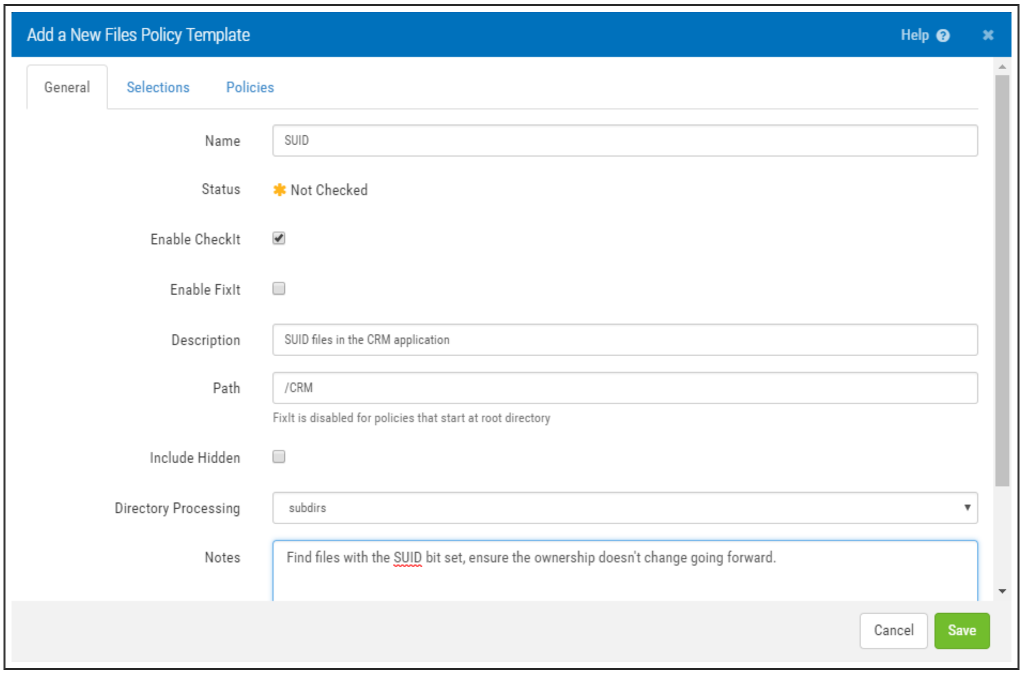
1. To get to the Files category, on the Manage Servers screen, click the F category for the Private or Group Policy in the row of the desired server.

   Files Policies not all checked

   Or, go to **Servers and Policies > [server name]**. In the drop-down lists, select whether this should be a Private or Group Policy, then select **Files.**

2. Click **New**. The Add a New Files Policy Template screen appears.
3. Fill in the General tab – see next example:



Add a New Files Policy Template

Name: SUID

Status: ✱ Not Checked

Enable CheckIt: ☑

Enable FixIt: ☐

Description: SUID files in the CRM application

Path: /CRM

FixIt is disabled for policies that start at root directory

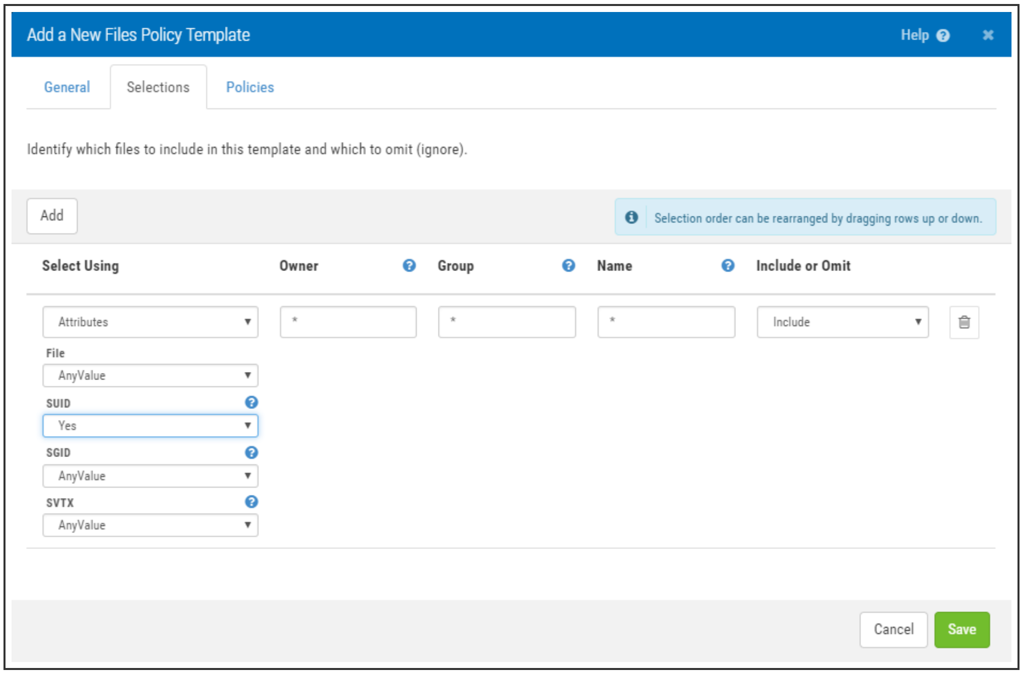
Include Hidden: ☐

Directory Processing: subdirs

Notes: Find files with the SUID bit set, ensure the ownership doesn't change going forward.

4. On the General tab name the template, give it a description, and then specify the path that is to be searched. The Notes section can provide more documentation about why the template is being implemented.

5. On the **Selections** tab, click **Add**, then click the drop-down under 'Select Using' and choose **Attributes**. For the SUID parameter, select **Yes**. Leave the others at **AnyValue**.



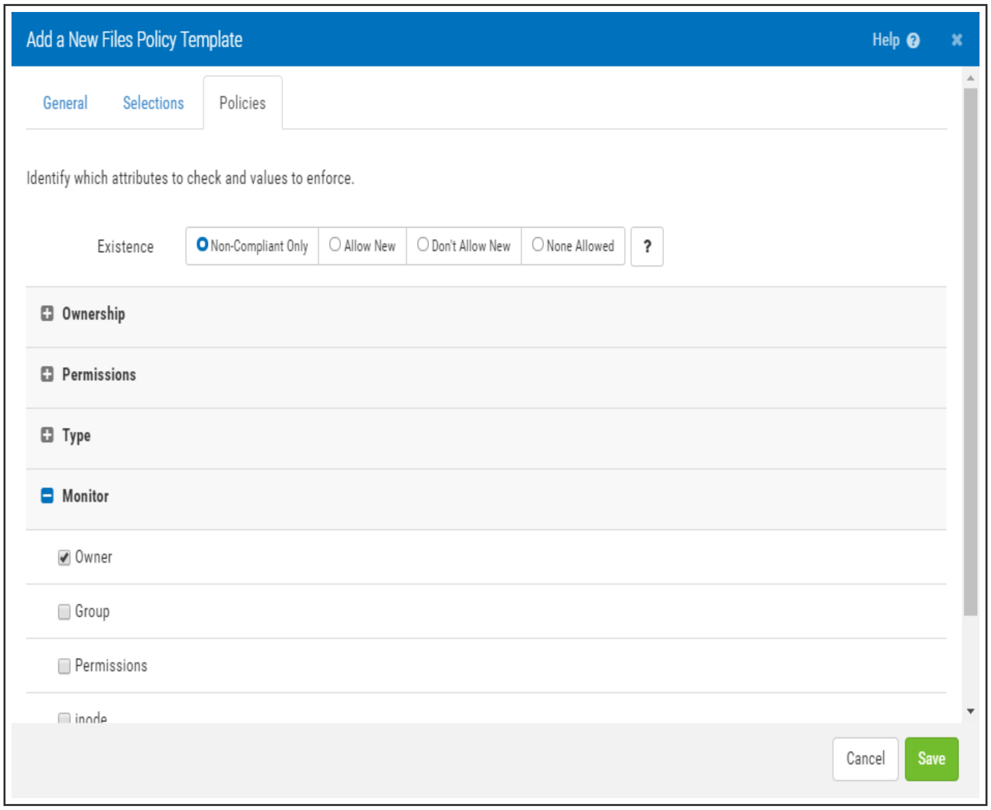
Add a New Files Policy Template

Identify which files to include in this template and which to omit (ignore).

Selection order can be rearranged by dragging rows up or down.

Select Using	Owner	Group	Name	Include or Omit
Attributes File: AnyValue SUID: Yes SGID: AnyValue SVTX: AnyValue	*	*	*	Include

6. On the **Policies** tab, open **Monitor** then check **Owner**.



Add a New Files Policy Template

Identify which attributes to check and values to enforce.

Existence ● Non-Compliant Only ○ Allow New ○ Don't Allow New ○ None Allowed ?

☑ Owner

□ Group

□ Permissions

□ inode

7. Click **Save**.

Running a compliance check

When you run a compliance check on this template, it will include the files with the SUID bit set on. The first compliance check records the current owner. Subsequent compliance checks will examine the owner of these files and if the owner is different, the file will be out of compliance.

To run a compliance check, do one of the following

- On the Manage Servers screen, click ✓ CheckIt ▾ and choose whether you want to check the Private Policy, Group Policy, or both for the server (or Server Group).
- On the Manage Servers screen, click F next to a server to open the server's Files policies.
  - Click ✓ for the Template under the Action column. Or,
  - Select one or more Templates and click **CheckIt**. This will run a compliance check on all the selected file Templates.
- Choose **Servers** > **CheckIt**. Choose the server from the Servers tab and then File Templates from the Policies tab, then click **CheckIt**.
- Schedule a regular compliance check. Go to **Admin tasks** > **Manage Scheduled Jobs**.

If the template is out of compliance (indicated by a ✖ in the Compliant column), click on the template name and then the Compliance tab to determine the files that are out of compliance. Click on the file name to see the details of why it’s out of compliance.

Example 2 – Ensuring a Specific File is Secured Correctly

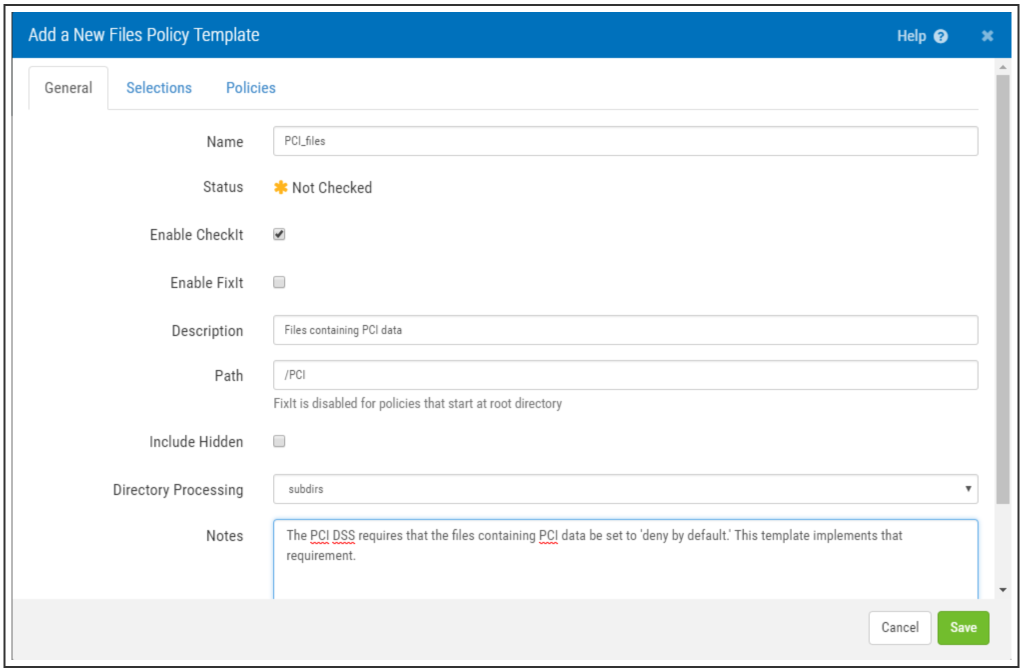
You may have an audit requirement to ensure a specific file(s) is secured appropriately. Perhaps it holds PCI or HR data or perhaps you want to make sure the directory containing payroll information is only accessible by the group processing payroll checks. Whatever the case, this is very easy to configure in Security Auditor.

Defining the template

1. To get to the Files category, on the Manage Servers screen, click the F category for the Private or Group Policy in the row of the desired server.

   Or, go to **Servers and Policies > [server name]**. In the drop-down lists, select whether this should be a Private or Group Policy, then select **Files**.

2. Click **New**.
3. Fill in the General tab – see next example:



Name: PCI_files

Status: Not Checked

Enable CheckIt: ☑

Enable FixIt: □

Description: Files containing PCI data

Path: /PCI

FixIt is disabled for policies that start at root directory

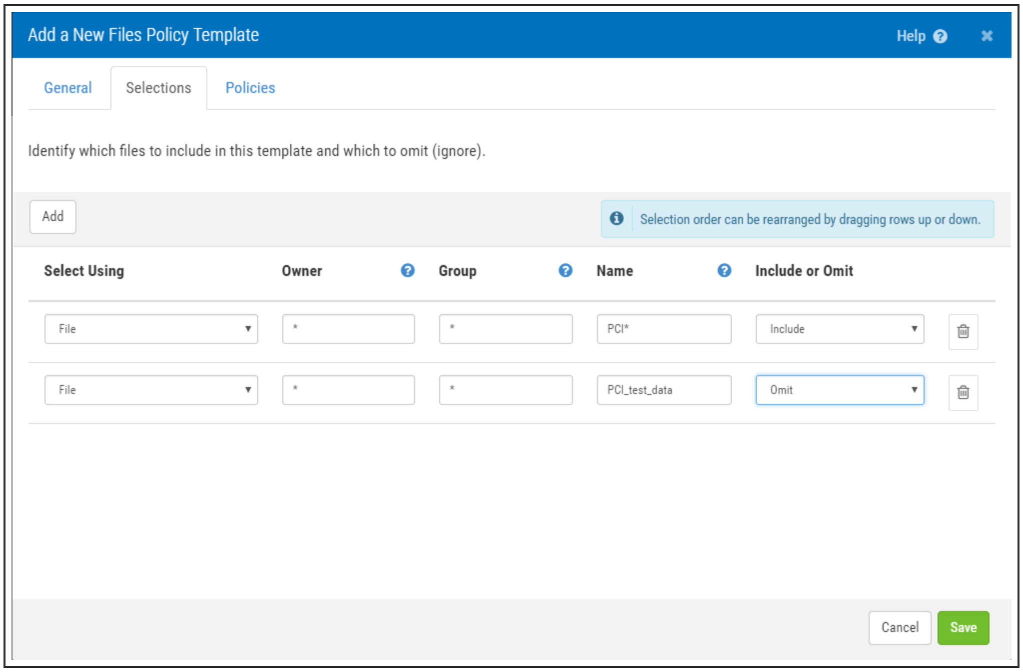
Include Hidden: □

Directory Processing: subdirs

Notes: The PCI DSS requires that the files containing PCI data be set to 'deny by default.' This template implements that requirement.

4. On the General tab:
   - Name the template and give it a description.
   - Type the path of the directory or file you want to work with in this template.
   - Specify whether or not to Include Subdirectories. If this box is unchecked, only the items in that path will be examined and no subdirectories will be traversed.
   - Use the Notes section to document the template. (These notes are displayed at the beginning of the print policy report.)
5. On the Selections tab, click **Add** for the files you want to include in the policy. With (for example) **File** selected under the drop-down menu, specify the files in the /PCI directory that you want examined. In the following screen, all files with the prefix of PCI will be examined on a compliance

check with the exception of the file, PCI_test_data.

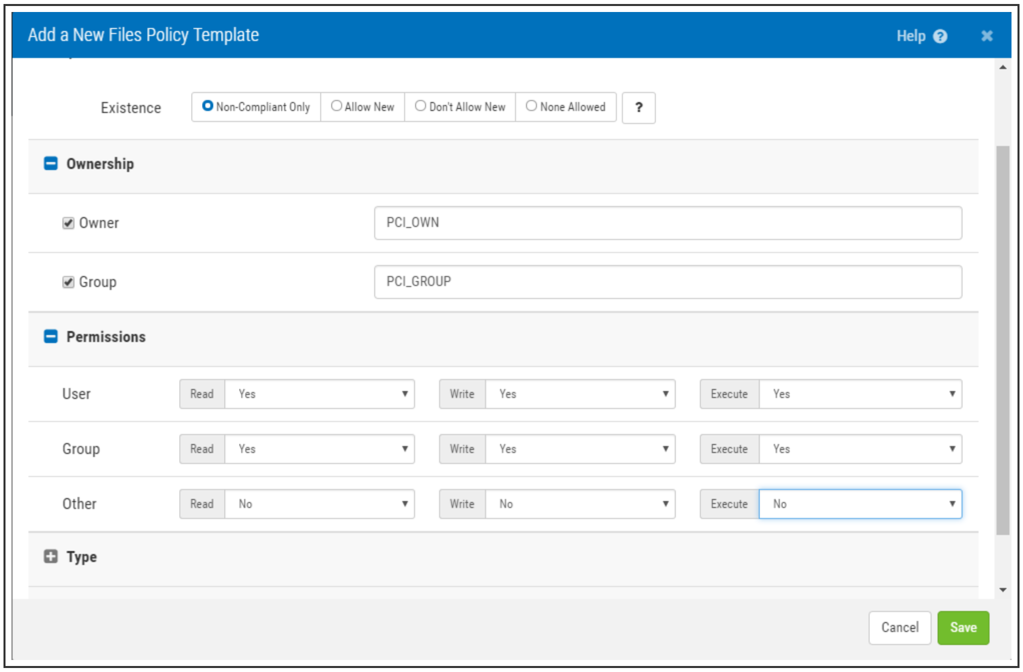

Add a New Files Policy Template

Identify which files to include in this template and which to omit (ignore).

Selection order can be rearranged by dragging rows up or down.

Select Using	Owner	Group	Name	Include or Omit
File	*	*	PCI*	Include
File	*	*	PCI_test_data	Omit

6. Click the Policies tab and specify the attributes that you want checked when a compliance check is run against this policy.


Add a New Files Policy Template

Existence ● Non-Compliant Only ○ Allow New ○ Don't Allow New ○ None Allowed

Ownership

☑ Owner PCI_OWN

☑ Group PCI_GROUP

Permissions

User	Read Yes	Write Yes	Execute Yes
Group	Read Yes	Write Yes	Execute Yes
Other	Read No	Write No	Execute No

Type

7. Click **Save**.

Running a compliance check

When you run a compliance check on this template the files will be checked to ensure the owner is PCI_OWN, the group is PCI_GROUP, the permissions are set to user RWX, group RWX, other --- and that the

SUID, SGID and SVTX bits are not set. If any of these don't match the current settings for these files, the file will be identified as out of compliance.

To run a compliance check, do one of the following

- On the Manage Servers screen, click ✓ CheckIt ▾ and choose whether you want to check the Private Policy, Group Policy, or both for the server (or Server Group).
- On the Manage Servers screen, click F next to a server to open the server's Files policies.
  - Click ✓ for the file Template under the Action column. Or,
  - Select one or more Templates and click **CheckIt**. This will run a compliance check on all the selected Templates.
- Choose **Servers > CheckIt**. Choose the server from the Servers tab and then file Templates from the Policies tab, then click **CheckIt**.
- Schedule a regular compliance check. Go to **Admin tasks > Manage Scheduled Jobs**.

If the template is out of compliance (indicated by a ✖ in the Compliant column), click on the template name and then the Compliance tab to determine the files that are out of compliance. Click on the file name to see the details of why it's out of compliance.

Running FixIt

FixIt changes the settings of the file to match the policy (as defined by the template.) To run FixIt, you must first enable it for this template.

To enable FixIt

1. Click on the template name then, on the General tab, check the **Enable FixIt** box.
2. Click **Save**.

Once you have enabled FixIt, you can run FixIt on the individual file that's out of compliance or run it on the entire template by selecting either the file or template and clicking the FixIt button.

Scripts

The Scripts category makes it possible for you to upload scripts into the Security Auditor console and run them as part of your compliance checks. Running your existing scripts through the Security Auditor for AIX console allows administrators to consolidate scripts in a central location and keep track of the last time they were run as well as take advantage of Security Auditor's reporting functions. The Scripts category shares the same features as other categories. The compliance status of each script run through Security Auditor is reflected in the console, included in Security Auditor reports and can be invoked through the integrated cron function.

The scripts run during a compliance check (CheckIt) are typically scripts written by administrators to view server configuration elements or the state of a server or element of a server but in reality, they can be any script you want to run via and the results reported through Security Auditor.

Defining a Script Policy

Defining a script policy is a two-step process.

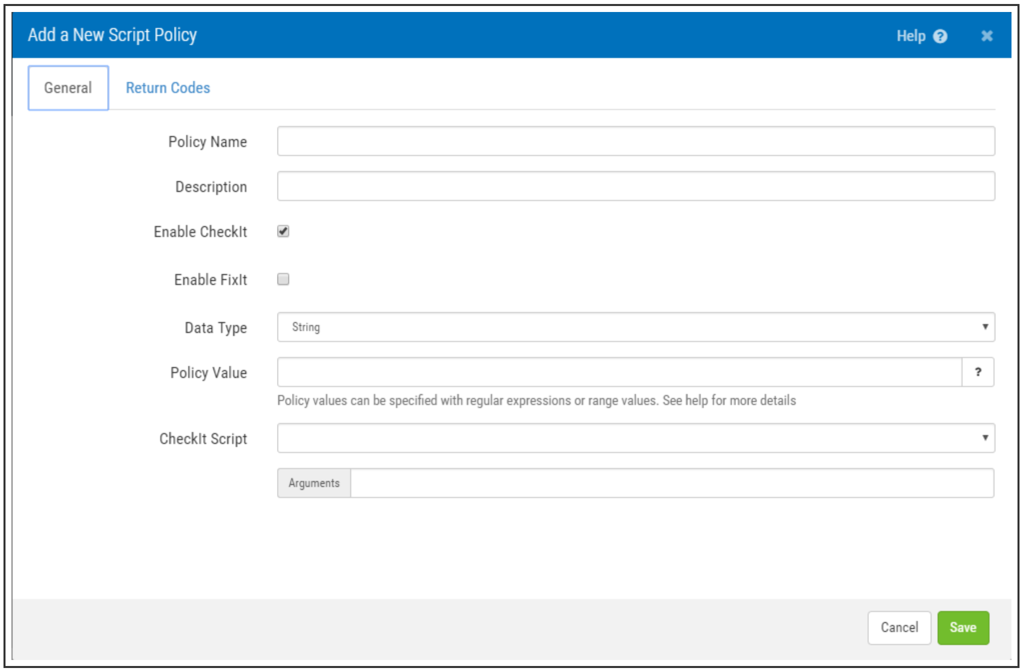
Step 1: Before a script policy can be defined, the script(s) must be uploaded to the server on which the Security Auditor console is running. Do this by going to **Admin Tasks > Scripts > Upload** to upload the script from your desktop to a Windows console.

Or, when running an AIX or Linux console, you can place the scripts in the following directory (where Security Auditor was installed):

…/PowerTech/SecurityAuditor/tomcat/webapps/securityauditor/scripts

Once a script has been uploaded or placed directly into the scripts directory, it will appear as a selection for the CheckIt script and FixIt script when defining a Script Policy.

Step 2: Once a script has been uploaded to the console, you can define a Script Policy. Go to **Servers and Policies > [server] >Scripts** and click **New** to get started.



Add a New Script Policy

Policy Name

Description

Enable CheckIt ☑

Enable FixIt □

Data Type: String

Policy Value

Policy values can be specified with regular expressions or range values. See help for more details

CheckIt Script

Arguments

The Policy Value is what you see as a result of running the script. Specify the Data Type that is appropriate for this result.

> **NOTE:** a valid result of running a script may be nothing or no value. In this case, leave the Policy Value field blank. When a compliance check is run on this script policy, the result of running the script will be compared against the value you specify in the Policy Value field. If they are equal the policy will be compliant. If they aren't, the script policy will be out of compliance.

Data types may be String, Integer, Boolean and date

- String values can be literal or regular expressions.
- The syntax for regular expressions follows a standard and is documented in the dialog. The documentation can be viewed in a popup dialog by clicking on the icon.
- Integer values can be a specific value, a range, or a list of ranges and specific values. The syntax for integers is also documented in the popup dialog.
- A Boolean value is considered true if it matches (ignoring case) any of the values "true", "t", "yes", "y" or "on" or if the value can be parsed as a number and does not equal zero.
- Date values can be a specific date, a before date, an after date or a date range.

Click on the CheckIt Script drop down to choose the script.

If the script requires arguments to be passed in, specify those in the Arguments field.

Running a Compliance Check

When a compliance check (CheckIt) is run, the Policy Value is compared to the value returned by the script. If the value returned by the script (which is called the Server Value in the script policy) matches the Policy Value, the policy is compliant. If they don't match, it's out of compliance (non-compliant.)

Notes:

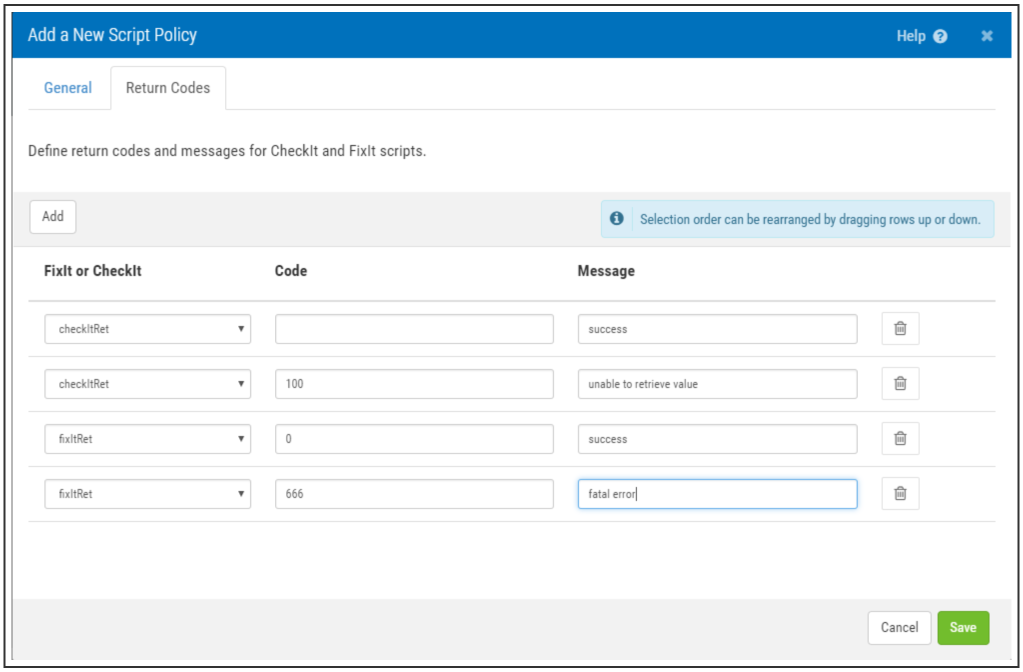
- The line returned by the script is compared to the policy value to determine compliance status.
- A valid result of running a script may be nothing or a blank result. When this is the case, the Policy Value field should be left empty (blank.)
- If multiple values are checked, they must be rolled up into a single line.
- A script may be given one or more arguments to be passed when invoked.
- When a script policy is run during the compliance check, the script is first transferred to the server using scp, run, then deleted from the server.
- See the Return Codes section (below) for considerations when using return codes in your script.

Running FixIt

You can enable FixIt for a Script Policy. If you check the Enable FixIt box, the FixIt script line will appear and you will have to select the script to run when FixIt is run for this policy. When selecting the script for FixIt, you will not be prompted for a Policy Value since FixIt is intended to change the server configuration or state to a compliant value and there will likely be no results expected from running the FixIt script.

Return Codes

By convention, a return code of 0 from a script indicates success. Any non-zero numeric value is, by convention, used to indicate specific error conditions. On the Return Codes panel, values can be associated with strings that will be shown when a script is run and returns that code. The associated strings are also shown in Security Auditor reports. Only when a script returns a success code AND the returned value matches the policy value is a script policy considered compliant. Return code of 0 is pre-defined for both CheckIt and FixIt.



Define return codes and messages for CheckIt and FixIt scripts.

Selection order can be rearranged by dragging rows up or down.

FixIt or CheckIt	Code	Message
checkItRet		success
checkItRet	100	unable to retrieve value
fixItRet	0	success
fixItRet	666	fatal error

Exporting and Importing Script Packages

You may want to utilize the same scripts on multiple Security Auditor consoles or those acquired elsewhere. In either case, you will need to use the Export / Import function of the Script category. This differs from the more general Export / Import policy function because this function imports both the script policy AND the scripts defined for the policy – we call this a script package.

To import a script package go to **Admin Tasks > Scripts > Import Package**.

> **NOTE:** To import a script package, it must first be on the console.

- For an AIX console, place the package in the following directory

  .../PowerTech/SecurityAuditor/tomcat/webapps/securityauditor/exports

- For a Windows console, go to **Admin Tasks > Scripts > Upload** to upload it to the console

Select the script package file to import and then select the servers to which the policy will be applied.

To export a script package, go to **Admin Tasks > Script > Export Package**.

FixIt

As noted in the previous sections, FixIt changes the settings on the server to match the policy. FixIt is very powerful and we encourage you to carefully review what is going to be fixed – that is, what is out of compliance – prior to running FixIt.

FixIt in Test Mode

Prior to running FixIt we encourage you to determine exactly what is going to be changed. You can do that in one of two ways:

- Examine the compliance reports to see what is out of compliance. The non-compliant items will be changed to match the policy settings.
- Take advantage of the Test mode parameter of FixIt. No changes will be made! Rather, the changes that would have been made are logged in the Security Auditor Message Log, but no values are actually changed. You can then review what changes would have been made had FixIt actually changed the values or settings. To enable / disable Test mode, go to **Admin Tasks > Preferences > General**. Check (or uncheck) **FixIt Test mode**.

Running FixIt

Several methods are available for running FixIt once it has been configured for a template or category and after a compliance check has been completed. (Don't forget, a compliance check must be run before FixIt is run!)

1. Enable FixIt by going into the Properties for the category or individual item. Then click on **FixIt**.
2. Run FixIt while viewing the items in the category or go to **Servers > FixIt**.
3. Schedule a cron job to run FixIt.

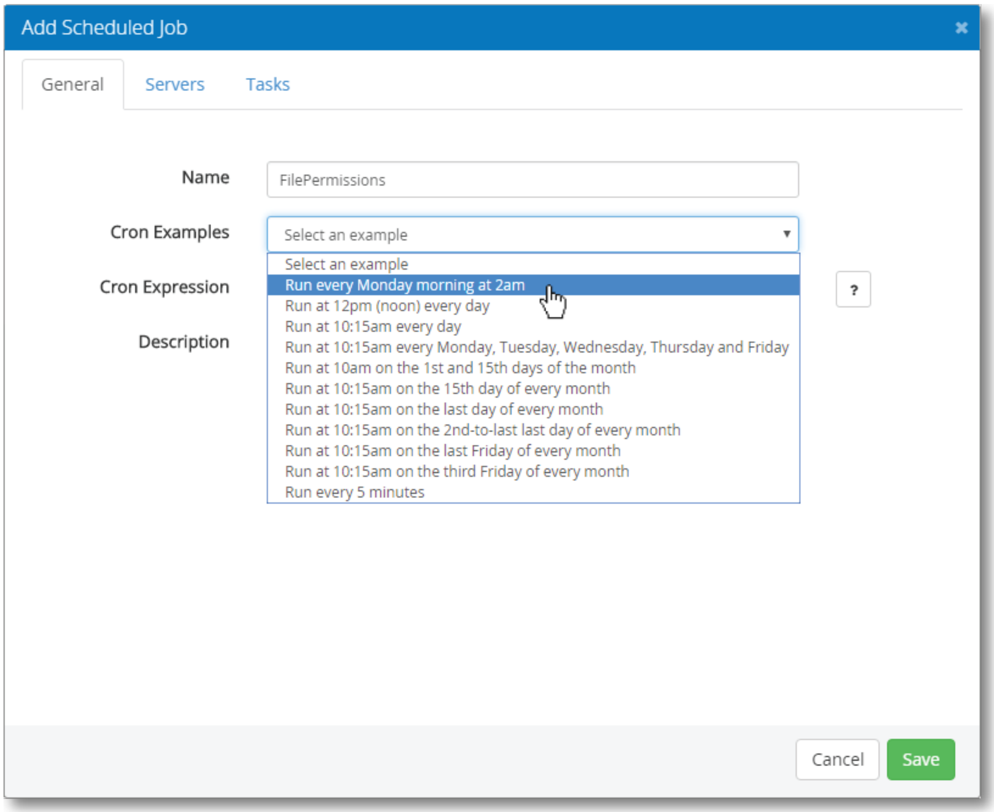
FixIt Restrictions

- Before running FixIt, you must first run a compliance check to identify the non-compliant items. (FixIt will only run against non-compliant items.)
- If you create a directory template that begins at the root ('/') directory FixIt will not run against this template. You can work with the objects in the template and run FixIt on an individual object in the template; however, FixIt will not work on the template as a whole. This restriction prevents running FixIt on the entire File System, which could be quite disruptive. You can create a template that starts with a directory lower than the root directory and run FixIt, but not on a template that starts with the root directory.

Scheduling Security Auditor Jobs

Security Auditor comes with its own, integrated scheduling function based on the traditional Unix cron functionality.

1. To schedule a job, choose **Admin Tasks > Manage Scheduled Jobs**.
2. To add a job, click **New**. On the General tab, specify the name and description along with the schedule of when the job is to run. Because the cron syntax is not at all obvious, we've provided some examples for you to use as is or modify to meet your specific requirements. Simply choose the schedule that most closely matches your requirement from the Cron Example drop down.



Add Scheduled Job
General
Servers
Tasks
Cron Expression
Description
?
Select an example
Run every Monday morning at 2am
Run at 12pm (noon) every day
Run at 10:15am every day
Run at 10:15am every Monday, Tuesday, Wednesday, Thursday and Friday
Run at 10am on the 1st and 15th days of the month
Run at 10:15am on the 15th day of every month
Run at 10:15am on the last day of every month
Run at 10:15am on the 2nd-to-last last day of every month
Run at 10:15am on the last Friday of every month
Run at 10:15am on the third Friday of every month
Run every 5 minutes
Cancel
Save

Name: FilePermissions

Cron Examples: Select an example

Two other sources of help are available. Clicking on the information icon will go to another website that explains cron functions. The builder icon is a website that helps you build the cron expression yourself.

3. On the Servers tab, choose one or more servers where the job is to run.
   - **Private Share Mode; Private • Group.**Choose **Private** to use the servers' Private Policy settings. These are the Policies assigned to servers individuality. Choose **Group** to specify that you want to use the Group Policy for the selected server. See Manage Servers screen. If you choose Group for the Policy Share Mode, any new servers added to the group will be included in the scheduled job (and servers removed from the Group will not be included).
   - **Server Selection; Specific Servers • Groups.** Choose **Specific Servers** to select the servers individually in the server list. Choose **Groups** to select server Groups only.
4. On the Tasks tab, specify the task(s) you wish to schedule. See Add Scheduled Job.

Backing Up Security Auditor

We recommend that you back up the following:

…\SecurityAuditor\db

…\SecurityAuditor\tomcat\webapps\SecurityAuditor\exports

…\SecurityAuditor\tomcat\webapps\SecurityAuditor\logs

…\SecurityAuditor\tomcat\webapps\SecurityAuditor\reports

…\SecurityAuditor\tomcat\webapps\SecurityAuditor\scripts

…\SecurityAuditor\tomcat\webapps\SecurityAuditor\WEB-INF\keys

…\SecurityAuditor\tomcat\webapps\SecurityAuditor\WEB-INF\license

Backup Scripts

The Security Auditor installation includes backup scripts you can use to automate the backup process.

> WARNING: These scripts are intended to be used as an example only. In order to be used for your backup process, they must be copied and modified to include the proper archive locations for your environment.

Script location

- General: *security auditor home***\sabackup**
- Windows: **C:\Program Files (x86)\Powertech\SecurityAuditor\sabackup**

Scripts

Windows:

- sa_backup.bat
- sa_restore.bat
- sa_setupenv.bat

Xnix (bash):

- sa_backup.sh
- sa_restore.sh
- sa_setupenv.sh

Running the Backup Scripts

Before running the scripts, stop the Security Auditor web server and database services.

By default, the backup script will create a backup folder here:

General:
`security auditor home\sabackup\backups\YourComputerName\timestamp`

Windows:
`C:\Program Files (x86)\Powertech\SecurityAuditor\sabackup\backups\YourComputerName\timestamp`

> **EXAMPLE:**
> `C:\Program Files (x86)\Powertech\SecurityAuditor\sabackup\backups\SAServer\20161231-235959`

Copy/modify the backup scripts to use a location more appropriate for your needs.

The restore script must be modified to restore from the proper backup location. To do so, change the “SABACKUP” environment variable.

Working with Reports

Reports are available to:

- Document your policies.
- Provide the results of the last compliance check.
- Document the changes made using the FixIt function, including the exact command that was run and the setting before FixIt was run.
- Document actions taken by Security Auditor administrators (see Working with the Message Log).

Documenting your Policy

You can print your policy definition by going to **Servers > Reports > Create Reports** and choosing the Policy report type. You can use this report as:

- Your documentation for the IBM AIX and Linux implementations of your overall security policy – some people call this their security “standards.”
- Documentation to show auditors as to how your security is configured
- An additional description can be added to the policy for each category or template. People often use this to describe the portion of the security policy being implemented, reasons why items are omitted from the template, document risk acceptance standards, etc

Checking compliance

After running a compliance check, the results you’re obviously looking for is an “empty” report. That is, a report with the summary stating that the status is “compliant.”

Unfortunately, there may be times when items are out of compliance. In this case, the items that are out of compliance will be listed and include the policy setting as well as the current setting – there’s no further investigation needed to determine the issue – it will be in the report.

Documenting what FixIt Fixed

It’s quite possible that your change management process requires that you document every change on your servers. The FixIt reports will assist with that requirement. The report shows the user that made the change, how the change was made, the new value and the original value.

Generating and Viewing Reports

To generate reports:

1. Choose **Reports**, then click **Create Reports**. (Or, go to **Servers > Create Reports**.) The Create Reports screen appears.
2. In the **Servers** tab, choose the servers or Server Groups from which you want the reports.

3. In the **Policies** tab:
   - Choose whether you want reports for Private Policies or Group Policies.
   - Select the Policies you want to include on the report.
   - For User Accounts, Files, and Scripts, you can choose **Selected** to choose from a list of available Policies. Choose All to include all policies for that type on the report.
4. In the **Options** tab:
   - Under Select Report Category, choose the type of report:
     - **Compliance.** This report shows compliance details for the selected servers and policies.
     - **Policy.** This report shows the policy details.
     - **FixIt.** This report shows FixIt activity details.
     - **Message Log.** This report shows a list of Security Auditor messages for the type(s) selected.
   - whether you want one report for each server, or one report that includes the information from all servers you've selected.
5. The reports can be viewed by selecting **Single-System Tasks > Reports**.

Report Formats

Both PDF and CSV formats are available. They are written to the following directory on the system running the console:

/PowerTech/SecurityAuditor/tomcat/webapps/securityauditor/reports

Emailing Reports

You can choose to email the report when the report is generated or while viewing the reports. In order to do so, you must configure an SMTP server. To change or manage the SMTP server settings, go to **Admin Tasks > Preferences > Email Server**. See Preferences screen.

> **NOTE:** The Default SMTP server option available in earlier versions of this software is no longer available. In order to send email from Security Auditor you will need to define an SMTP server.

Removing Security Auditor from your Servers

To remove Security Auditor from a server, simply delete the server from the console. This removes Security Auditor from the server as well as deletes the data from the console associated with the server and frees its license so it can be used for another server.

Removing Security Auditor from the Console:

On Windows, go to **Start > All Programs > Powertech > Security Auditor** and run the following (in this order):

1. Stop Security Auditor
2. Uninstall Powertech Security Auditor

Notes:

- Make sure that the directory where Security Auditor was installed has been deleted and delete it if it remains on the computer.
- You will have to restart the computer to complete the uninstall.

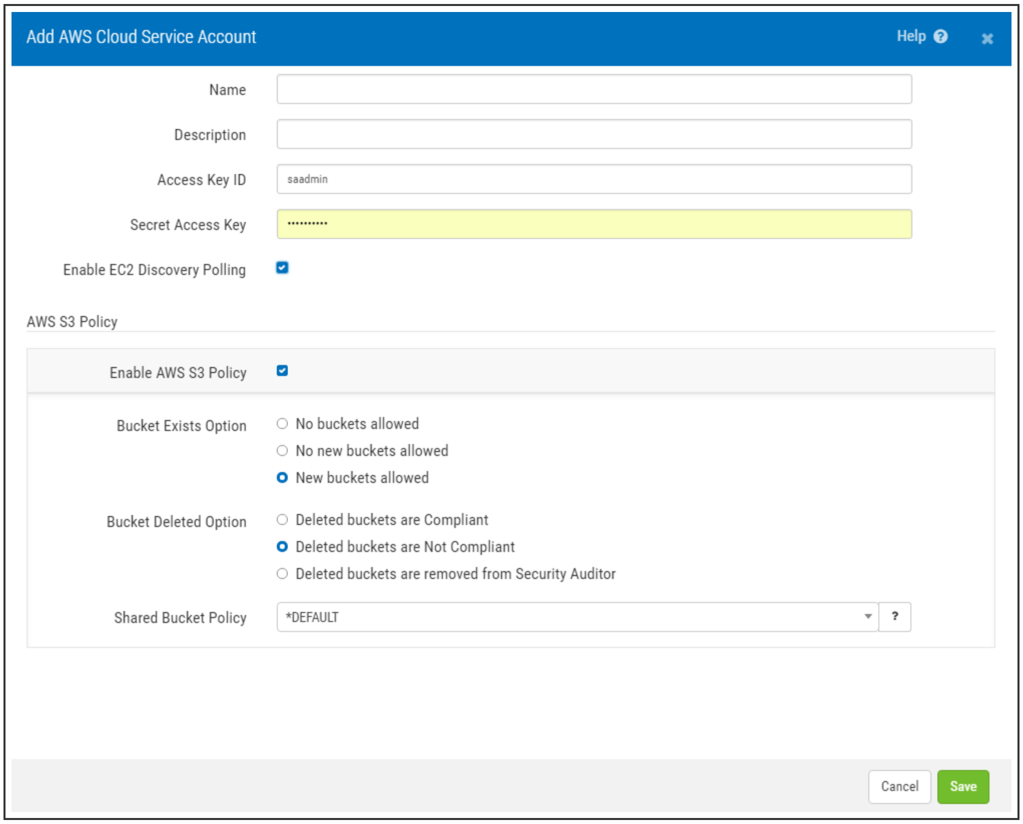
On AIX or Linux, navigate to where Security Auditor was installed and run the stoppm.sh script then execute the Uninstall file. You may need to delete the last Installation file (used to install or upgrade) if you have not already done so.

> **NOTE:** All user data, including all polices, templates, server definitions and logs are removed during the uninstall process.

Reference

The topics in this section include descriptions of Security Auditor's options and controls.

Add/Modify AWS Cloud Service Account



Add AWS Cloud Service Account

Name

Description

Access Key ID: saadmin

Secret Access Key: ••••••••••

Enable EC2 Discovery Polling ☑

AWS S3 Policy

Enable AWS S3 Policy ☑

Bucket Exists Option
○ No buckets allowed
○ No new buckets allowed
● New buckets allowed

Bucket Deleted Option
○ Deleted buckets are Compliant
● Deleted buckets are Not Compliant
○ Deleted buckets are removed from Security Auditor

Shared Bucket Policy: *DEFAULT

How to Get There

From the AWS Accounts menu, choose **Add AWS Account**.

Or, on the Manage AWS Cloud Service Accounts screen, click **Add**.

Or, click an existing account to modify it.

What it Does

Use this screen to create or modify an AWS account definition.

This screen allows you to define access to an Amazon Web Services (AWS) Elastic Compute Cloud account. Security Auditor will interact with this service to detect and automatically monitor the policy settings on these servers.

You can define one or more accounts and associated filter settings that will automatically map AWS server instances to Security Auditor Managed Services with Shared Group Policy definitions.

These options also allow you to enable an S3 policy and define how it is enforced for buckets in the account.

Options

Name

This is a unique name for the account.

Description

An optional description of the account.

Access Key ID • Secret Access Key

The Access Key ID and Secret Access Key of your cloud services account.

Enable Discovery Polling

Check this box to enable server instance discovery. With this option enabled, new servers added to your cloud service will be identified by Security Auditor and added as managed servers based on your filter settings. See the Manage Filters screen and Add/Modify Filter screen.

AWS S3 Policy

Enable AWS S3 Policy

Use this check box to enable or disable an S3 Bucket Policy.

Bucket Exists Option

If Enable AWS S3 Policy is checked, these options are available.

- **No buckets allowed.** Choose this option to consider any/all buckets in the account non-compliant.
- **No new buckets allowed.** Choose this option to consider new buckets non-compliant. With this option selected, the first CheckIt establishes the baseline bucket list. New buckets are non-compliant until allowed. (A Policy can be defined on “allowed” buckets.)

  > **NOTE:** A 'not allowed' icon ⊘ under the Compliant column in the Manage Service Buckets screen for the account identifies buckets that are not allowed. You can click ⊕ (Add to Baseline) on this screen to add an exception to the 'not allowed' list for a particular bucket.

- **New buckets allowed.** New buckets are allowed upon which a Policy can be defined.

Bucket Deleted Option

If Enable AWS S3 Policy is checked, these options are available. These options control how Security Auditor reacts when buckets are deleted from the AWS account.

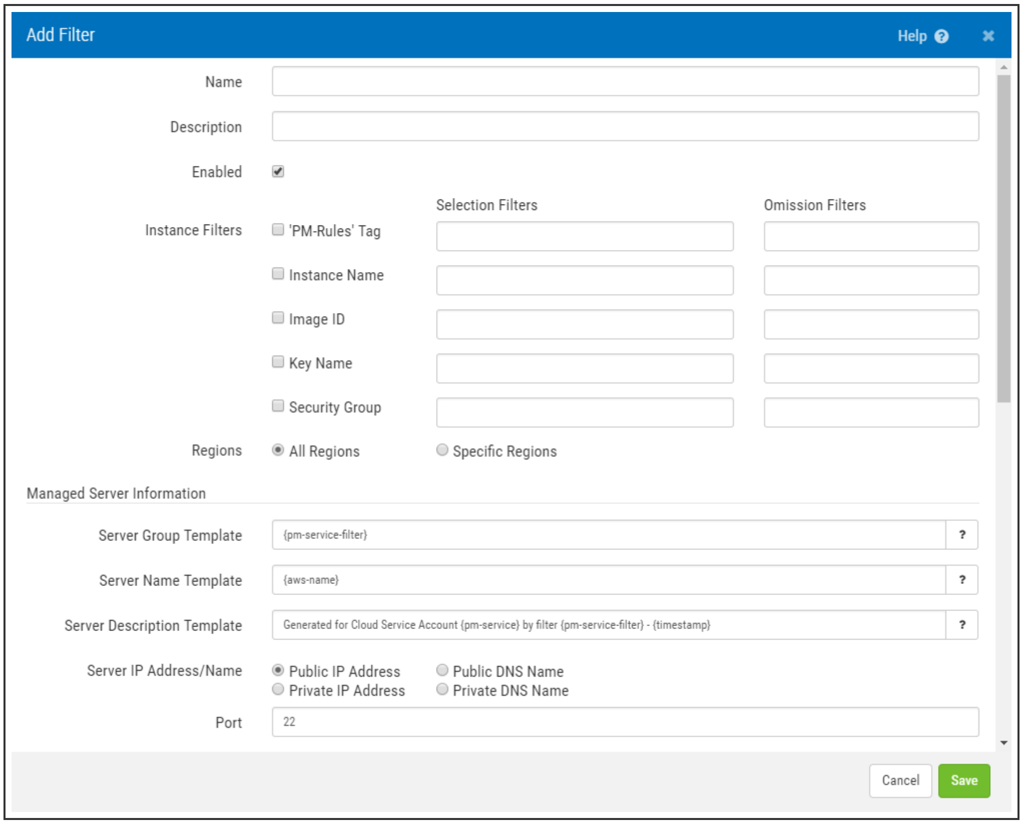
- **Deleted buckets are Compliant.** Choose this option to consider buckets deleted from the account compliant.
- **Deleted buckets are Not Compliant.** Choose this option to consider buckets deleted from the account not compliant.

- **Deleted buckets are removed from Security Auditor.** Choose this option to remove buckets deleted from the AWS account from Security Auditor as well.

Shared Bucket Policy

Select a Shared Bucket Policy object that will be assigned to buckets when they are found in the account.

Add/Edit Filter



Name

Description

Enabled ☑

Instance Filters

	Selection Filters	Omission Filters
□ 'PM-Rules' Tag		
□ Instance Name		
□ Image ID		
□ Key Name		
□ Security Group		

Regions ● All Regions ○ Specific Regions

Managed Server Information

Server Group Template: {pm-service-filter}

Server Name Template: {aws-name}

Server Description Template: Generated for Cloud Service Account {pm-service} by filter {pm-service-filter} - {timestamp}

Server IP Address/Name: ● Public IP Address ○ Public DNS Name ○ Private IP Address ○ Private DNS Name

Port: 22

How to Get There

Create a new Cloud Service Account in the Manage AWS Cloud Service Accounts screen. Click (Edit Filters).

What it Does

Security Auditor uses the Filter settings to create Managed Servers for the discovered instances automatically.

Options

Name

The name of the Filter. Since a Filter can only add servers to a single group, and a group must contain instances of the same Linux distribution, consider including the distribution in the name of the filter.

Description

The description of the Filter.

Enabled

Check this box to use the Filter settings to create Managed Servers.

Instance Filters; Selection Filters • Omission Filters

Filters allow you to identify the server instances you would like to add automatically during polling. Use the Selection Filters column to identify the server instance to add, and the Omission Filters column to identify the server instances to omit. For each enabled filter attribute, the Selection filters are processed first, then the Omission filters remove omitted instances from the results. When multiple filter attributes are selected, only server instances that match *every* enabled attribute filter are selected. Instances are selected or omitted when *any* one of the selection/omission values are met.

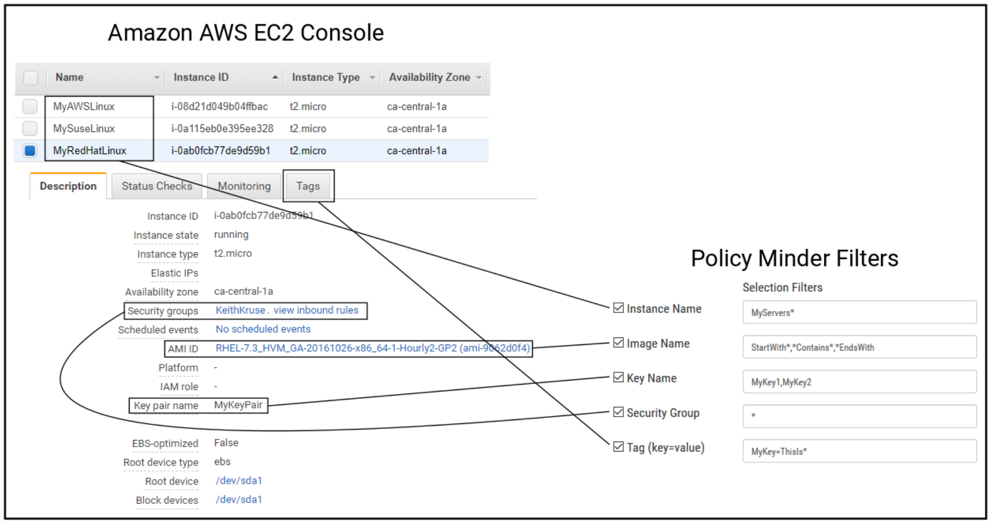
Use the following to help specify server instances by Instance Name, Image Name, Key Name, and Security Group:

- Select all instances with * (asterisk).
- Use * as a wildcard character (StartsWith*).
- Separate multiple values with a comma (StartsWithA*, *EndsWithB, *ContainsC*).

Use the following to help specify server instances by Tag:

- The Tag Filter format is TagKey=TagValue.
- Select all instances with TagKey=*.
- Supports * (any string) and ? (any character) wildcards and multiple comma separated selections (TagA=StartsWithA*, TagB=*EndWithB,TagC=*ContainsC*).

NOTE: The filters comparison is not case sensitive.



Amazon AWS EC2 Console

☐	Name	Instance ID	Instance Type	Availability Zone
☐	MyAWSLinux	i-08d21d049b04ffbac	t2.micro	ca-central-1a
☐	MySuseLinux	i-0a115eb0e395ee328	t2.micro	ca-central-1a
■	MyRedHatLinux	i-0ab0fcb77de9d59b1	t2.micro	ca-central-1a

Instance ID	i-0ab0fcb77de9d59b1
Instance state	running
Instance type	t2.micro
Elastic IPs	
Availability zone	ca-central-1a
Security groups	KeithKruse . view inbound rules
Scheduled events	No scheduled events
AMI ID	RHEL-7.3_HVM_GA-20161026-x86_64-1-Hourly2-GP2 (ami-9062d0f4)
Platform	-
IAM role	-
Key pair name	MyKeyPair
EBS-optimized	False
Root device type	ebs
Root device	/dev/sda1
Block devices	/dev/sda1

Policy Minder Filters

	Selection Filters
☑ Instance Name	MyServers*
☑ Image Name	StartWith*,*Contains*,*EndsWith
☑ Key Name	MyKey1,MyKey2
☑ Security Group	*
☑ Tag (key=value)	MyKey=ThisIs*

- **Instance Name.** Use this field to identify server instances by the Name of the AWS instance, if defined. If no Name is defined, and a value is entered here, Security Auditor looks for the Instance ID.

- **Image Name.** Use this field to identify server instances by the Image Name. In Amazon AWS, this is listed as the AMI ID.
- **Key Name.** Use this field to identify server instances by the Key Pair Name.
- **Security Group.** The Security Group assigned to the instance.
- **Tag (key=value).** Use this field to identify server instances with Tags.

Regions; All Regions • Specific Regions

Choose **All Regions** to perform the filter comparison for all Amazon AWS server regions. Choose **Specific Regions** to identify the regions to perform the filter comparison. Choose the minimum number of required regions for optimal performance.

Managed Server Information

Server Group Template

The name of the Server Group that discovered servers will be assigned to. Aim to include servers that share policies in the same Group in order to reduce the number of policies that must be defined. Supports the following variables:

- {aws-key}
- {aws-security-group}
- {pm-service}
- {pm-service-filter}
- {os}

Server Name Template

The unique name of the Managed Servers created for discovered servers. Supports the following variables:

- 'Server Group Template' variables
- {server-group}
- {aws-name}
- {aws-instance-id}
- {aws-private-ip}
- {aws-public-ip}
- {aws-public-dns}
- {aws-private-dns}
- {host-name}

Server Description Template

The Description of the Managed Servers created for discovered servers. Supports the following variables:

- 'Server Name Template' variables
- {server-name}
- {date}
- {time}
- {timestamp}

Server IP Address/Name; Public IP Address • Public DNS Name • Private IP Address • Private DNS Name

Specify whether the managed server uses a Public/Private IP Address/DNS Name.

Port

The ssh port - default is port 22. (Unix-based servers.)

Installation Connection Information

Installation Connection Information is needed to initially access the server to configure future connections (See 'Installation Configuration' below). The servers are accessed using this information only when the server is initially added as a Managed Server.

Installation User Name

The user name used for installation.

Authenticate With; Password • Managed Key

Choose **Password** and enter the password if you are using a password for authentication.

Choose **Managed Key** to select an existing Managed Key. Managed Private Keys are created and managed using **Admin Tasks > Manage Private Keys**. See Manage Private Keys.

Elevate Permission With; sudo • su • Do Not Elevate

Use this drop-down to specify whether or not you would like to elevate permissions, and the method for doing so (sudo or su).

Authorization Password

This is the password required to elevate permissions. If no password is required this field may be left blank.

Installation Configuration

Installation will create the user and group below, create public/private key pair allowing the Security Auditor console ssh access as that user, and update the sudo configuration to allow that user authority to perform commands required for Security Auditor's agentless access.

Security Auditor User • Specify UID

A user with this name will be created on the managed server and used by Security Auditor for agentless control.

Security Auditor Group • Specify GID

A group with this name will be created on the managed server and used by Security Auditor for agentless control.

sudoers file • Use sudoers d

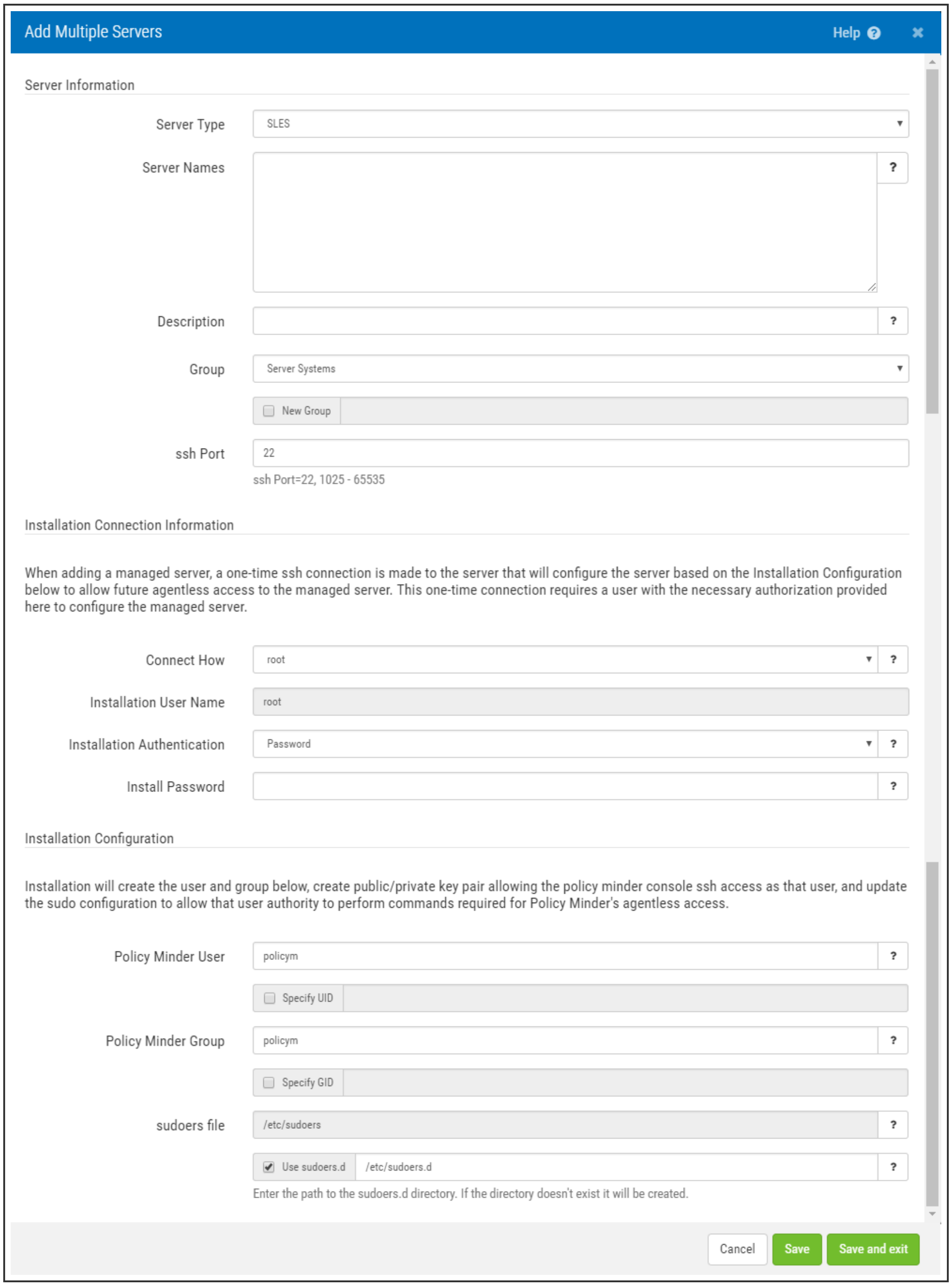
Enter the path to the sudoers file where sudo config is located. If 'Use sudoers.d' is checked then the necessary sudoers additions for the Security Auditor user to execute commands via sudo will be placed in a new file in the sudoers.d directory (this is a best practice). If unchecked then the necessary changes will be appended to the sudoers file.

Cancel • Save

Choose **Cancel** to dismiss the screen without saving changes. Choose **Save** to save changes and return to the Manage Filters screen.

Add Multiple Servers screen

Use this screen to add multiple servers at once. When new managed servers are added, Security Auditor makes an ssh connection, creates a group, user and ssh keys, and configures sudo so that the new server can be managed by Security Auditor's agentless control.



Server Information

Server Type: SLES

Server Names:

Description:

Group: Server Systems

□ New Group

ssh Port: 22

ssh Port=22, 1025 - 65535

Installation Connection Information

When adding a managed server, a one-time ssh connection is made to the server that will configure the server based on the Installation Configuration below to allow future agentless access to the managed server. This one-time connection requires a user with the necessary authorization provided here to configure the managed server.

Connect How: root

Installation User Name: root

Installation Authentication: Password

Install Password:

Installation Configuration

Installation will create the user and group below, create public/private key pair allowing the policy minder console ssh access as that user, and update the sudo configuration to allow that user authority to perform commands required for Policy Minder's agentless access.

Policy Minder User: policym

□ Specify UID

Policy Minder Group: policym

□ Specify GID

sudoers file: /etc/sudoers

☑ Use sudoers.d: /etc/sudoers.d

Enter the path to the sudoers.d directory. If the directory doesn't exist it will be created.

How to get there

Choose **Servers > Add Multiple Servers**.

Server Information

Server Type

Here, choose the OS of the servers you are adding.

Server Names

Specify one or more names that can be used as a server and DNS name:

- MyServer or
- 192.168.11

or a server@dnsname combination name:

- MyServer@192.168.1.1 or
- MyServer@DNSName.com

Multiple names are delimited by separate lines or semicolons

- Server1; Server2; Server3@192.168.1.1

Dynamic names can be specified, such as

- Server[1-100]
- Server[001-100]
- Server[a,b,c,x,z]
- Server[10,15-20,35]
- MyServer@192.168.‘l.[1-10]

Description

A description of the servers can be added here.

Description Variables:

- {name}
- {nameoripaddress}
- {servertype}
- {hostname}

Group • New Group

Choose a group from this drop-down list to assign the server to one of Security Auditor's Groups. Check New Group and type the name of the new Group in the adjacent text box to add a new one. Organizing servers into Groups can help you more easily view and manage servers as you work with policies and compliance. A sever can only be assigned to one group.

ssh Port

The ssh port - default is port 22. (Unix-based servers.)

Installation Information

Connect How

If root is selected then install will be performed as root. If "su" is selected, before installation begins the install program will log on using the user and password given and then su to root with the password given. If "sudo" is selected, install will be performed as a user who can execute admin commands using sudo (with their own password).

Installation User Name

If "root" is selected for Connect How, "root" appears here. Choose "su" or "sudo" for Connect How to enter the name you would like to use for product installation on the server.

Installation Authentication

The authentication method must be specified for the Installation User.

- **Password** If this option is selected, you must provide the password required for the Installation User.
- **Private key** If this option is selected, you must paste or type the contents of a private key file (.pem).
- **Private key .pem file** If this option is selected, you must select a .pem file from the file system.
- **Managed Private Key** If this option is selected you must select a Private Key defined under the 'Admin Tasks' menu.

Install Password

Password is used only for install and is not saved. If the console is not configured for https (see manual) then the password will be sent clear text one time from browser to server.

Security Auditor User • Specify UID

A user with this name will be created on the managed server and used by Security Auditor for agentless control.

Security Auditor Group • Specify GID

A group with this name will be created on the managed server and used by Security Auditor for agentless control.

sudoers file • Use sudoers d

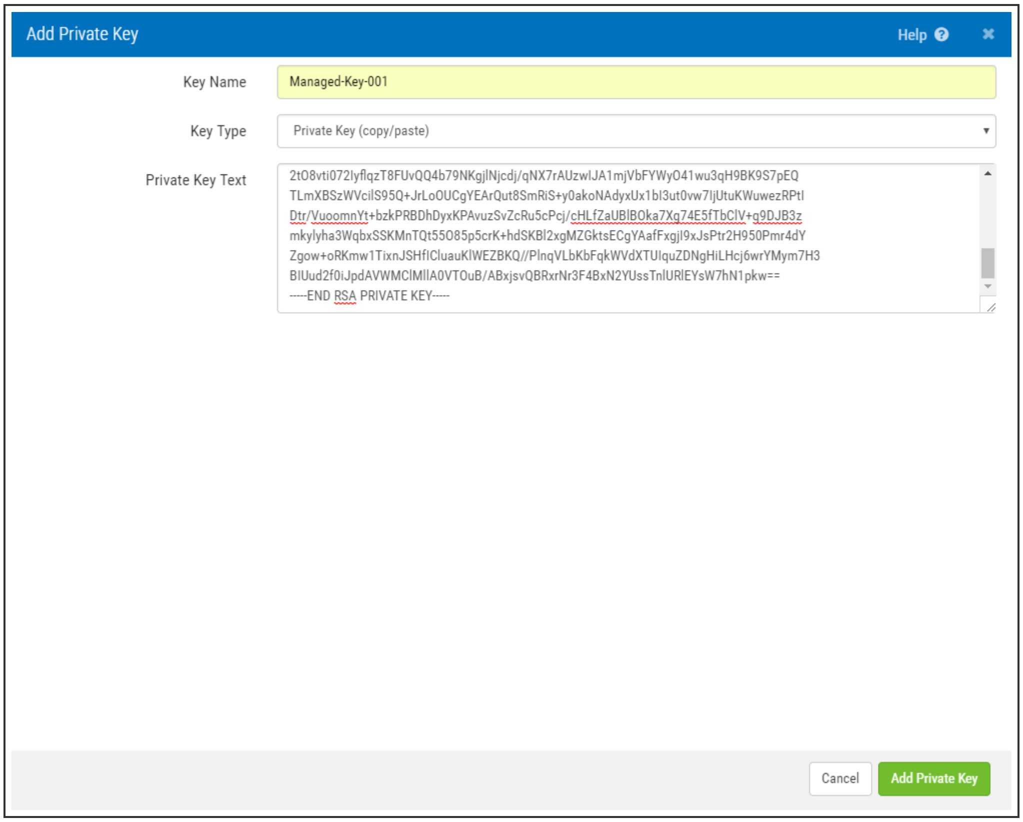
Enter the path to the sudoers file where sudo config is located. If 'Use sudoers.d' is checked then the necessary sudoers additions for the Security Auditor user to execute commands via sudo will be placed in a new file in the sudoers.d directory (this is a best practice). If unchecked then the necessary changes will be appended to the sudoers file.

Cancel • Save

Click **Cancel** to dismiss this screen without making changes. Click **Save** to save the current settings without dismissing the screen. Click **Save and exit** to save the current settings and dismiss the screen.

Add/Modify Private Key

Use this screen to add one or more private keys in order to connect to a managed server with SSH.



Key Name: Managed-Key-001

Key Type: Private Key (copy/paste)

Private Key Text:

```
2tO8vti072IyflqzT8FUvQQ4b79NKgjlNjcdj/qNX7rAUzwIJA1mjVbFYWyO41wu3qH9BK9S7pEQ
TLmXBSzWVcilS95Q+JrLoOUCgYEArQut8SmRiS+y0akoNAdyxUx1bl3ut0vw7IjUtuKWuwezRPtI
Dtr/VuoomnYt+bzkPRBDhDyxKPAvuzSvZcRu5cPcj/cHLfZaUBlBOka7Xg74E5fTbClV+g9DJB3z
mkylyha3WqbxSSKMnTQt55O85p5crK+hdSKBl2xgMZGktsECgYAafFxgjl9xJsPtr2H950Pmr4dY
Zgow+oRKmw1TixnJSHfICluauKlWEZBKQ//PlnqVLbKbFqkWVdXTUIquZDNgHiLHcj6wrYMym7H3
BIUud2f0iJpdAVWMClMllA0VTOuB/ABxjsvQBRxrNr3F4BxN2YUssTnlURlEYsW7hN1pkw==
-----END RSA PRIVATE KEY-----
```

How to Get There

On the Manage Private Keys screen, click **Add Private Key**.

Options

Key Name

Enter the name of the key. This is the label that will be used to identify the key in the future.

Key Type

- **Private Key (Copy/Paste):** Choose this option to paste the private key text in the window below.
- **Private Key .pem File (Browse):** Choose this option to choose the .pem file containing the private key from your file system.

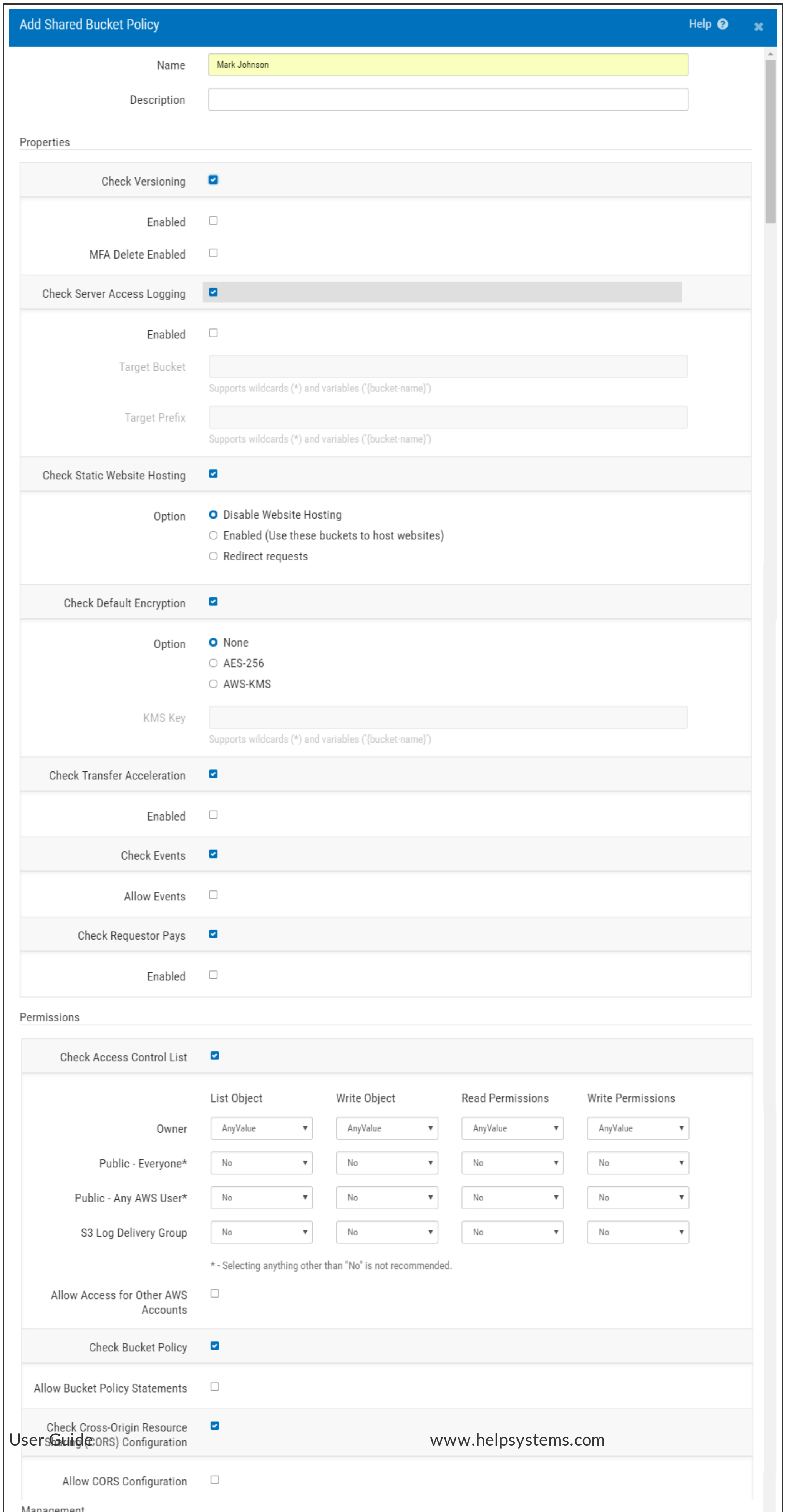
Private Key Text • Private Key File; Choose File

If Private Key (copy/paste) is selected, paste the test of the private key in this text box. If Private Key .pem File (Browse) is selected, click **Choose File** to select the file containing the private key.

Cancel • Add Private Key

Click **Cancel** to dismiss the screen without making changes. Click **Add Private Key** to load the private key into Security Auditor's database.

Add/Modify Shared Bucket Policy



Add Shared Bucket Policy

Name: Mark Johnson

Description:

Properties

Check Versioning ☑

Enabled □

MFA Delete Enabled □

Check Server Access Logging ☑

Enabled □

Target Bucket:

Supports wildcards (*) and variables ('{bucket-name}')

Target Prefix:

Supports wildcards (*) and variables ('{bucket-name}')

Check Static Website Hosting ☑

Option
- ● Disable Website Hosting
- ○ Enabled (Use these buckets to host websites)
- ○ Redirect requests

Check Default Encryption ☑

Option
- ● None
- ○ AES-256
- ○ AWS-KMS

KMS Key:

Supports wildcards (*) and variables ('{bucket-name}')

Check Transfer Acceleration ☑

Enabled □

Check Events ☑

Allow Events □

Check Requestor Pays ☑

Enabled □

Permissions

Check Access Control List ☑

	List Object	Write Object	Read Permissions	Write Permissions
Owner	AnyValue	AnyValue	AnyValue	AnyValue
Public - Everyone*	No	No	No	No
Public - Any AWS User*	No	No	No	No
S3 Log Delivery Group	No	No	No	No

* - Selecting anything other than "No" is not recommended.

Allow Access for Other AWS Accounts □

Check Bucket Policy ☑

Allow Bucket Policy Statements □

Check Cross-Origin Resource Sharing (CORS) Configuration ☑

Allow CORS Configuration □

Management

How to Get There

On the Manage Shared Bucket policy screen, click **Add**, or click an existing shared policy to edit it.

What it Does

Use this screen to add or edit an AWS S3 Shared Bucket Policy. Security Auditor includes a *DEFAULT Shared Bucket Policy that includes standard default settings for S3 buckets. Shared Bucket Policies include many (but not all) S3 bucket settings so that the same shared policy can be used to check many S3 buckets. Where individual buckets or settings within buckets should differ from a Shared bucket policy a Private Policy would be used, overriding the Shared Bucket Policy.

Options

Name

The name of the shared bucket policy.

Description

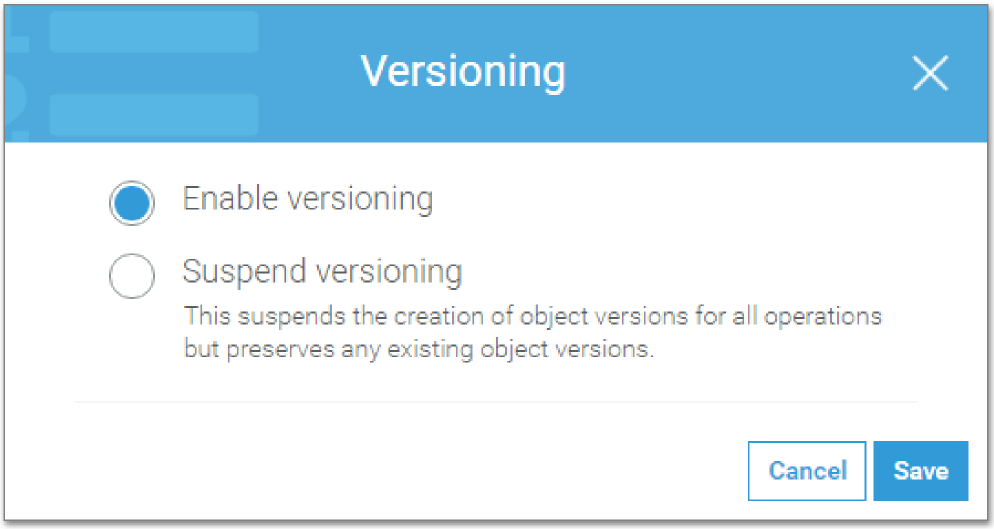
The description of the shared bucket policy.

Properties

The following Amazon S3 Bucket properties can be configured in a Shared Bucket Policy.

> **NOTE:** See the Amazon S3 help for complete details regarding these S3 Bucket properties.

Check Versioning; Enabled • Disabled • MFA Delete Enabled



Versioning

● Enable versioning

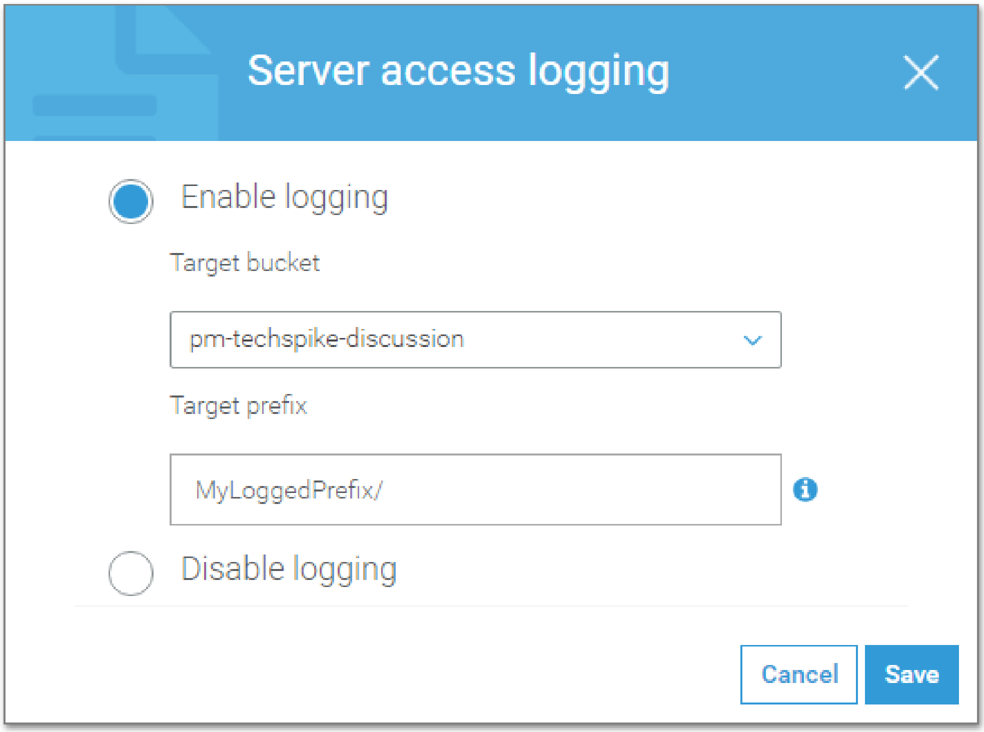
○ Suspend versioning

This suspends the creation of object versions for all operations but preserves any existing object versions.

Select **Check Versioning** to include the S3 Bucket's Versioning setting as part of the Shared Bucket Policy. If checked, the subsequent options become active.

If selected, choose **Enabled** to indicate that the 'Enable Versioning' setting is compliant with the policy. Uncheck **Enabled** to indicate the 'Suspended Versioning' setting is compliant with the policy. Select **MFA Delete Enabled** to indicate the MFA Delete setting must be enabled in order to be compliant with the policy (available for AWS administrators).

Check Server Access Logging; Enabled • Target Bucket • Target Prefix



Server access logging

● Enable logging

Target bucket

pm-techspike-discussion

Target prefix

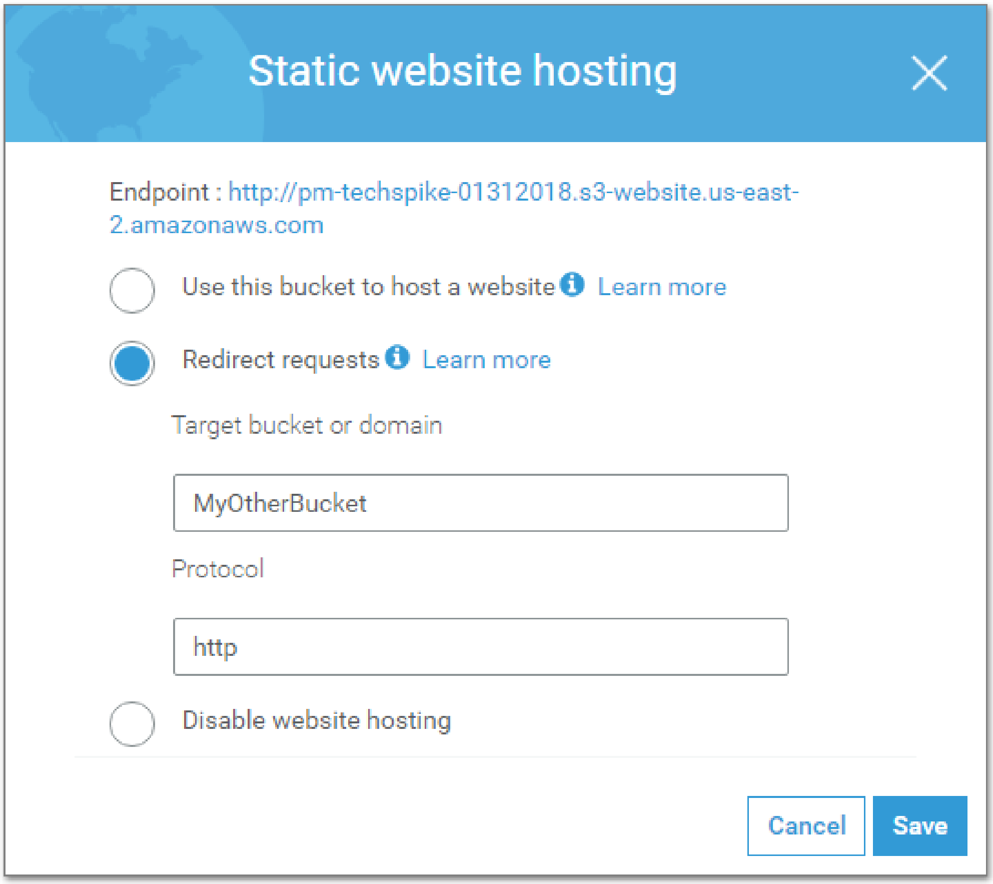
MyLoggedPrefix/

○ Disable logging

Select **Check Server Access Logging** to include the S3 Bucket's Server Access Logging settings as part of the Shared Bucket Policy. If checked, the subsequent options become active.

Check **Enabled** to indicate the 'Enable Logging' setting must be chosen in order order to be compliant with the policy. Uncheck **Enabled** to indicate 'Disable Logging' must be selected in order to be compliant. You can also specify a Target Bucket or Target Prefix as part of your policy requirements. Both fields support wildcards (*) and variables ('{bucket-name}').

Check Static Website Hosting; Disable Website Hosting • Enabled (Use these buckets to host websites) • Redirect requests


Static website hosting

Endpoint : http://pm-techspike-01312018.s3-website.us-east-2.amazonaws.com

○ Use this bucket to host a website Learn more

● Redirect requests Learn more

Target bucket or domain: MyOtherBucket

Protocol: http

○ Disable website hosting

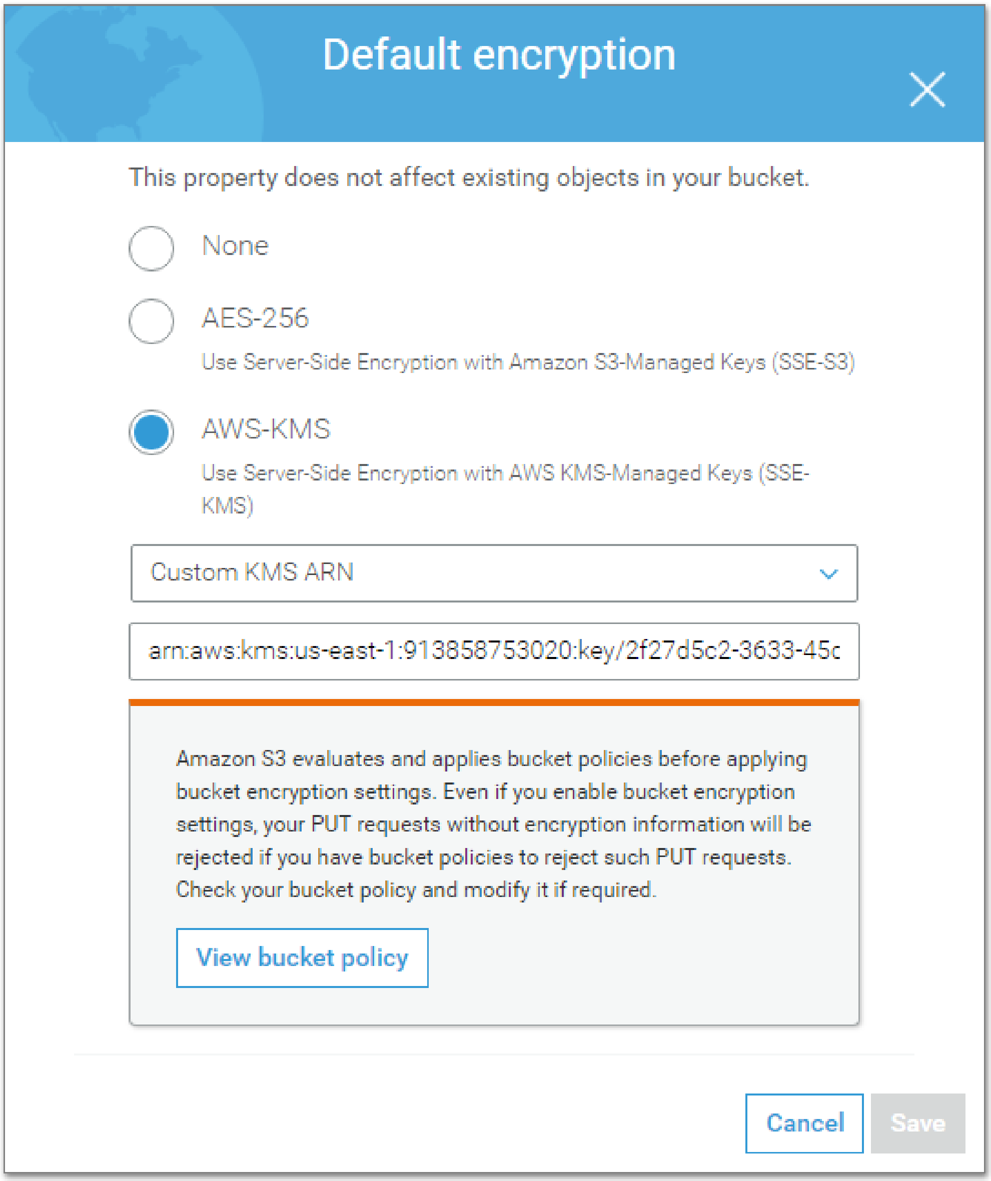
Select **Check Static Website Hosting** to include the S3 Bucket's Static Website Hosting settings as part of the Shared Bucket Policy. If checked, the subsequent options become active.

Choose **Disable Website Hosting** to specify disabled hosting as a policy requirement.

Choose **Enabled** to specify the 'Use These Buckets to Host Websites' setting as a policy requirement.

Choose **Redirect Requests** to specify the 'Redirect Requests' setting as a policy requirement.

Check Default Encryption; None • AES-256 • AWS-KMS • KMS Key



Default encryption

This property does not affect existing objects in your bucket.

○ None

○ AES-256

Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

● AWS-KMS

Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Custom KMS ARN

arn:aws:kms:us-east-1:913858753020:key/2f27d5c2-3633-45c

Amazon S3 evaluates and applies bucket policies before applying bucket encryption settings. Even if you enable bucket encryption settings, your PUT requests without encryption information will be rejected if you have bucket policies to reject such PUT requests. Check your bucket policy and modify it if required.

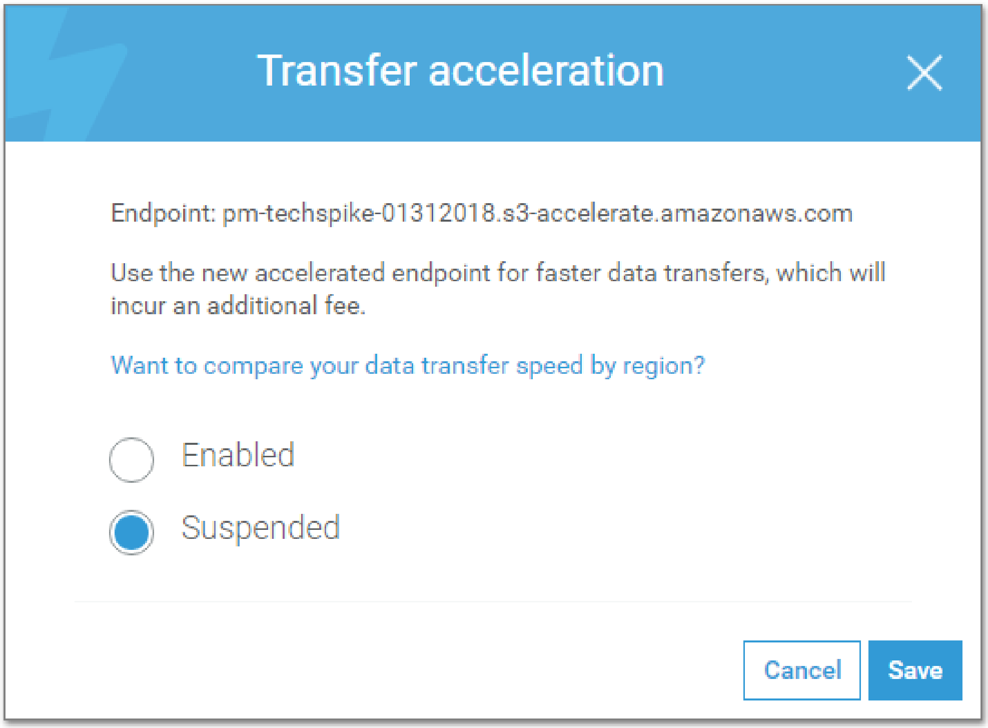
Select **Check Default Encryption** to include the S3 Bucket's Default Encryption settings as part of the Shared Bucket Policy. If checked, the subsequent encryption options becomes active.

Choose **None** to specify no encryption as a policy requirement.

Choose **AES-256** to specify AES-256 encryption as a policy requirement.

Choose **AWS-KMS** to specify AWS-KMS encryption as a policy requirement. If selected, the subsequent KMS Key text box becomes active, which allows you to specify a KMS Key as part of the policy.

Check Transfer Accelleration



Transfer acceleration

Endpoint: pm-techspike-01312018.s3-accelerate.amazonaws.com

Use the new accelerated endpoint for faster data transfers, which will incur an additional fee.

Want to compare your data transfer speed by region?

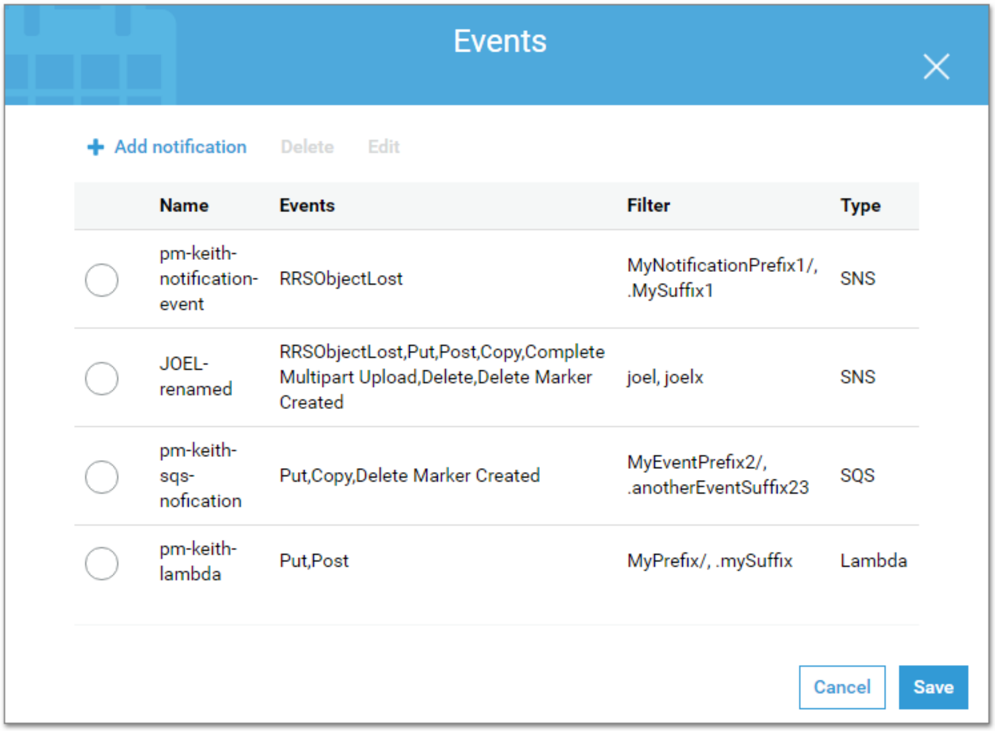
○ Enabled

● Suspended

Select **Check Transfer Acceleration** to include the S3 Bucket's Transfer Acceleration setting as part of the Shared Bucket Policy. If checked, the subsequent Enabled check box becomes active.

Check **Enabled** to specify the 'Enabled' setting as a policy requirement.

Check Events

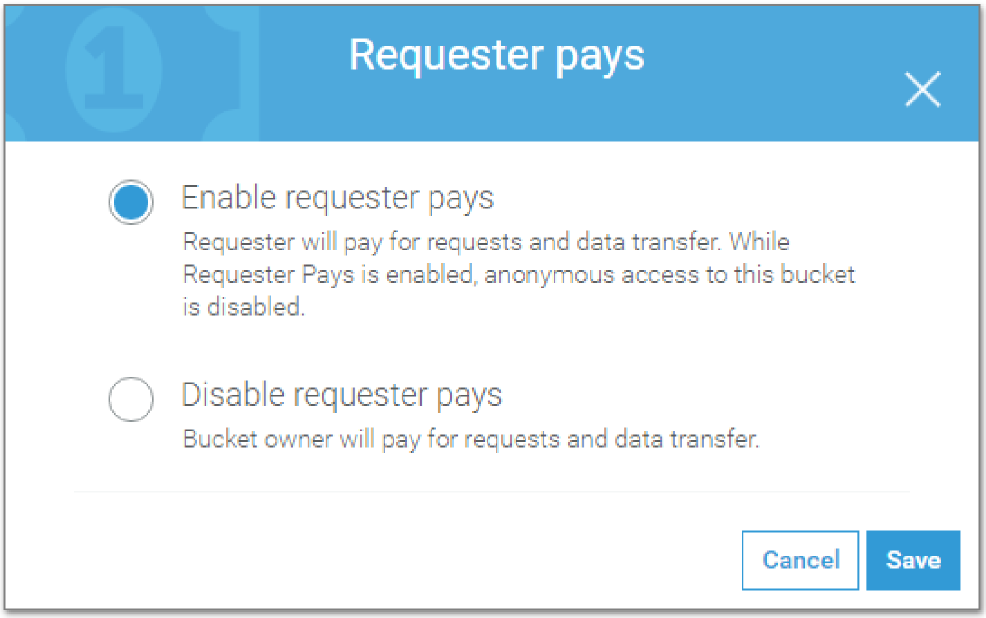


	Name	Events	Filter	Type
○	pm-keith-notification-event	RRSObjectLost	MyNotificationPrefix1/, .MySuffix1	SNS
○	JOEL-renamed	RRSObjectLost,Put,Post,Copy,Complete Multipart Upload,Delete,Delete Marker Created	joel, joelx	SNS
○	pm-keith-sqs-nofication	Put,Copy,Delete Marker Created	MyEventPrefix2/, .anotherEventSuffix23	SQS
○	pm-keith-lambda	Put,Post	MyPrefix/, .mySuffix	Lambda

Select **Check Events** to include the S3 Bucket's Events as part of the Shared Bucket Policy. If checked, the subsequent Allow Events check box becomes active.

Check **Allow Events** in order for events to be allowed as part of the policy. If Allow Events is unchecked, the existence of one or more events will result in a policy failure.

Requester Pays



● Enable requester pays

Requester will pay for requests and data transfer. While Requester Pays is enabled, anonymous access to this bucket is disabled.

○ Disable requester pays

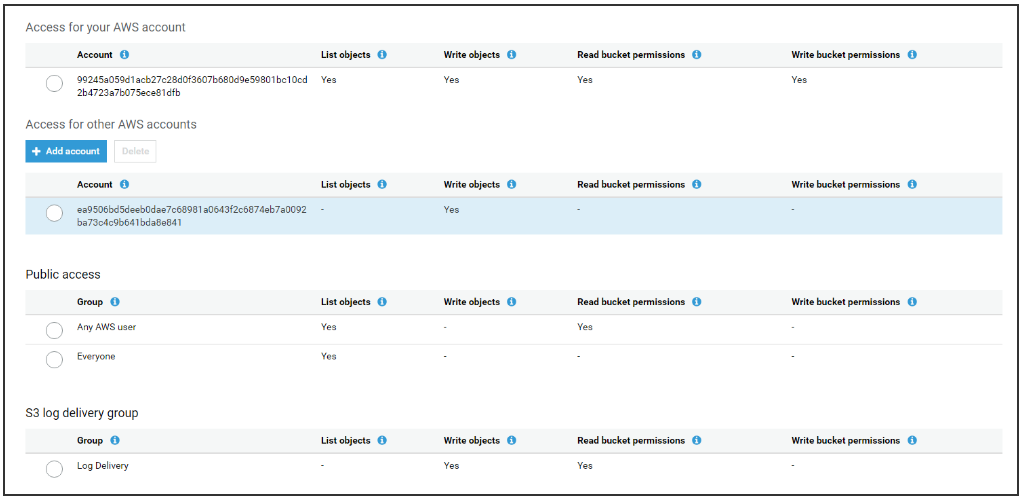
Bucket owner will pay for requests and data transfer.

Select **Check Requester** to include the S3 Bucket's Events as part of the Shared Bucket Policy. If checked, the subsequent Allow Events check box becomes active.

Permissions

Check Access Control List

Select **Check Access Control List** to include the S3 Access settings as part of your policy. Once selected, the subsequent access matrix settings are activated.



Access for your AWS account

	Account	List objects	Write objects	Read bucket permissions	Write bucket permissions
○	99245a059d1acb27c28d0f3607b680d9e59801bc10cd 2b4723a7b075ece81dfb	Yes	Yes	Yes	Yes

Access for other AWS accounts

	Account	List objects	Write objects	Read bucket permissions	Write bucket permissions
○	ea9506bd5deeb0dae7c68981a0643f2c6874eb7a0092 ba73c4c9b641bda8e841	-	Yes	-	-

Public access

	Group	List objects	Write objects	Read bucket permissions	Write bucket permissions
○	Any AWS user	Yes	-	Yes	-
○	Everyone	Yes	-	-	-

S3 log delivery group

	Group	List objects	Write objects	Read bucket permissions	Write bucket permissions
○	Log Delivery	-	Yes	Yes	-

> **NOTE:** Refer to the ℹ icons in the AWS S3 Access Control List page for a description of these settings.

For each item in the matrix, you can select one of the following options.

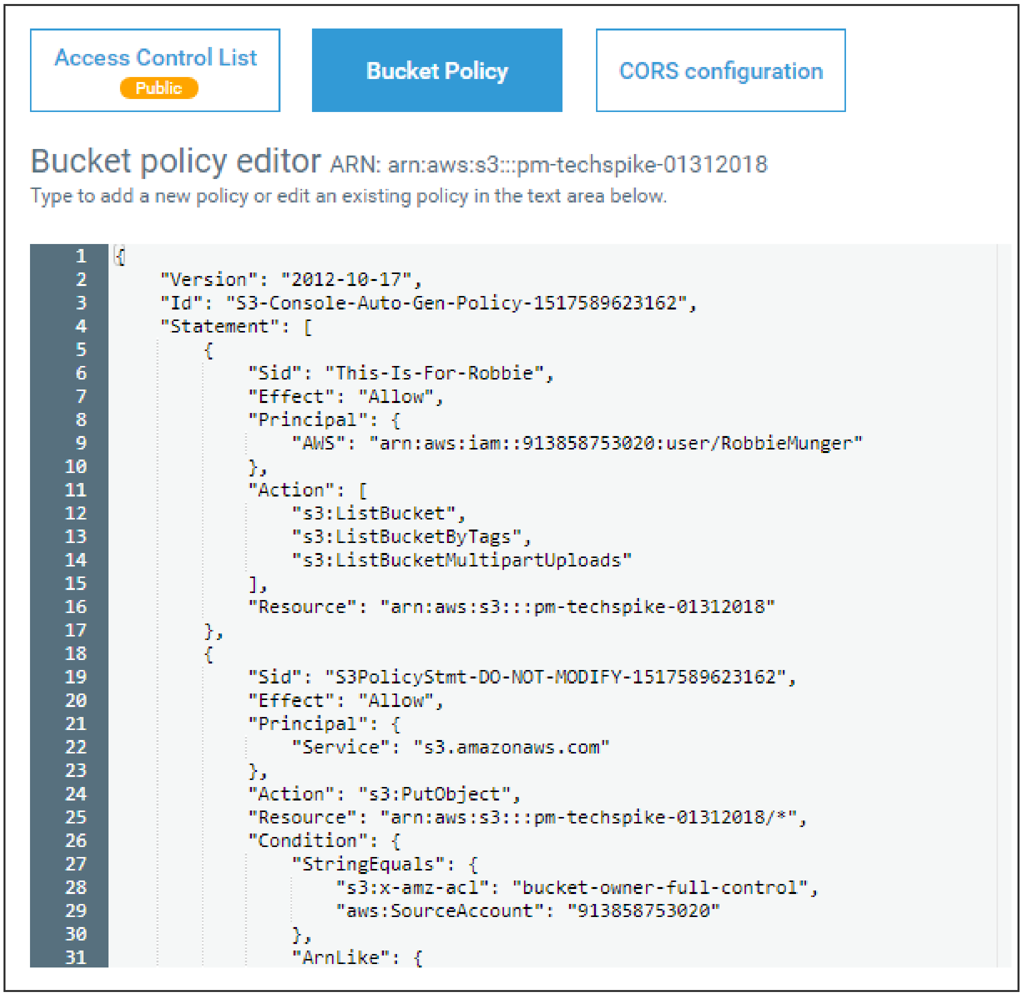
- **AnyValue:** Choose **AnyValue** to indicate the setting is always compliant, regardless of its state.
- **Yes:** Choose **Yes** to indicate the item must be set to "Yes" in order to be compliant.
- **No:** Choose **No** to indicate the item must be set to "No" in order to be compliant.

> **NOTE:** For the "Public - Everyone" and "Public - Any AWS User" rows, selecting anything other than "No" is not recommended.

Allow Access for Other AWS Accounts

Check this option to permit Other AWS Accounts in your policy. If this option is unchecked, Other AWS Accounts in the S3 bucket are non-compliant.

Check Bucket Policy



Bucket policy editor ARN: arn:aws:s3:::pm-techspike-01312018

Type to add a new policy or edit an existing policy in the text area below.

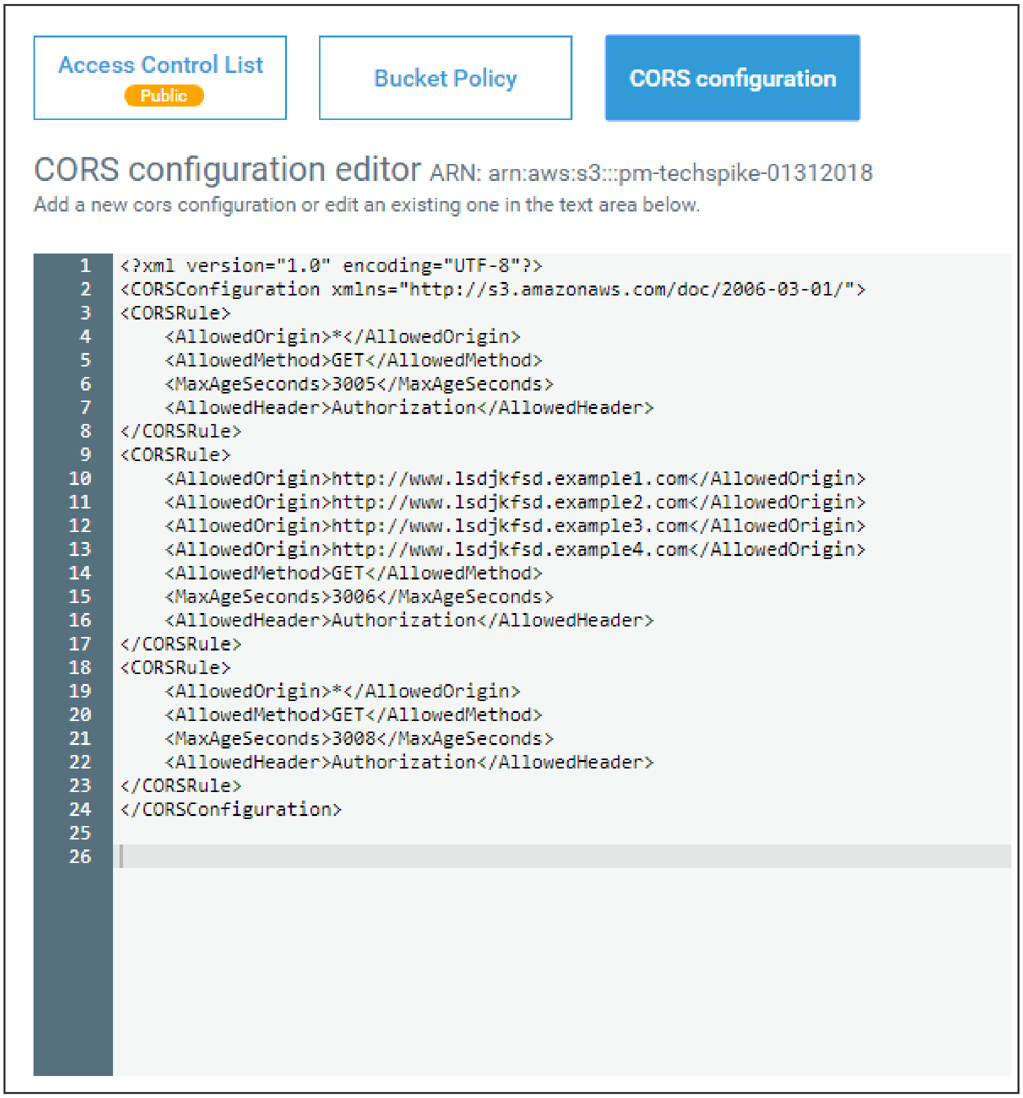
```
{
    "Version": "2012-10-17",
    "Id": "S3-Console-Auto-Gen-Policy-1517589623162",
    "Statement": [
        {
            "Sid": "This-Is-For-Robbie",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::913858753020:user/RobbieMunger"
            },
            "Action": [
                "s3:ListBucket",
                "s3:ListBucketByTags",
                "s3:ListBucketMultipartUploads"
            ],
            "Resource": "arn:aws:s3:::pm-techspike-01312018"
        },
        {
            "Sid": "S3PolicyStmt-DO-NOT-MODIFY-1517589623162",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::pm-techspike-01312018/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": "913858753020"
                },
                "ArnLike": {
```

Select **Check Bucket Policy** to include Bucket Policy Statements text as part of your policy. If checked, the subsequent option becomes active.

Allow Bucket Policy Statements

Check this option to permit Bucket Policy Statements in your policy. If this option is unchecked, Bucket policy Statements in the S3 bucket are non-compliant.

Check Cross-Origin Resource Sharing (CORS) Configuration



CORS configuration editor ARN: arn:aws:s3:::pm-techspike-01312018

Add a new cors configuration or edit an existing one in the text area below.

```
<?xml version="1.0" encoding="UTF-8"?>
<CORSConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
<CORSRule>
    <AllowedOrigin>*</AllowedOrigin>
    <AllowedMethod>GET</AllowedMethod>
    <MaxAgeSeconds>3005</MaxAgeSeconds>
    <AllowedHeader>Authorization</AllowedHeader>
</CORSRule>
<CORSRule>
    <AllowedOrigin>http://www.lsdjkfsd.example1.com</AllowedOrigin>
    <AllowedOrigin>http://www.lsdjkfsd.example2.com</AllowedOrigin>
    <AllowedOrigin>http://www.lsdjkfsd.example3.com</AllowedOrigin>
    <AllowedOrigin>http://www.lsdjkfsd.example4.com</AllowedOrigin>
    <AllowedMethod>GET</AllowedMethod>
    <MaxAgeSeconds>3006</MaxAgeSeconds>
    <AllowedHeader>Authorization</AllowedHeader>
</CORSRule>
<CORSRule>
    <AllowedOrigin>*</AllowedOrigin>
    <AllowedMethod>GET</AllowedMethod>
    <MaxAgeSeconds>3008</MaxAgeSeconds>
    <AllowedHeader>Authorization</AllowedHeader>
</CORSRule>
</CORSConfiguration>
```

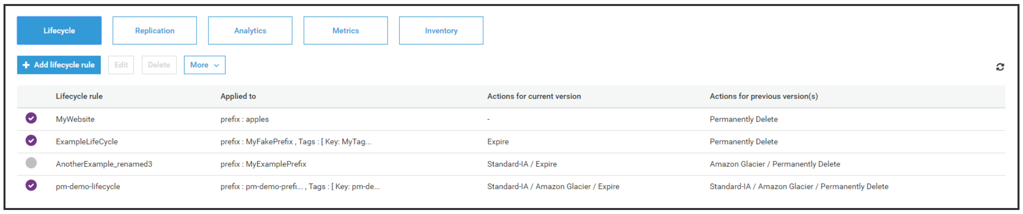
Select **Check Cross-Origin Resource Sharing (CORS) Configuration** to include CORS Configuration as part of your policy. If checked, the subsequent option becomes active.

Allow CORS Configuration

Check this option to permit CORS Configuration rules in your policy. If this option is unchecked, CORS rules in the S3 bucket are non-compliant.

Management

Check Lifecycle



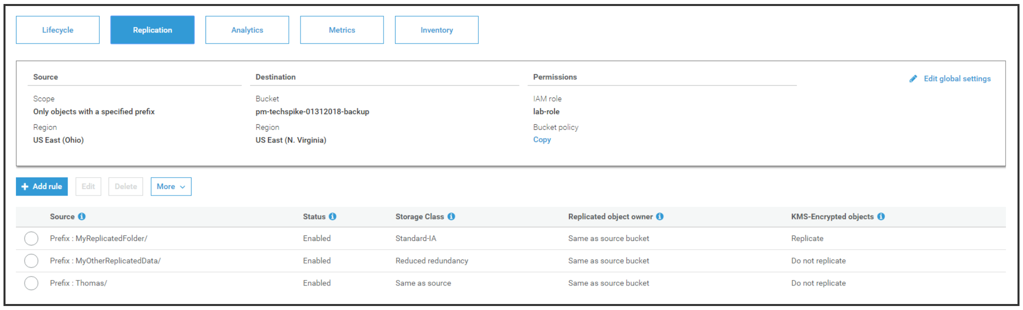
	Lifecycle rule	Applied to	Actions for current version	Actions for previous version(s)
✓	MyWebsite	prefix : apples	-	Permanently Delete
✓	ExampleLifeCycle	prefix : MyFakePrefix , Tags : [Key: MyTag...	Expire	Permanently Delete
●	AnotherExample_renamed3	prefix : MyExamplePrefix	Standard-IA / Expire	Amazon Glacier / Permanently Delete
✓	pm-demo-lifecycle	prefix : pm-demo-prefi... , Tags : [Key: pm-de...	Standard-IA / Amazon Glacier / Expire	Standard-IA / Amazon Glacier / Permanently Delete

Select **Check Lifecycle** to include the AWS S3 Lifecycle setting in your policy. If checked, the subsequent option becomes active.

Allow Lifecycle Rules

Check this option to permit Lifecycle Rules in your policy. If this option is unchecked, Lifecycle Rules in the S3 bucket are non-compliant.

Check Replication



Source

Scope
Only objects with a specified prefix
Region
US East (Ohio)

Destination

Bucket
pm-techspike-01312018-backup
Region
US East (N. Virginia)

Permissions

IAM role
lab-role
Bucket policy
Copy

	Source	Status	Storage Class	Replicated object owner	KMS-Encrypted objects
○	Prefix : MyReplicatedFolder/	Enabled	Standard-IA	Same as source bucket	Replicate
○	Prefix : MyOtherReplicatedData/	Enabled	Reduced redundancy	Same as source bucket	Do not replicate
○	Prefix : Thomas/	Enabled	Same as source	Same as source bucket	Do not replicate

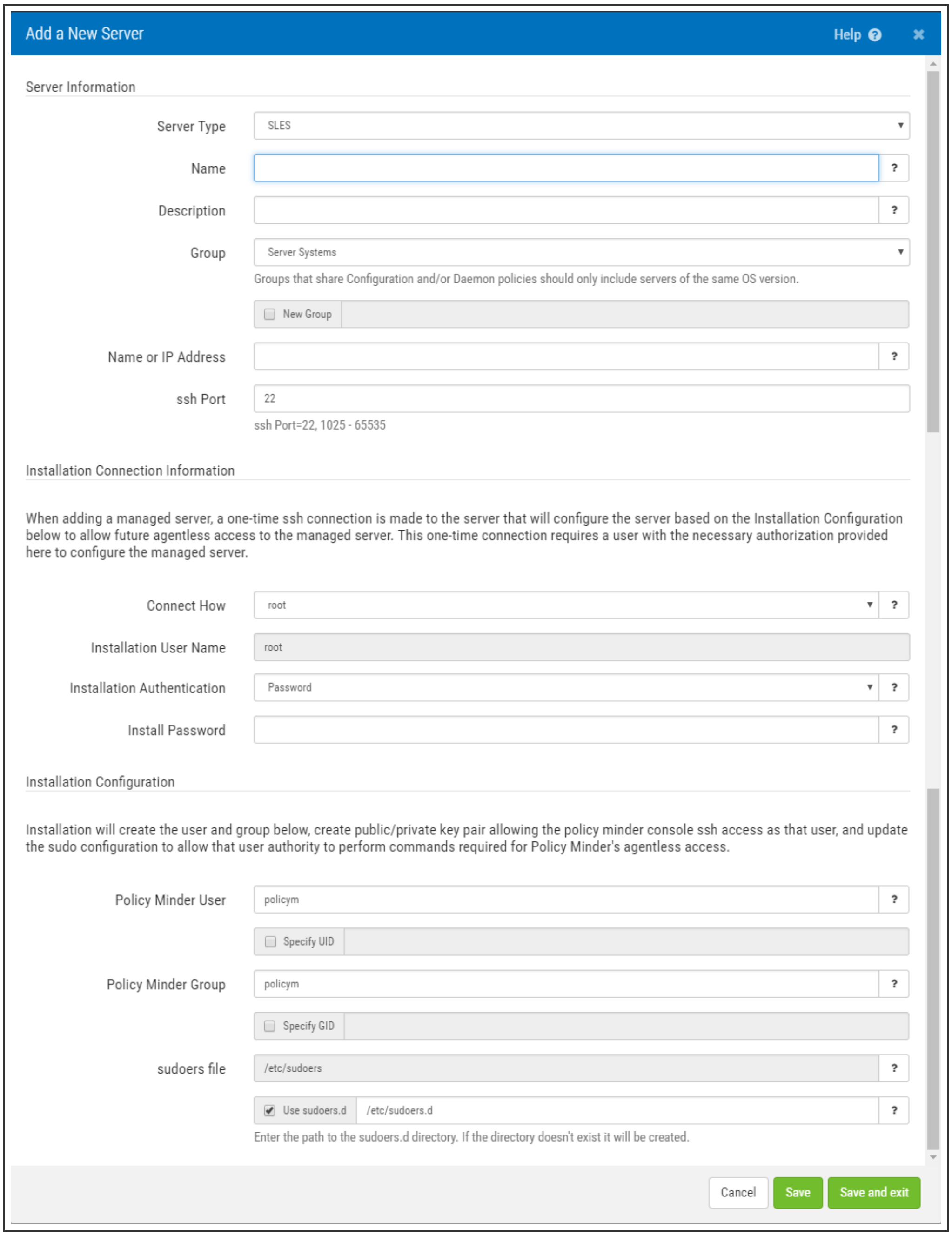
Select **Check Replication** to include the AWS S3 Replication settings in your policy. If checked, the subsequent option becomes active.

Allow Replication Rules

Check this option to permit Replication Rules in your policy. If this option is unchecked, Replication Rules in the S3 bucket are non-compliant.

Add a New Server screen

Use this screen to add a new server. When a new managed server is added, Security Auditor makes an ssh connection, creates a group, user and ssh keys, and configures sudo so that the new server can be managed by Security Auditor's agentless control.



Server Information

Server Type	SLES ▾	
Name		?
Description		?
Group	Server Systems ▾ Groups that share Configuration and/or Daemon policies should only include servers of the same OS version. □ New Group	
Name or IP Address		?
ssh Port	22 ssh Port=22, 1025 - 65535	

Installation Connection Information

When adding a managed server, a one-time ssh connection is made to the server that will configure the server based on the Installation Configuration below to allow future agentless access to the managed server. This one-time connection requires a user with the necessary authorization provided here to configure the managed server.

Connect How	root ▾	?
Installation User Name	root	
Installation Authentication	Password ▾	?
Install Password		?

Installation Configuration

Installation will create the user and group below, create public/private key pair allowing the policy minder console ssh access as that user, and update the sudo configuration to allow that user authority to perform commands required for Policy Minder's agentless access.

Policy Minder User	policym □ Specify UID	?
Policy Minder Group	policym □ Specify GID	?
sudoers file	/etc/sudoers	?
	☑ Use sudoers.d /etc/sudoers.d Enter the path to the sudoers.d directory. If the directory doesn't exist it will be created.	?

How to get there

Choose **Servers** > **Add a Server**. Or, from the Manage Servers screen, click **Add**.

Server Information

Server Type

Here, choose the OS of the server you are adding.

Name

This is the name of the server as it will appear in Security Auditor.

Name variables:

- {nameoripaddress}
- {servertype}
- {hostname}

Description

A description of the server can be added here.

Description Variables:

- {name}
- {nameoripaddress}
- {servertype}
- {hostname}

Group • New Group

Choose a group from this drop-down list to assign the server to one of Security Auditor's Groups. Check New Group and type the name of the new Group in the adjacent text box to add a new one. Organizing servers into Groups can help you more easily view and manage servers as you work with policies and compliance. A server can only be assigned to one group.

New Group shares policy

Check this box if the servers in the Group should have a Shared Policy. If this option is not checked, a Shared Policy will not be available for this Group. See Policy Overview for more details.

> **NOTE:** If you check 'New Group' and the Group already exists, Security Auditor will add the servers to the existing Group.

Name or IP Address

The name of the server or its IP address.

Name or IP Variables:

- {name}

ssh Port

The ssh port. The default is port 22 for Unix-based servers.

Installation Information

When a new managed server is added Security Auditor will make an ssh connection, create a group, user and ssh keys and configure sudo so that the new server can be managed by Security Auditor's agentless control.

Connect How

If root is selected then install will be performed as root. If Use SU is selected then before installation begins the install program will log on using the user and password given and then su to root with the password given. If sudo is selected then install will be performed as a user who can execute admin commands using sudo (with their own password).

Connection Option (Windows only)

If Default User and Password is selected, installation will use the shared ID. If Server User and Password is selected, an ID specific to this server will be used. The Default User and Password is specified in Security Auditor's Preferences screen.

The following settings apply to non-Windows servers only:

Installation User Name

If "root" is selected for Connect How, "root" appears here. Choose "su" or "sudo" for Connect How to enter the name you would like to use for product installation on the server.

Installation Authentication

The authentication method must be specified for the Installation User.

- **Password** If this option is selected, you must provide the password required for the Installation User.
- **Private key** If this option is selected, you must paste or type the contents of a private key file (.pem).
- **Private key .pem file** If this option is selected, you must select a .pem file from the file system.
- **Managed Private Key** If this option is selected you must select a Private Key defined under the 'Admin Tasks' menu.

Install Password

Password is used only for install and is not saved. If the console is not configured for https (see manual) then the password will be sent clear text one time from browser to server.

Security Auditor User • Specify UID

A user with this name will be created on the managed server and used by Security Auditor for agentless control.

Security Auditor Group • Specify GID

A group with this name will be created on the managed server and used by Security Auditor for agentless control.

sudoers file • Use sudoers d

Enter the path to the sudoers file where sudo config is located. If 'Use sudoers.d' is checked then the necessary sudoers additions for the Security Auditor user to execute commands via sudo will be placed in a new file in the sudoers.d directory (this is a best practice). If unchecked then the necessary changes will be appended to the sudoers file.

Cancel • Save • Save and Exit

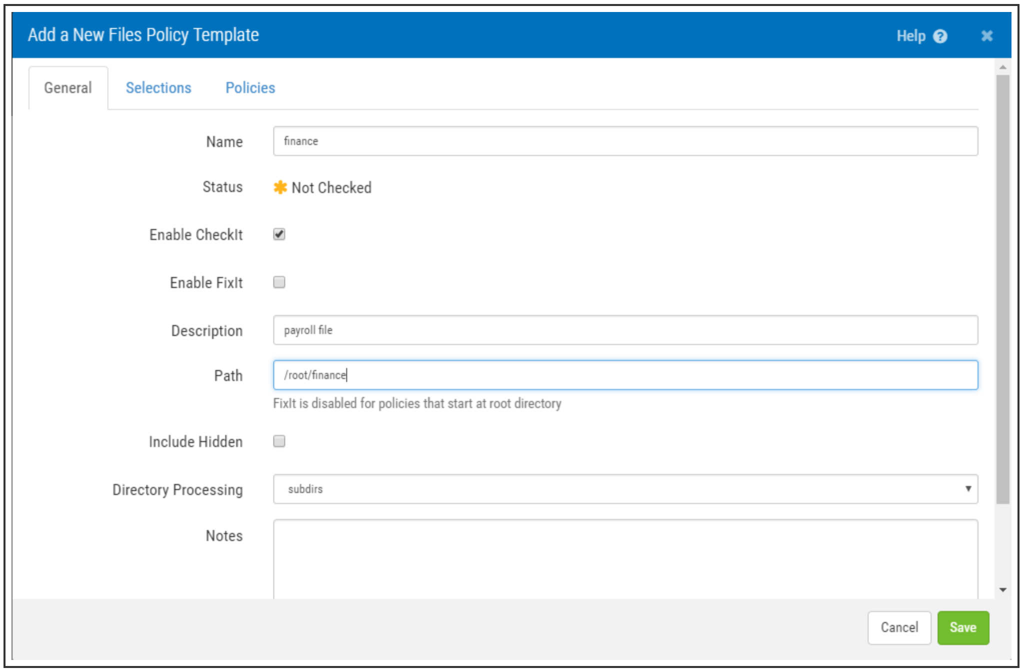
Click **Save** to add the server without dismissing the Add a New Server screen. Click **Cancel** to dismiss this screen without making changes. Click **Save and exit** to add the server and dismiss the screen.

> **NOTE:** Pressing Enter selects **Save and Exit**.

Getting Started

Add/Modify Files Template screen

If you are modifying an existing Files Policy Template, the title of this screen is "Modify template [template name]." This screen allows you to define a Files Policy template, or modify an existing one.



Name: finance

Status: ✱ Not Checked

Enable CheckIt ☑

Enable FixIt □

Description: payroll file

Path: /root/finance

FixIt is disabled for policies that start at root directory

Include Hidden □

Directory Processing: subdirs ▾

Notes:

How to get there

On the Manage Servers screen, click F for the server whose policy you would like to add or modify. Or, from the Servers and Policies screen, choose the Scripts category and click **New**, or to modify an existing template, click the template.

What it Does

Use these options to add or modify a Files Policy Template.

General tab

Name

The name of the Files Policy template.

Status

The status of the Files Policy template. Not checked ✱, Not Compliant ✖ , or Compliant ✔.

Checked On

Lists the date and time this policy was last checked (modify only)

Enable CheckIt

Check this box to allow Security Auditor to check this value on the server to determine its status.

Enable FixIt

Check this box to allow Security Auditor to fix this value on the server (i.e. change it to match the template value).

Description

A description of the file.

Path

The path of the file on the server. FixIt is disabled for policies that start at root directory.

Include Hidden

Check this box to include hidden files in the policy.

Directory Processing

Choose 'subdirs' to include subdirectories. Choose 'noSubDirs' to omit suibdirectories. Choose specifyMinMaxDepth to indicate the minimum and maximum directory depth.

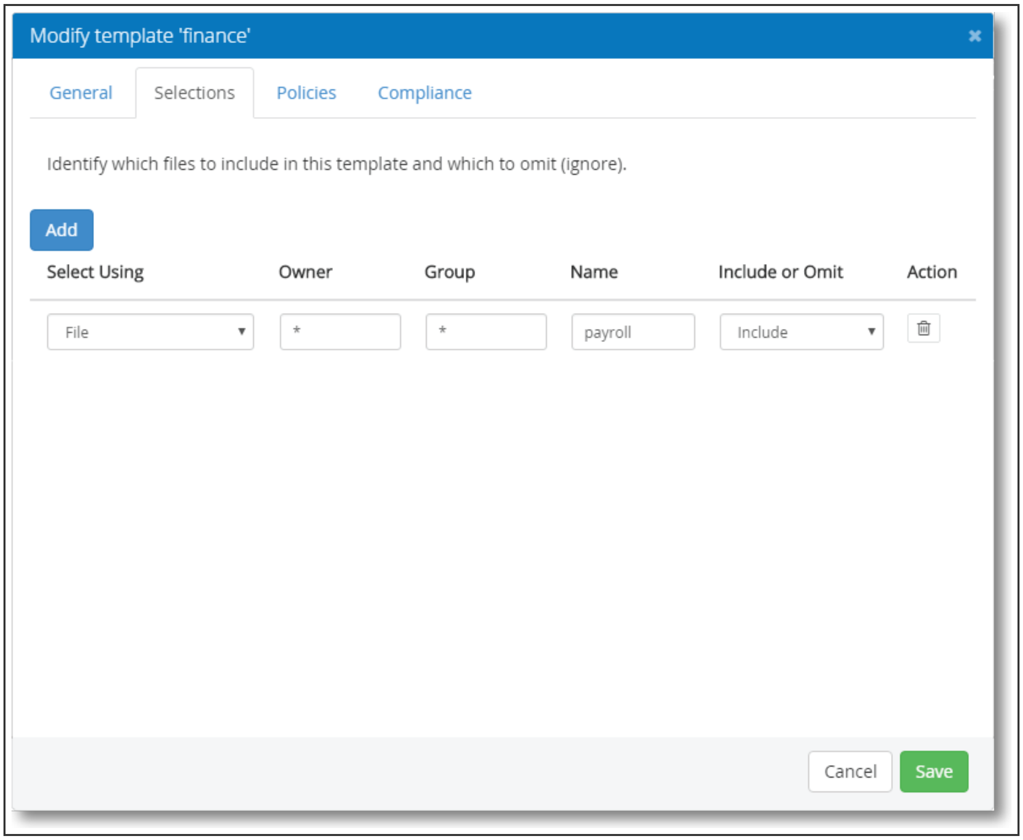
- **Minimum Depth:** Do not apply any tests or actions at levels less than n (a non-negative integer). -mindepth 1 means process all files except the starting-points.
- **Maximum Depth:** Descend at most n levels (a non-negative integer) of directories below the starting-points. -maxdepth 0 means only apply the tests and actions to the starting-points themselves.

Notes

Enter notes here. Notes show up in reports and provide a place to explain the intent of defined policies.

Selections tab

Use this tab to identify which files to include in this Template and which to omit (ignore).



Identify which files to include in this template and which to omit (ignore).

Select Using	Owner	Group	Name	Include or Omit	Action
File ▾	*	*	payroll	Include ▾	🗑

Add

Click **Add** to add an additional user account.

Select Using

Use this list to choose what criteria you would like to use for selection: file, directory, attributes, files with no owner, files with no group, directories with no owner, or directories with no group.

Owner • Group • Name

Unix glob characters allowed: *= one or more chars, ?=a single char, [xyz]=a char from set, [!xyz]=a char not from set. Also the '!' operator (e.g. !staff) preceding the pattern means anything other than the pattern specified.

Include or Omit

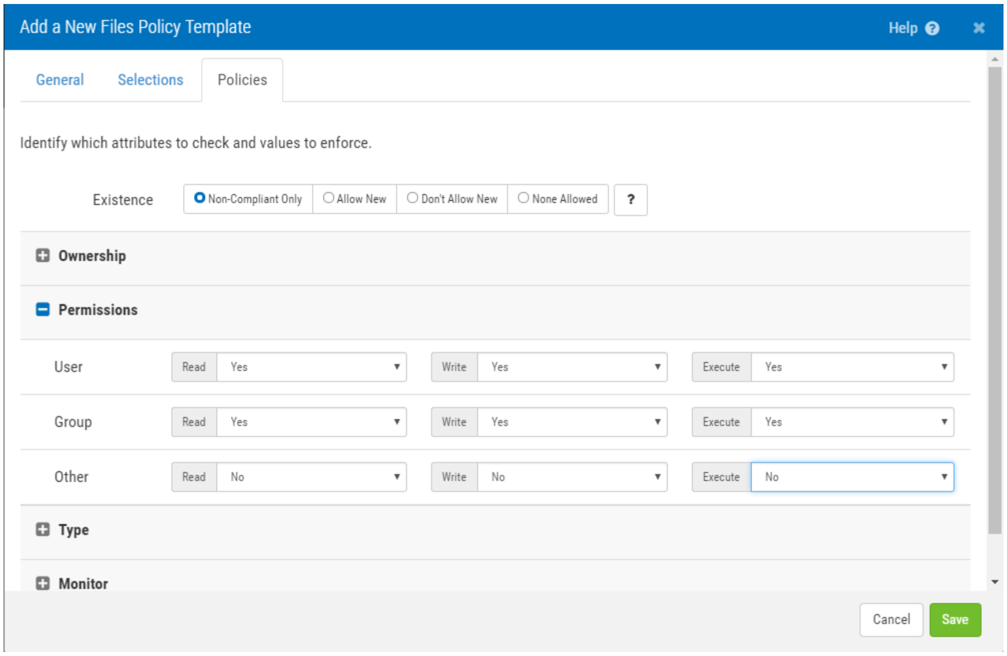
Choose whether you want to include or omit this criteria.

Action

Select 🗑 (Remove) to delete the policy item, respectively.

Policies tab

Use this tab to identify which attributes to check and values to enforce.



Identify which attributes to check and values to enforce.

Existence ● Non-Compliant Only ○ Allow New ○ Don't Allow New ○ None Allowed ?

User	Read: Yes	Write: Yes	Execute: Yes
Group	Read: Yes	Write: Yes	Execute: Yes
Other	Read: No	Write: No	Execute: No

Existence: Non-Compliant Only • Allow New • Don't Allow New • None Allowed

If 'Allow New' then new instances of the user accounts selected will not be identified as out of compliance. If 'Don't Allow New' then new instances of the user accounts selected that are not in the baseline will be identified as out of compliance. (The baseline is created when the first compliance check (CheckIt) is run. Non-compliant (new) users can be accepted into the baseline after subsequent checks.) If 'None Allowed', any user accounts discovered on a compliance check are non-compliant.

Ownership • Attributes • Permissions • Extended Permissions • Type • Monitor

> **NOTE:** Extended Permissions are AIX-specific File policy attributes.

Here, specify policy criteria for file ownership, attributes, permissions, extended permissions, type, and specify what to monitor. The categories available here depend on the operating system of the server.

Attributes (Windows):

> **NOTE:** * FixIt is not supported for these attributes

- **Archive:** A file or directory that is an archive file or directory. Applications typically use this attribute to mark files for backup or removal.
- **Compressed*:** A file or directory that is compressed. For a file, all of the data in the file is compressed. For a directory, compression is the default for newly created files and subdirectories.
- **Encrypted*:** A file or directory that is encrypted. For a file, all data streams in the file are encrypted. For a directory, encryption is the default for newly created files and subdirectories.
- **Hidden:** The file or directory is hidden. It is not included in an ordinary directory listing.
- **NotContentIndexed:** The file or directory is not to be indexed by the content indexing service.

- **ReadOnly:** A file that is read-only. Applications can read the file, but cannot write to it or delete it. This attribute is not honored on directories.
- **System:** A file or directory that the operating system uses a part of, or uses exclusively.

Type:

- **SUID:** SUID on an executable file means that when the file is executed, the process runs with an effective UID of the owner of the file. The SUID is not supported on shell scripts, and it has no meaning on a directory.
- **SGID:** SGID on an executable file means that when the file is executed, the process runs with an effective GID of the group owner of the file. The SGID on a directory means that any file or directory created within the directory will have the same group ownership as the directory, rather than of the primary group of the user. The SGID permission bits are propagated down through the directory structure, so any directory created within a directory with the SGID bit set also inherits that bit.
- **SVTX:** SVTX on a directory means that even if the directory has global write permission (such as /tmp), users cannot delete a file in the directory unless they own the file or the directory.

NOTE:
The format for the “Specify”, “Deny”, and “Permit” values of Extended Permissions (AIX) are:

- One or more “mode strings” separated by an “&” character.
- A “mode string” has two parts separated by a space:
  - Three character “rwx” mode. (Hyphen replaces unspecified permission)

    Examples:

    `rwx` = Read, Write, and Execute

    `r--` = Read

    `-wx` = Write and Execute
  - User/Group Info String:
    - User string example:
      `u:username`
    - Group string example:
      `g:groupname`
- Complete “mode string” examples:

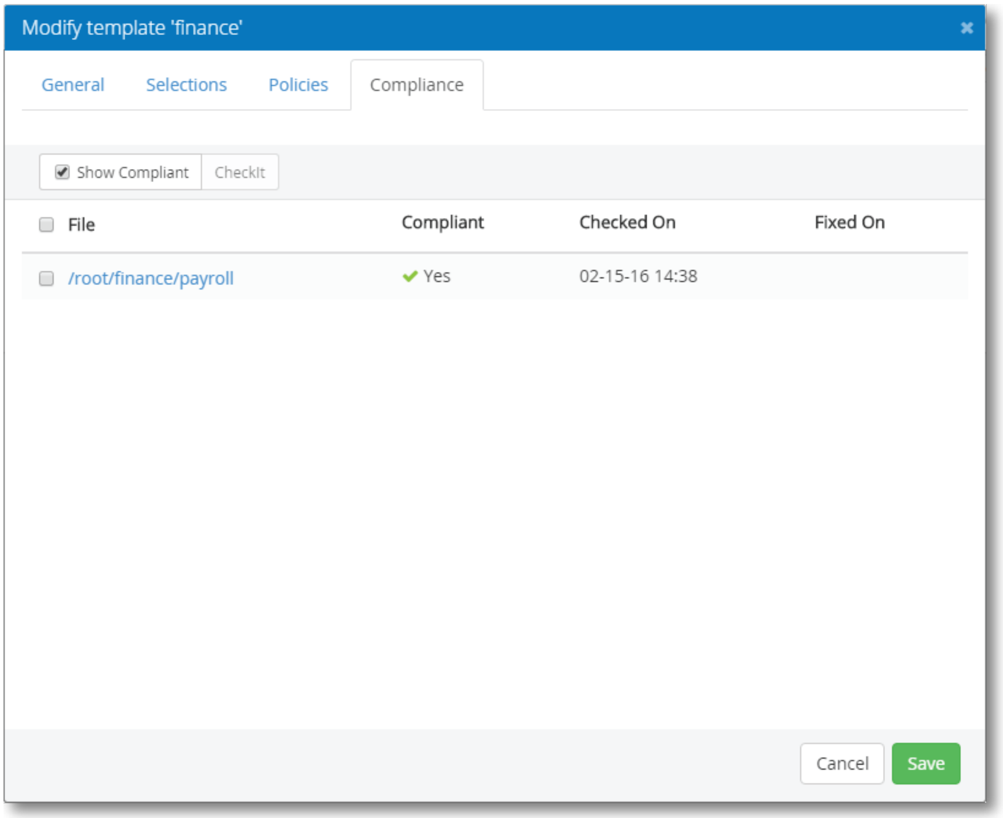
  `rwx u:user1` = Read, Write, and Execute authority to User “user1”

  `--x g:group1` = Execute authority to Group “group1”
- Examples of complete policy strings for “Specify”, “Deny”, and “Permit” attributes are:

  ```
  r-- u:user1
  --x g:group1
  rwx u:user1&--x g:group1&rw- g:group2
  rwx u:user1& rwx u:user2& rwx u:user3
  ```

Compliance tab

Use this tab to view and check existing Files Policies.



☑ Show Compliant | CheckIt

□ File	Compliant	Checked On	Fixed On
□ /root/finance/payroll	✓ Yes	02-15-16 14:38	

Show Compliant

Check this box to show compliant files.

CheckIt

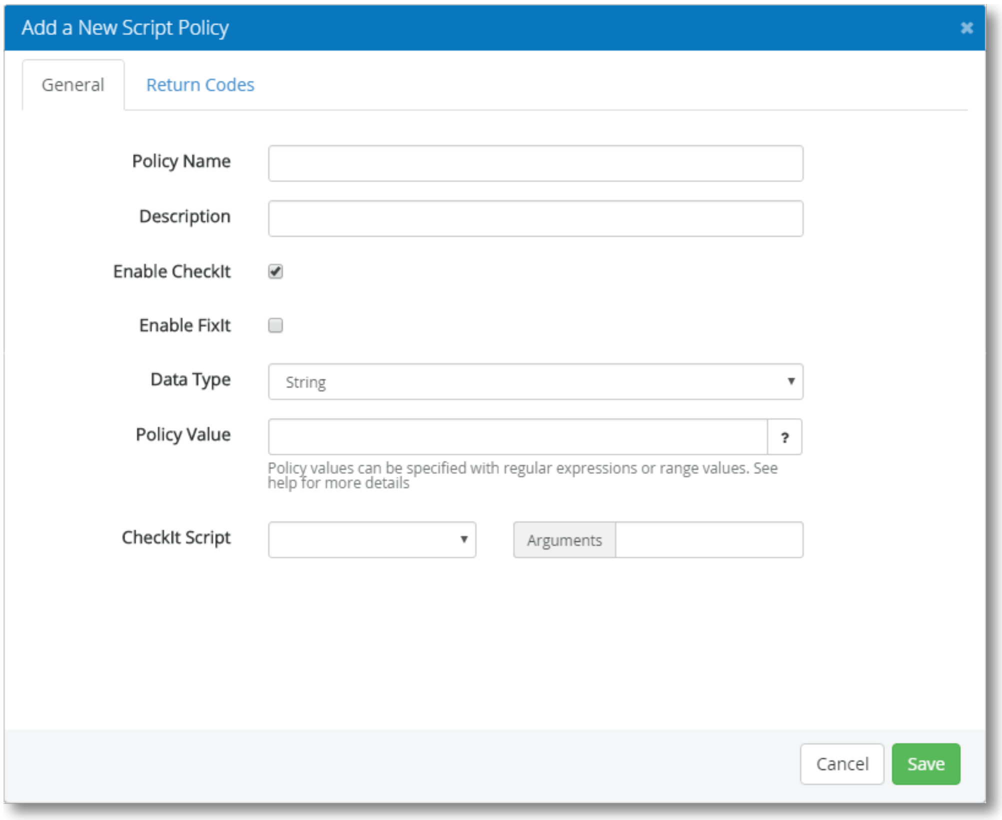
Use this button to run CheckIt, which performs a compliance check for the selected files.

Cancel • Save

Click **Cancel** to dismiss this screen without making changes. Click **Save** to add or save changes to the Policy Template.

Add a New Script Policy screen

If you are modifying an existing Script Policy template, the title of this screen is "Modify template [template name]." This screen allows you to define a Script Policy template, or modify an existing one.



Policy Name

Description

Enable CheckIt ☑

Enable FixIt □

Data Type: String

Policy Value

Policy values can be specified with regular expressions or range values. See help for more details

CheckIt Script

Arguments

How to Get There

On the Manage Servers screen, click S for the server whose policy you would like to add or modify. Or, from the Servers and Policies screen, choose the Scripts category and click **New**, or to modify an existing template, click the template.

What it Does

Use these options to add a new Script Policy Template for the selected server.

General tab

Policy Name

The name of the template.

Description

The template description.

Enable CheckIt

Check this box to allow Security Auditor to check this value on the server to determine its status.

Enable FixIt

Check this box to allow Security Auditor to fix this value on the server (i.e. change it to match the template value).

Data Type

Data types may be String, Integer, Boolean and date.

- String values can be literal or regular expressions.
- The syntax for regular expressions follows a standard and is documented in the dialog. The documentation can be viewed in a popup dialog by clicking on the icon.
- Integer values can be a specific value, a range, or a list of ranges and specific values. The syntax for integers is also documented in the popup dialog.
- A Boolean value is considered true if it matches (ignoring case) any of the values "true", "t", "yes", "y" or "on" or if the value can be parsed as a number and does not equal zero.
- Date values can be a specific date, a before date, an after date or a date range.

Click on the CheckIt Script drop down to choose the script.

If the script requires arguments to be passed in, specify those in the Arguments field.

Policy Value

The Policy Value is what you see as a result of running the script. Specify the Data Type that is appropriate for this result. See Policy Values for more information.

> **NOTE:** a valid result of running a script may be nothing or no value. In this case, leave the Policy Value field blank. When a compliance check is run on this script policy, the result of running the script will be compared against the value you specify in the Policy Value field. If they are equal the policy will be compliant. If they aren’t, the script policy will be out of compliance.

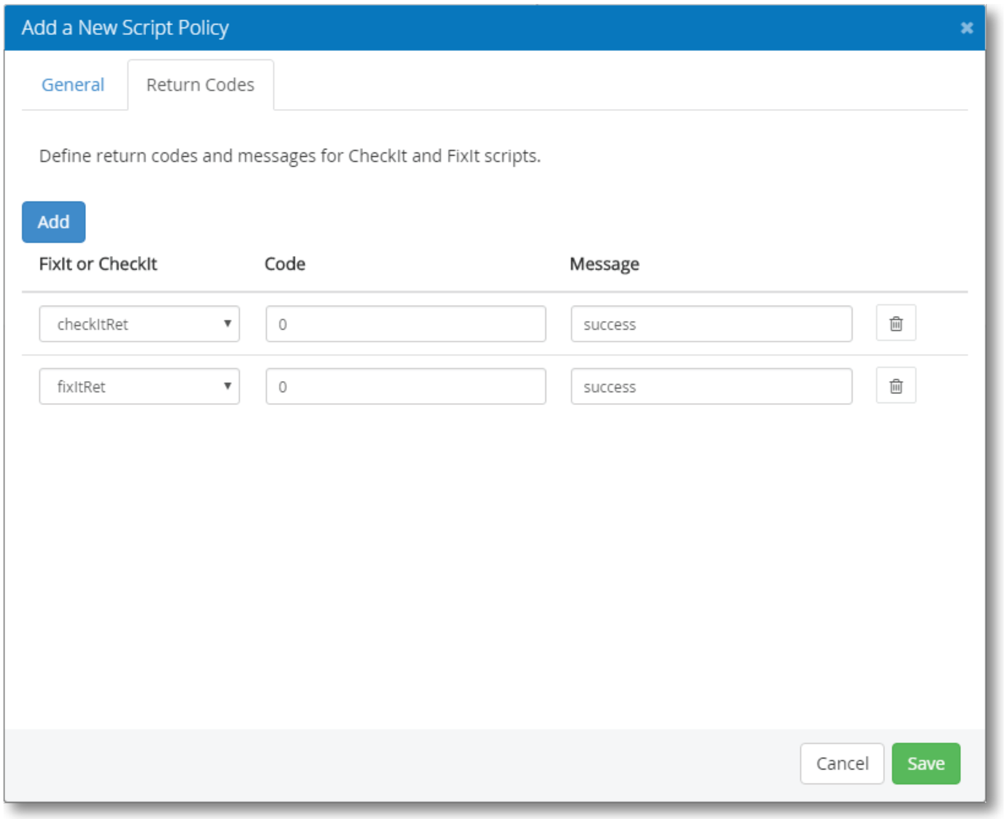
CheckIt Script • Arguments

Once a script has been uploaded or placed directly into the scripts directory, it will appear as a selection for the CheckIt script and FixIt script when defining a Script Policy.

Arguments are passed to script when run on host. Arguments can be concrete values, or the $SERVERTYPE macro (replaced with AIX, RHEL, Ubuntu, etc. at runtime).

Return Codes tab

This tab allows you to define return codes and messages for CheckIt and FixIt scripts.



Define return codes and messages for CheckIt and FixIt scripts.

FixIt or CheckIt	Code	Message
checkItRet	0	success
fixItRet	0	success

Add

Click **Add** to add a new Return Code entry below.

FixIt or CheckIt • Code • Message

Here, choose whether it is a CheckIt or FixIt script, enter the code, and add a message.

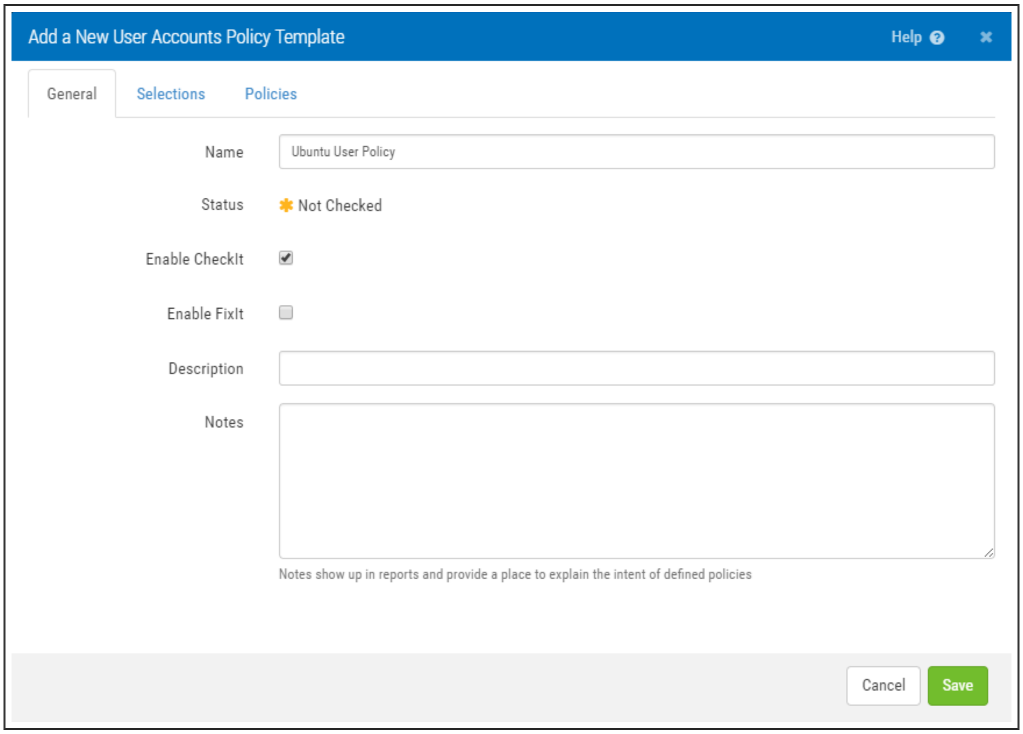
Cancel • Save

Click **Cancel** to dismiss the Add a New Script Policy screen without making changes. Click **Save** to save changes and return to the Servers and Policies screen.

Scripts

Add a New User Accounts Policy Template screen

If you are modifying an existing User Accounts Policy Template, the title of this screen is "Modify template [template name]." This screen allows you to define a User Accounts Policy template, or modify an existing one.



Name: Ubuntu User Policy

Status: ✱ Not Checked

Enable CheckIt: ☑

Enable FixIt: □

Description:

Notes:

Notes show up in reports and provide a place to explain the intent of defined policies

How to get there

On the Manage Servers screen, click U for the server whose policy you would like to add or modify. From the Servers and Policies screen, choose the User Accounts category and click **New**. Or to modify an existing template, click the template.

What it Does

Use these options to add a new User Accounts Policy Template for the selected server.

General tab

Name

The name of the policy template.

Status

Lists whether the server is Not checked ✱, Not Compliant ✖ , or Compliant ✓.

Checked On

Lists the date and time this template was most recently checked.

Enable CheckIt

Check this box to allow Security Auditor to check this value on the server to determine its status.

Enable FixIt

Check this box to allow Security Auditor to fix this value on the server (i.e. change it to match the template value).

Description

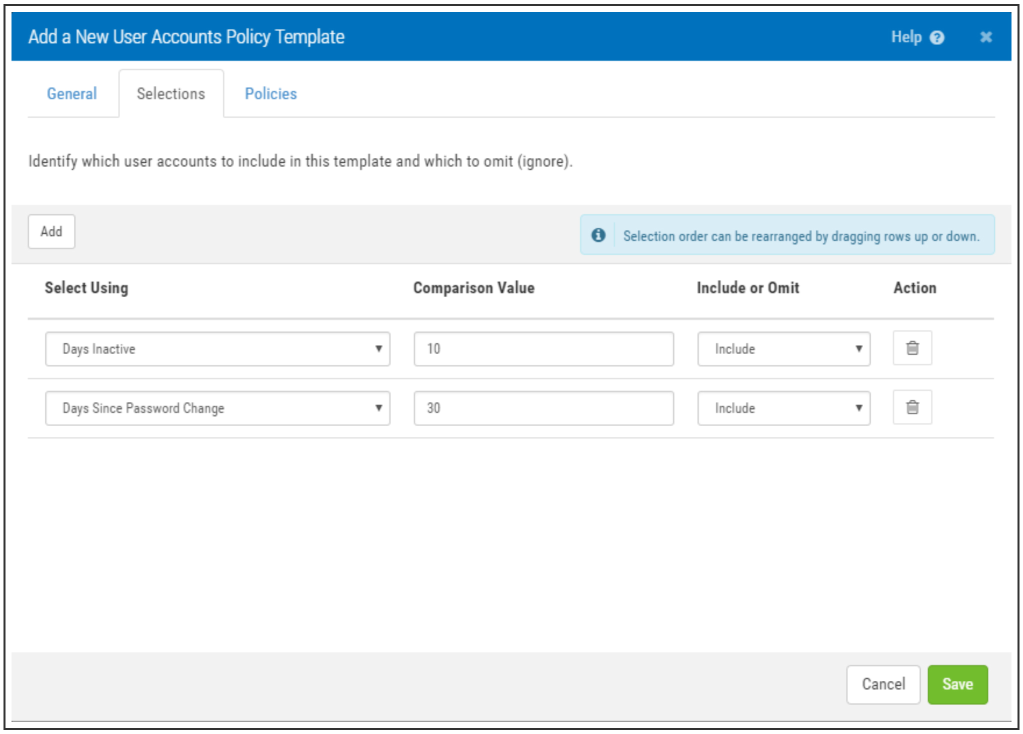
This is the template description.

Notes

Enter notes here. Notes show up in reports and provide a place to explain the intent of defined policies.

Selections tab

Use these options to identify which user accounts to include in this template and which to omit (ignore).



Identify which user accounts to include in this template and which to omit (ignore).

Selection order can be rearranged by dragging rows up or down.

Select Using	Comparison Value	Include or Omit	Action
Days Inactive	10	Include	🗑
Days Since Password Change	30	Include	🗑

Add

Click this button to add additional user account selection criteria. A new row is added to the section below. The new criteria will be additive to the existing criteria, and not restrictive. In other words, each row defines a new criteria for users to be included or omitted in the selection. (The rows represent an 'or' and not an 'and' relationship.)

> **NOTE:** Selection order can be rearranged by dragging rows up or down.

Select Using

Use this list to choose what criteria you would like to use to select the user account.

Comparison Value

Enter the value to compare with the criteria selected (e.g. the user logon name you want to include).

- **User Logon Name • Primary Group • Group Member.** The user name can be specified exactly or using standard 'glob' characters {*, ?, [],}. Also the '!' character can be placed before the comparison value to get all users that don‘t match.
- **Days Inactive.** Users who have not logged on in more days than the comparison value will be selected.
- **Days Since Password Change.** Users who have not changed their password in more days than the comparison value will be selected.
- **UID • No Password • Non Unique UID.** Integer values can be a single value, a set of values, a range or a set of ranges and values. A set of acceptable values are separated by the character ';' like 1;7;11. A range of acceptable values are separated by a ':' like 1:20. If an endpoint is missing (e.g. 500:) it implies all numbers less than or greater than the specified endpoint. A set of ranges and values are separated by both ';' and ':' like 1:20;25;30:35.

Include or Omit

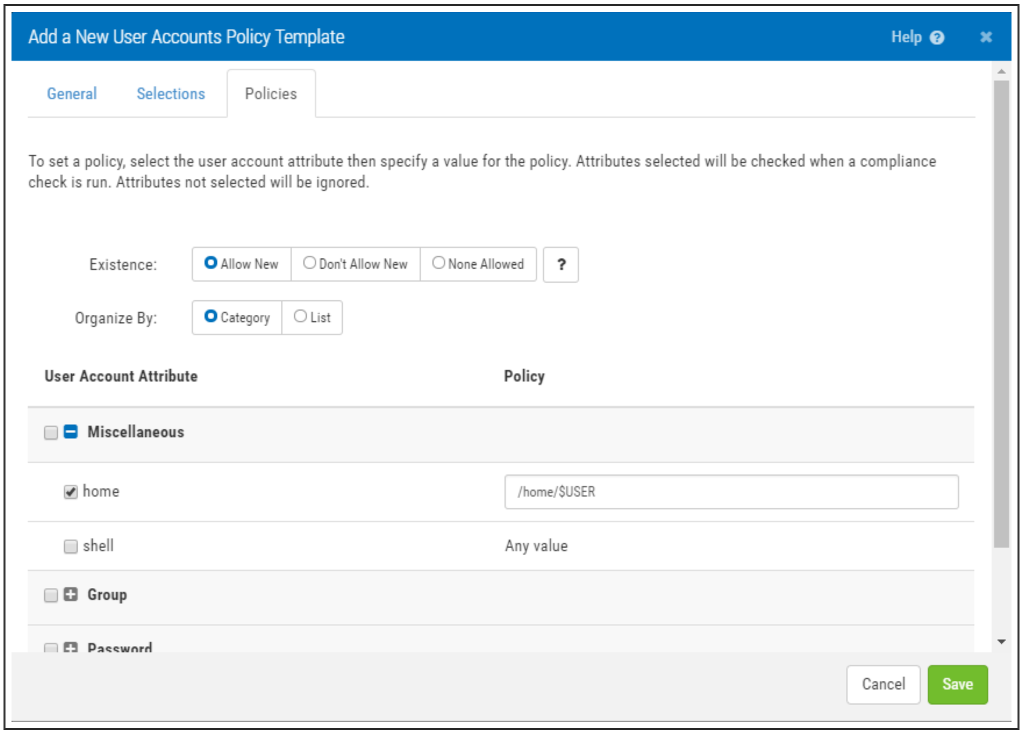
Choose whether you want to include or omit user accounts that match this criteria.

Action

Select 🗑 (Remove) to delete the policy item, respectively.

Policies tab

Use the options on this tab to define your Policy. To set a policy, select the user account attribute then specify a value for the policy. Attributes selected will be checked when a compliance check is run. Attributes not selected will be ignored.



To set a policy, select the user account attribute then specify a value for the policy. Attributes selected will be checked when a compliance check is run. Attributes not selected will be ignored.

Existence: ● Allow New ○ Don't Allow New ○ None Allowed ?

Organize By: ● Category ○ List

User Account Attribute	Policy
□ Miscellaneous	
☑ home	/home/$USER
□ shell	Any value
□ Group	
□ Password	

Existence: Allow New • Don't Allow New • None Allowed

If 'Allow New' then new instances of the user accounts selected will not be identified as out of compliance. If 'Don't Allow New' then new instances of the user accounts selected that are not in the baseline will be identified as out of compliance. (The baseline is created when the first compliance check (CheckIt) is run. Non-compliant (new) users can be accepted into the baseline after subsequent checks.) If 'None Allowed', any user accounts discovered on a compliance check are non-compliant.

Organize By: Category • List

Use these buttons to select how you would like to organize the attributes.

Linux User Account Attributes (Ubuntu, RHEL, CentOS, Oracle, SLES)

Miscellaneous

home

Full path name of the home directory of the user. The $USER macro can be used for defining policy, e.g. /home/$USER.

shell

Defines the program run for the user at session initiation - full path name.

Group

pgrp

Identifies the users primary group - value cannot be null. The $USER macro can be used for defining policy, e.g. $USER.

groups

Identifies the groups the user belongs to. The $USER macro can be used for defining policy, e.g. $USER group2 group3.

Password

pass_max_days

The maximum number of days a password may be used. If the password is older than this, a password change will be forced. If not specified, -1 will be assumed (which disables the restriction).

pass_min_days

The minimum number of days allowed between password changes. Any password changes attempted sooner than this will be rejected. if not specified, -1 will be assumed (which disables the restriction).

pass_warn_age

The number of days warning given before a password expires. A zero means warning is given only upon the day of expiration, a negative value means no warning is given. If not specified, no warning will be provided.

Login

account_expires

Set the date or number of days since January 1, 1970 on which the users account will no longer be accessible. The date may also be expressed in the format WW-MM-DD (or the format more commonly used in your area). A user whose account is locked must contact the system administrator before being able to use the system again. Note that an account expiration differs from a password expiration. In case of an acount expiration, the user shall not be allowed to login. In case of a password expiration, the user is not allowed to login using her password.

inactive

The number of days after password expires that account is disabled.

pass_locked

Indicates if the user account is locked. This is indicated in the shadow password file by a prefix before the encrypted password. A user with password locked may still login through other mechanisms such as a ssh key.

AIX User Account Attributes

Miscellaneous

admin

Defines the administrative status of the user. Possible values are: (1) true - The user is an administrator. Only the root user can change the attributes of users defined as administrators. (2) false - The user is not an administrator. This is the default value.

admgroups

Lists the groups the user administrates. The value parameter is a comma-separated list of group names.

auth1

Primary auth method (Deprecated: use SYSTEM). Lists the primary methods for authenticating the user.

auth2

Lists the secondary methods for authenticating the user.

SYSTEM

Defines the system authentication mechanism for the user.

capabilities

Defines the system privileges (capabilities) which are granted to a user by the login or su commands. The Value parameter is a list of comma-separated classes.

default_roles

Specifies the default roles for the user; can only contain roles assigned to the user in the roles attribute. You can use the ALL keyword to signify that the default roles for the user are all their assigned roles. The Value parameter is a list of comma-separated classes.

home

Full path name of the home directory of the user. The $USER macro can be used for defining policy, e.g. /home/$USER.

rcmds

Controls the remote execution of the r-commands (rsh, rexec, rcp); Possible values are allow (default), deny, and hostlogincontrol, which specifies that the ability of remote command execution is determined by the hostsallowedlogin and hostsdeniedlogin attributes. The user is only allowed to execute remote commands on a target system if the user (or target user) is allowed to log in the target system.

roles

Lists the administrative roles for this user. The Value parameter is a list of role names, separated by commas.

shell

Defines the program run for the use: at session initiation - full path name.

su

Indicates whether another user can switch to the specified user account with the su command - true (default) or false.

sugroups

Lists the groups that can use the su command to switch to the specified user account a value of ALL indicates all groups. An ! (exclamation point) in front of a group name excludes that group. If this attribute is not specified, all groups can switch to this user account with the su command

unmask

Determines file permissions at time of creation; the default is 022.

Auditing

auditclasses

Lists the users audit classes. The Value parameter is a list of comma-separated classes, or a value of ALL to indicate all audit classes.

Group

pgrp

Identifies the users primary group - value cannot be null. The $USER macro can be used for defining policy, e.g. $USER.

groups

Identifies the groups the user belongs to. The $USER macro can be used for defining policy, e.g. $USER group2 group3.

Password

dictionlist

Defines the password dictionaries used when creating new passwords.

histexpire

Defines the period of time (in weeks) that a user cannot reuse a password. The value is a decimal integer string. The default is 0, indicating that no time limit is set. Only an administrative user can change this attribute.

histsize

Defines the number of previous passwords a user cannot reuse. The value is a decimal integer string. The default is 0. Only an administrative user can change this attribute.

maxage

Defines the maximum age in weeks of a password. The password must be changed by this time. The value is a decimal integer string. The default is a value of 0, indicating no maximum age. Range: 0 to 52

maxexpired

Defines the maximum time in weeks beyond maxage that a user can change an expired password. After this defined time, only an administrative user can change the password. The value is a decimal integer string. The default is -1, which means the user can always change their expired password regardless of how many weeks have passed. If the maxexpired attribute is 0, the password expires when the maxage value is met. If the maxage attribute is 0, the maxexpired attribute is ignored. Range: 0 to 52 (a root user is exempt from maxexpired)

maxrepeats

Defines the maximum number of times a character can be repeated in a new password. Since a value of 0 is meaningless, the default value of 8 indicates that there is no maximum number. The value is a decimal integer string. Ranqe: 0 to 8

minage

Defines the minimum age (in weeks) a password must be before it can be changed. The value is a decimal integer string. The default is a value of 0, indicating no minimum age. Range: 0 to 52

minalpha

Defines the minimum number of alphabetic characters that must be in a new password. The value is a decimal integer string. The default is a value of 0, indicating no minimum number. Range: 0 to 8

mindiff

Defines the minimum number of characters required in a new password that were not in the old password. The value is a decimal integer string. The default is a value of 0, indicating no minimum number. Range: 0 to 8

minlen

Defines the minimum length of a password. The value is a decimal integer string. The default is a value of 0, indicating no minimum length. The maximum value allowed is 8. This attribute is determined by minlen and/or minalpha + minother, whichever is greater. minalpha + minother should never be greater than 8. If minalpha + minother is greater than 8, then the effective value for minother is reduced to 8 - minalpha.

minother

Defines the minimum number of non-alphabetic characters that must be in a new password. The value is a decimal integer string. The default is a value of 0, indicating no minimum number. Range: 0 to 8

pwdchecks

Defines the password restriction methods enforced on new passwords. The value is a list of comma-separated method names and is evaluated from left to right. A method name is either an absolute path name or a path name relative to /usr/lib of an executable load module.

pwdwarntime

Defines the number of days before the system issues a warning that a password change is required. The value is a decimal integer string. A zero or negative value indicates that no message is issued. The value must be less than the difference of the maxage and minage attributes. Values greater than this difference are ignored and a message is issued when the minage value is reached.

Login

account_locked

Indicates if the user account is locked - yes, true, and always are equivalent no, false, and never are equivalent.

expires

Identifies the expiration date of the account. The Value parameter is a 10-character string in the MMDDhhmmYY form, where MM = month, DD = day, hh = hour, mm = minute, and YY = last 2 digits of the years 1939 through 2038. All characters are numeric. If the Value parameter is 0, the account does not expire. The default is 0.

login

Indicates if the user can log into the system with the login command - true (default) or false.

loginretries

Defines the number of unsuccessful login attempts allowed after the last successful login before the system locks the account. A zero or negative value indicate that no limit exists.

maxulogs

Defines the maximum number of logins for the user. If the concurrent login number for a user exceeds the maximum number of allowed logins, the login is denied.

rlogin

Indicates if the user can access the account remotely with the telnet or rlogin commands - true (default) or false.

Windows User Account Attributes

Miscellaneous

Home Directory

The home directory of the user. The $USER macro can be used for defining policy, e.g. /home/$USER.

Group

groups

The list of groups that the user is a member of. The policy value is a comma separated list of group names. The $USER macro is supported.

Password

User May Change Password

Can the user change the password?

Password Expired *

Has the password expired?

Password Expires *

Does the password expire?

Password Expiration Date *

The Password Expiration Date. The policy value can be the expiration timestamp [yyyy-mm-dd hh:mm:ss], the expiration day [yyyy-mm-dd], expires within x days [number], expires during days range [number:number], or no expiration [blank].

Password Required

Is a password required to log on?

Login

Account Expired *

Has the account expired?

Account Expires *

Does the account expire?

Account Expiration Date

The account expiration date. The policy value can be the expiration timestamp [yyyy-mm-dd hh:mm:ss], the expiration day [yyyy-mm-dd], expires within x days [number], expires during days range [number:number], or no expiration [blank]. FixIt only supports expiration day or no expiration [blank].

Account Active

Is the account active? The policy value can be yes, no, or locked. FixIt only supports yes or no.

Logon Script

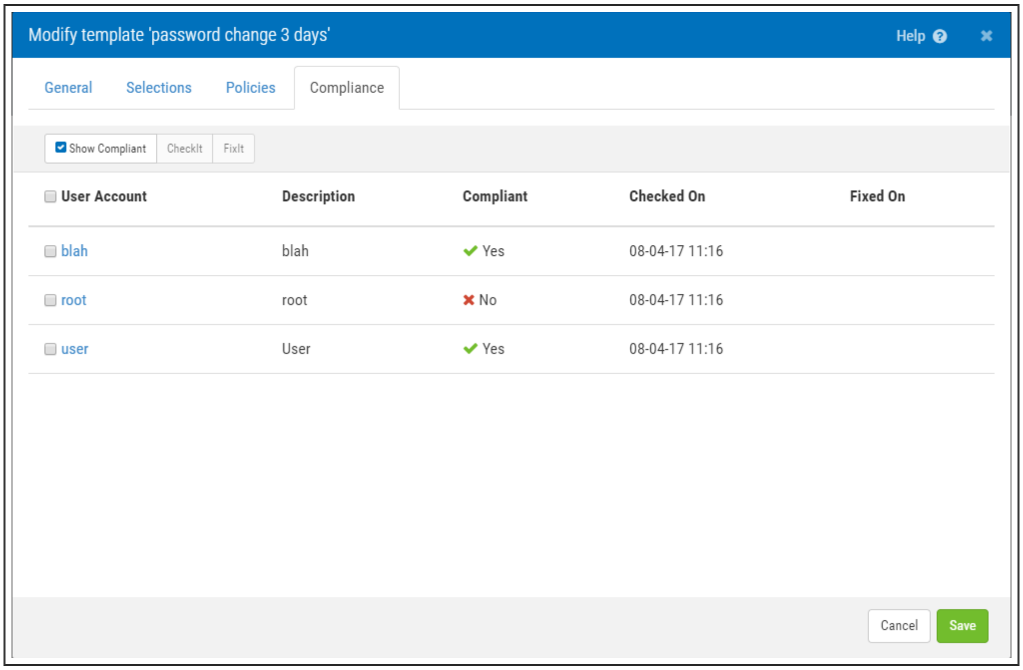
The logon script for the user. $USER macro is supported.

Profile Path

The profile path to the user account. $USER macro is supported.

Compliance tab

This tab appears if CheckIt results exist, and shows the status of user accounts that have been checked.



□ User Account	Description	Compliant	Checked On	Fixed On
□ blah	blah	✓ Yes	08-04-17 11:16	
□ root	root	✗ No	08-04-17 11:16	
□ user	User	✓ Yes	08-04-17 11:16	

Show Compliant

Check this box to show compliant records.

CheckIt

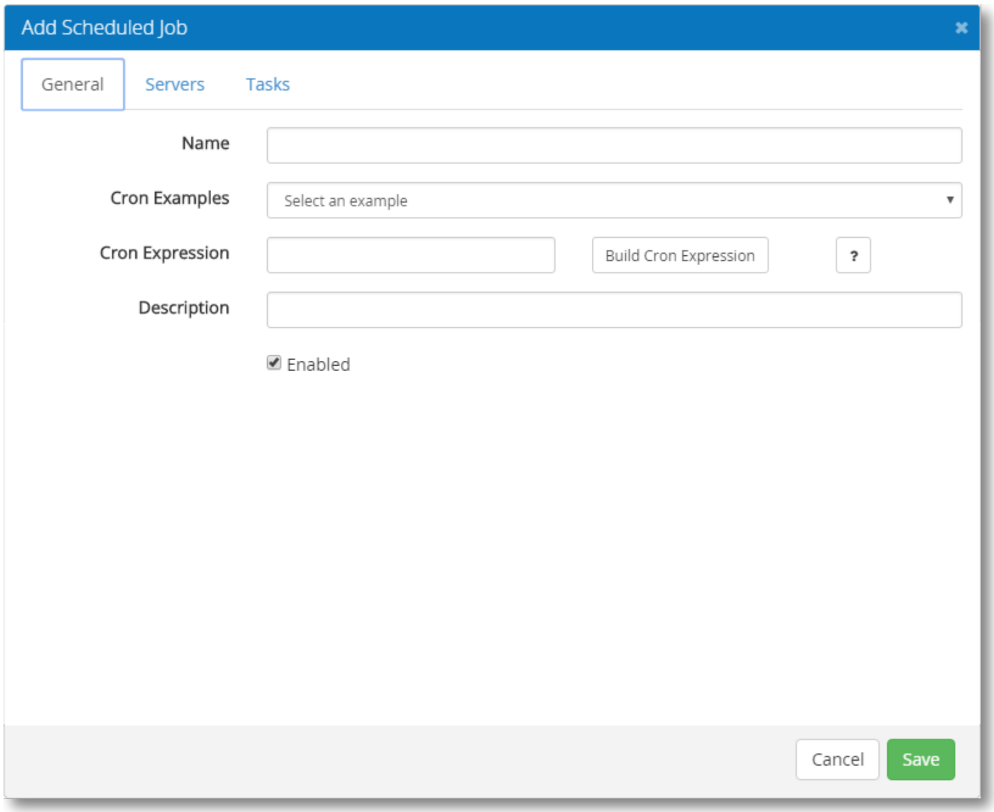
Use this button to run CheckIt, which performs a compliance check for the selected files.

Cancel • Save

Click **Cancel** to dismiss this screen without making changes. Click **Save** to save changes.

Add/Modify Scheduled Job

Use the Add Scheduled Job screen to create a new Scheduled Job. Use the Modify Scheduled Job screen to change an existing Scheduled Job.



How to Get There

To add a new Scheduled Job, choose **Admin Tasks > Manage Scheduled Jobs** and click **New**.

To change an existing scheduled job, click the Scheduled Job name.

Options

General tab

Name

Enter a name for the Scheduled Job.

Cron Examples

This drop-down list includes several cron expressions. Select one to add the code to the Cron Expression field below.

Cron Expression • Build Cron Expression

This is the cron expression code. Click **Build Cron Expression** to open http://www.cronmaker.com which includes a utility to help you build cron expressions.

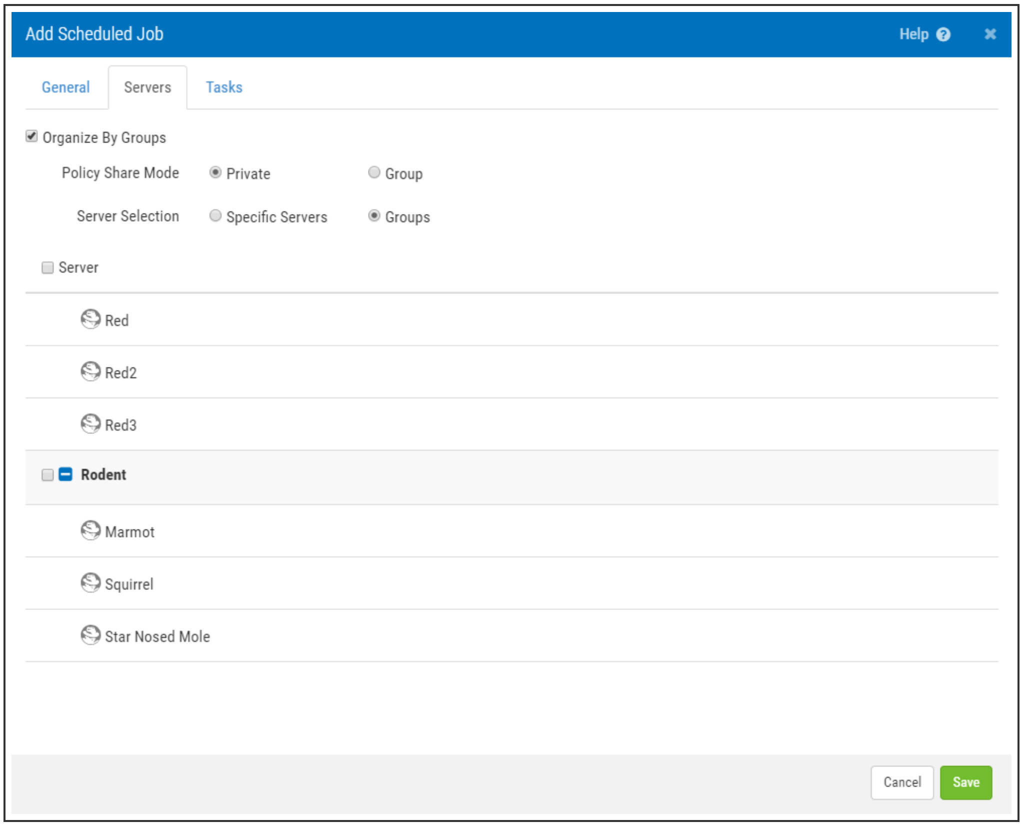
Description

This is the description of the cron expression.

Enabled

Check this box to enable the Scheduled Job.

Servers tab



☑ Organize By Groups

Policy Share Mode ● Private ○ Group

Server Selection ○ Specific Servers ● Groups

□ Server

Red

Red2

Red3

□ Rodent

Marmot

Squirrel

Star Nosed Mole

Organize by groups

Enables the Server Selection option.

Policy Share Mode; Private • Group

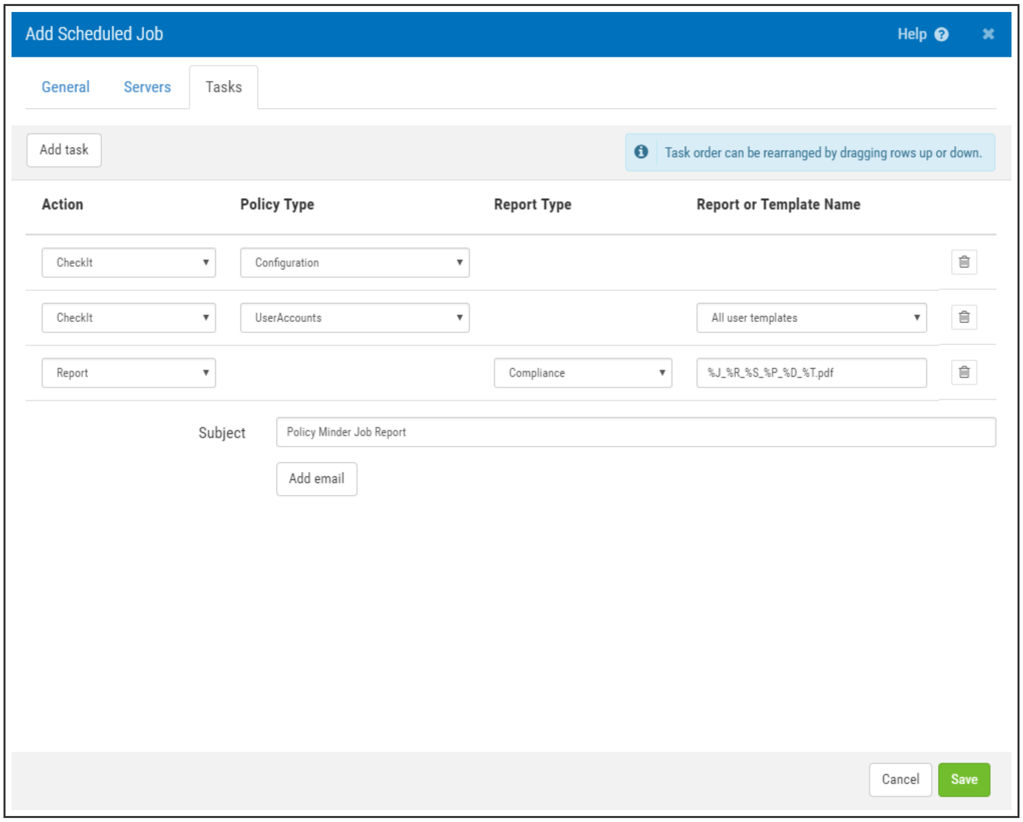
Choose **Private** to use the Private Policy assigned to the server. Choose **Group** to use the Group Policy assigned to the server. See Manage Servers screen for details.

Server Selection; Specific Servers • Groups

Choose **Specific Servers** to choose any combination of servers, regardless of the Groups they are assigned to. Choose **Groups** to limit your selection to all the Servers contained within the selected Server

Groups. If Group is selected, all servers in the Group when the job runs will be included, including any servers added to the group after the Scheduled Job was defined.

Tasks tab



Task order can be rearranged by dragging rows up or down.

Action	Policy Type	Report Type	Report or Template Name
CheckIt	Configuration		
CheckIt	UserAccounts		All user templates
Report		Compliance	%J_%R_%S_%P_%D_%T.pdf

Subject: Policy Minder Job Report

Add Task

Click **Add Task** to create a new task. A new row is added to task list below.

Task List Field Descriptions

NOTE: Task order can be rearranged by dragging rows up or down.

Action

Choose the type of action you would like the Scheduled Job to perform. Options pertaining to the Action you choose appear on the screen. See CheckIt, FixIt, and Reports for more details. Use DeleteData to delete old report data based on the Server and General settings specified.

Policy Type

For CheckIt and FixIt Actions, choose the Policy Type you would like to check or fix. See the topics under Using Security Auditor for a description of the Categories.

Report Type

This drop-down menu is available if Report is selected for the Action, and includes Security Auditor's available report types (see Create Reports screen) as well as the option to create a consolidated report with all types.

Enter and email subject in the Subject field and click **Add Email** to specify an email recipient for the report. You can click **Add Email** again to enter multiple email addresses.

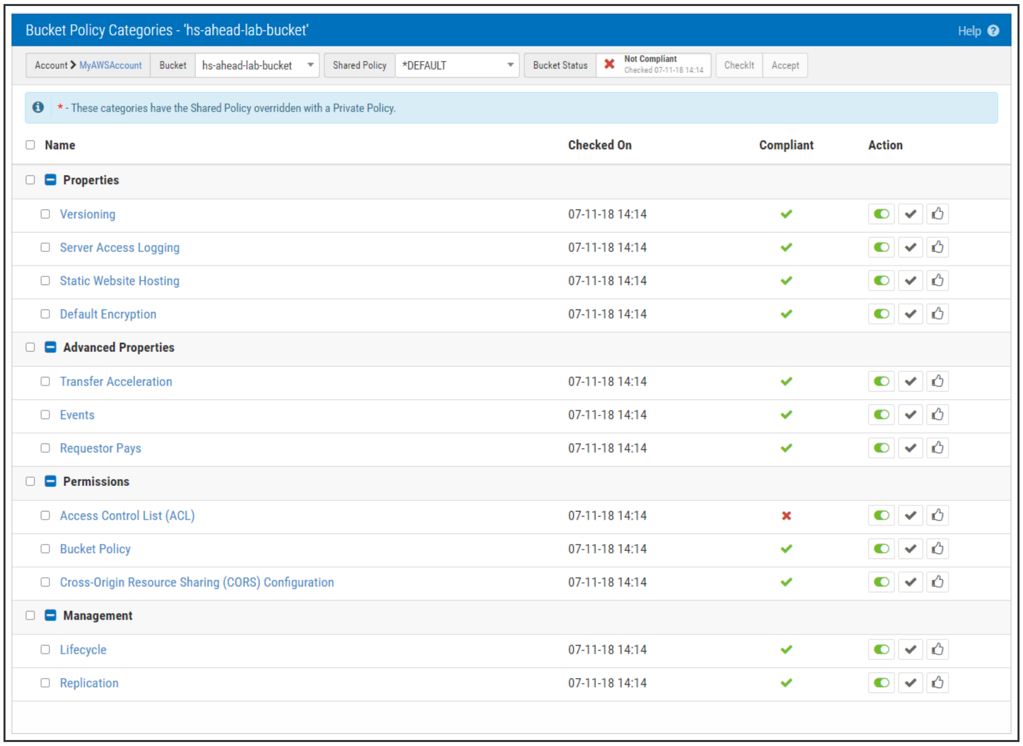
Report or Template Name

Indicate the report name. You can use the following macros: Report Type=%R, Server=%S, User=%U, Policies=%P, Date=%D, Time=%T

Cancel • Save

Click **Cancel** to dismiss the screen without making changes. Click **Save** to save changes.

Bucket Policy Categories



Bucket Policy Categories - 'hs-ahead-lab-bucket'

* - These categories have the Shared Policy overridden with a Private Policy.

Name	Checked On	Compliant	Action
Properties			
Versioning	07-11-18 14:14	✓	
Server Access Logging	07-11-18 14:14	✓	
Static Website Hosting	07-11-18 14:14	✓	
Default Encryption	07-11-18 14:14	✓	
Advanced Properties			
Transfer Acceleration	07-11-18 14:14	✓	
Events	07-11-18 14:14	✓	
Requestor Pays	07-11-18 14:14	✓	
Permissions			
Access Control List (ACL)	07-11-18 14:14	✗	
Bucket Policy	07-11-18 14:14	✓	
Cross-Origin Resource Sharing (CORS) Configuration	07-11-18 14:14	✓	
Management			
Lifecycle	07-11-18 14:14	✓	
Replication	07-11-18 14:14	✓	

How to Get There

In the Manage Service Buckets screen, click a Bucket Policy.

What it Does

This screen allows you to view, check, enable, disable, or accept S3 Bucket categories. For example, you can use this screen to override Shared Bucket Policy category settings with a Private Policy category setting for cases that require the value of a specific Bucket to differ from the general Shared Bucket Policy.

Options

Account > *[Account Name]* • Bucket

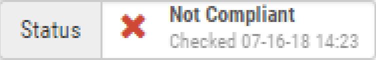
This indicates the current AWS Account. Click the account name to return to the Manage Service Buckets screen where you can select from the full list of Buckets in the AWS account. Or, choose a different S3 Bucket from the adjacent Bucket drop-down list.

Shared Policy

This drop-down list includes the Shared Bucket Policies defined in the Manage Shared Bucket Policy screen. Choose a Shared Policy from this list and use the CheckIt Action to check it against the available

S3 Bucket settings.

Status


Status ✖ Not Compliant
Checked 07-16-18 14:23

The status of S3 Bucket Policy. Not checked ✱, Not Compliant ✖ , or Compliant ✓. The date and time this policy was last checked is also displayed.

CheckIt CheckIt

Select one or more Categories and click CheckIt to compare them with either the currently selected Shared Bucket Policy, or the Private Policy (indicated with a * for the setting). Review the "Compliant" column to identify whether each Bucket is compliant or not.

Accept Accept

Select one or more categories and click Accept, then confirm, to redefine the Bucket Policy category settings to match that of the S3 Bucket.

Columns

Name

The name of the S3 Bucket category. Click the Name to open the corresponding Bucket Policy Category Details screen, where you can view details, check the setting against the policy, or accept the setting as part of the policy.

Checked On

The date and time the Bucket Policy category was last checked.

Compliant

This column shows the status of each S3 Bucket category: Not checked ✱, Not Compliant ✖ , or Compliant ✓.

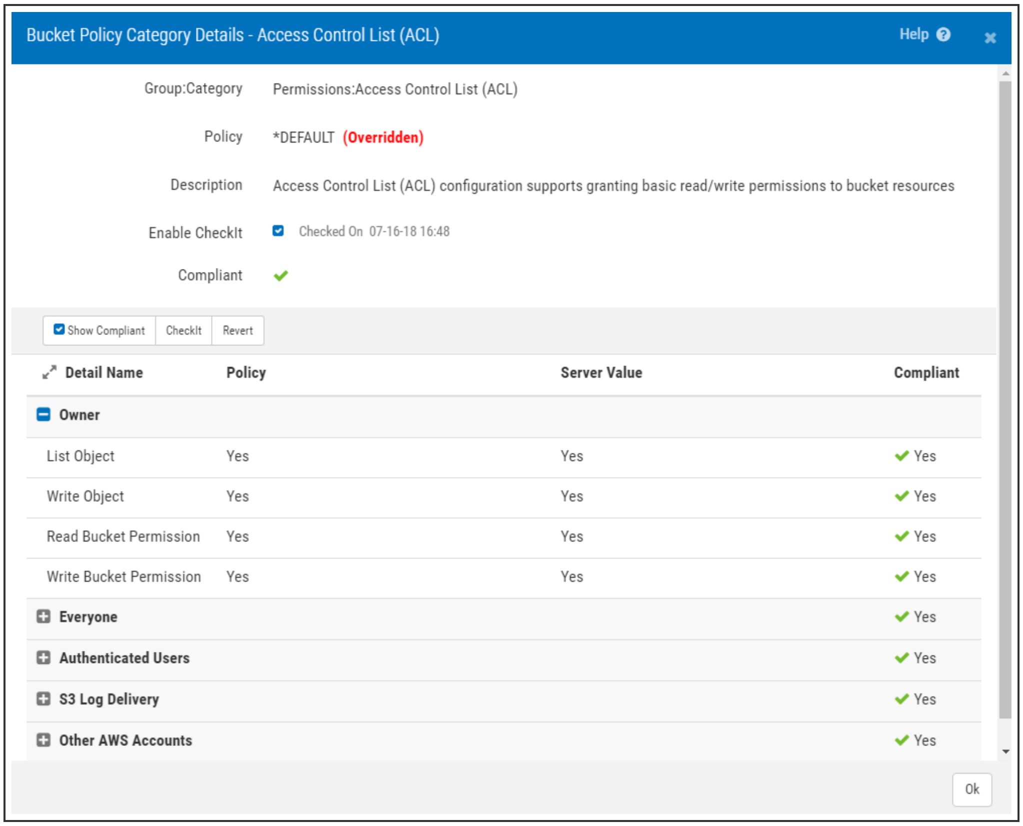
Action

- Click ● **(Disable CheckIt)** or ○ **(Enable CheckIt)** to turn CheckIt off or on, respectively. If set to Disable, the category will not be included when CheckIt is run for Bucket (see Manage Service Buckets screen).
- Click ✓ to run CheckIt for the category.
- Click 👍 to accept the S3 Bucket server values into the Private Policy.

  > **NOTE:** * indicates categories that have been overridden with a Private Policy.

- Click ↺ to revert the category back to the Shared Policy.

Bucket Policy Category Details



Bucket Policy Category Details - Access Control List (ACL)

Group:Category	Permissions:Access Control List (ACL)
Policy	*DEFAULT **(Overridden)**
Description	Access Control List (ACL) configuration supports granting basic read/write permissions to bucket resources
Enable CheckIt	☑ Checked On 07-16-18 16:48
Compliant	✓

Detail Name	Policy	Server Value	Compliant
⊟ **Owner**			
List Object	Yes	Yes	✓ Yes
Write Object	Yes	Yes	✓ Yes
Read Bucket Permission	Yes	Yes	✓ Yes
Write Bucket Permission	Yes	Yes	✓ Yes
⊞ **Everyone**			✓ Yes
⊞ **Authenticated Users**			✓ Yes
⊞ **S3 Log Delivery**			✓ Yes
⊞ **Other AWS Accounts**			✓ Yes

How to Get There

On the Bucket Policy Category screen, click the name of a Category.

What it Does

This screen includes a description of the Bucket setting and additional details including the server value. It also allows you to run CheckIt, Accept the value as the Policy value, and Revert to the Shared Bucket Policy.

Options

Show Compliant

Check this option to show server values compliant with the policy.

CheckIt

Click this button to run CheckIt for the category.

Accept As Policy

Click this button to accept these S3 Bucket server values into the Private Policy, overriding the Shared Policy.

Revert

Click this button to revert the policy setting back to that of the Shared Policy.

Columns

Detail Name

The name of the S3 Bucket setting.

Policy

The value of the Security Auditor policy.

Server Value

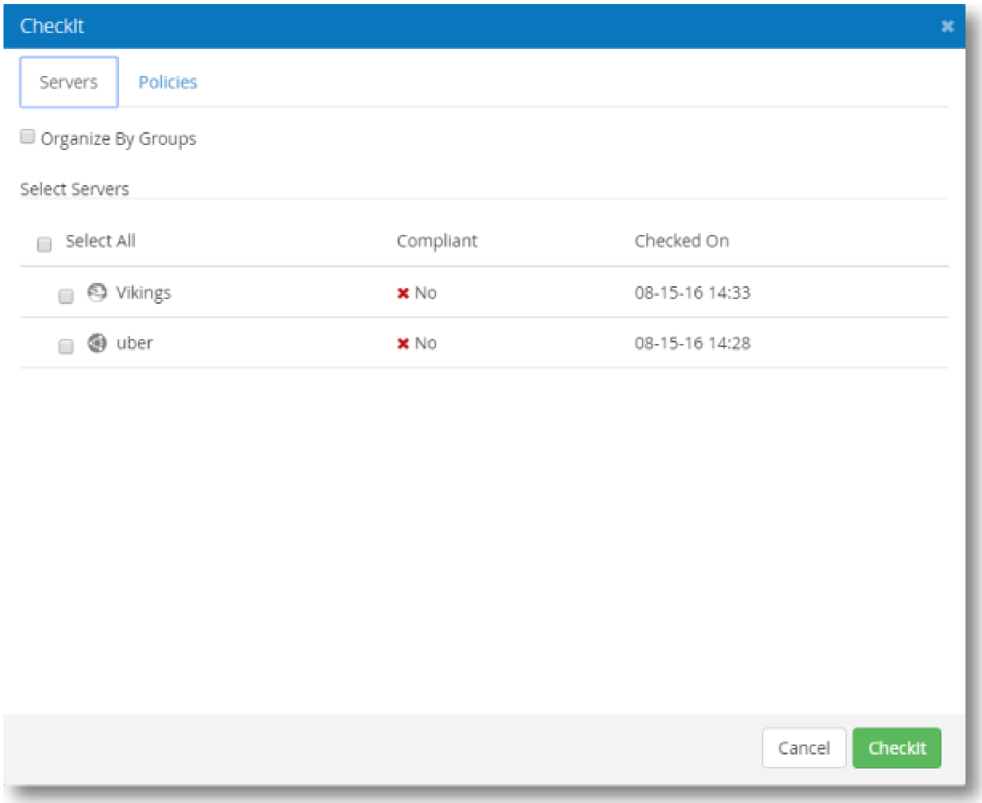
The value of the S3 Bucket Setting on the server.

Compliant

The status of each value: Not checked ✱, Not Compliant ✖ , or Compliant ✓.

CheckIt Screen

CheckIt will go to the selected servers and check attributes of selected Policies.



☐ Select All	Compliant	Checked On
☐ Vikings	✖ No	08-15-16 14:33
☐ uber	✖ No	08-15-16 14:28

How to get there

Choose **Servers** > **CheckIt**.

Servers tab

Organize By Groups

Check Organize By Groups to organize the following policies by group.

Select Servers

Select All

Check Select All to select all of the servers.

Field Descriptions

Compliant

This column indicates if the server is compliant, not compliance, or not checked.

Checked On

This column indicates when the server was checked.

Policies tab

Select Policy Categories

CheckIt will go to the selected Servers and check attributes of selected Policies.

Select All

Check Select All to select all of the policy categories.

Configuration

This will check for configuration policy.

Exported Directories

This will check for exported directories policy.

Daemons

This will check for daemons policy.

User Accounts; Selected • All

This function allows for selected or all user accounts to be checked.

Files; Selected • All

This function allows for selected or all files to be checked.

Scripts; Selected • All

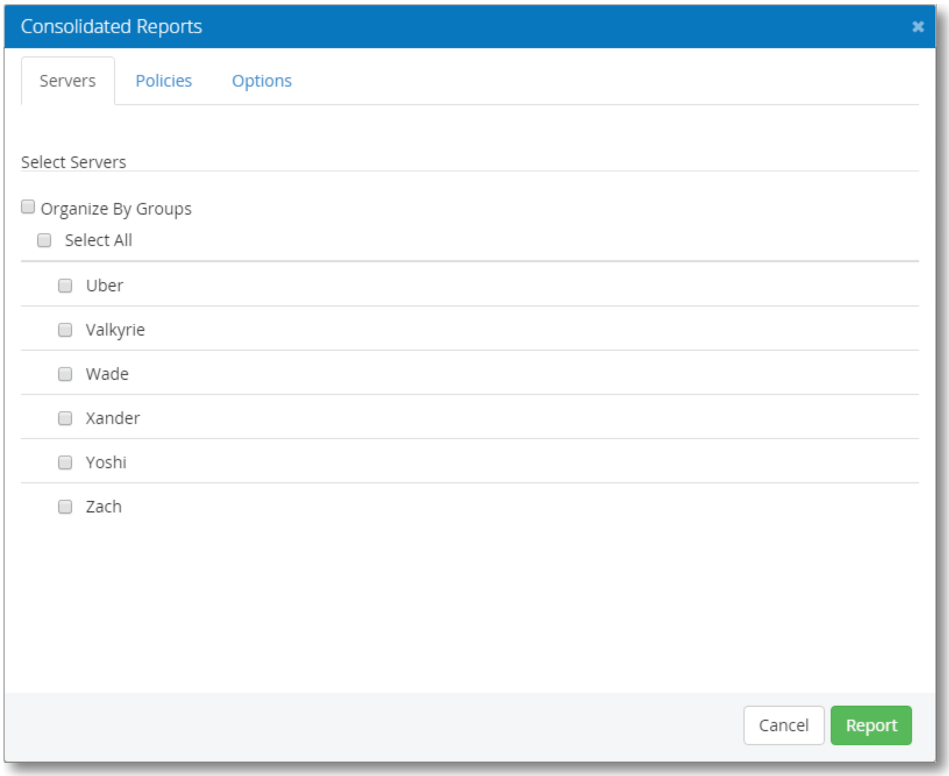
This function allows for selected of all scripts to be checked.

Cancel • CheckIt

Chick **Cancel** to dismiss this screen without making changes. Click **CheckIt** to perform CheckIt on the selected policy categories.

Consolidated Reports screen

This screen allows you to select the policies and servers to include in your report.



Select Servers

□ Organize By Groups

□ Select All

□ Uber

□ Valkyrie

□ Wade

□ Xander

□ Yoshi

□ Zach

How to get there

Choose **Servers** > **Create Consolidated Reports**.

Servers tab

Select Servers

Organize By Groups

Check Organize By Groups to organize the following servers by group.

Select All

Check Select All to select all of the following server categories.

Policies tab

Select Policy Categories

Select All

Check Select All to select all of the following policy categories.

Configuration

Check this box to include the configuration policy.

Exported Directories

Check this box to include the exported directories policy.

Daemons

Check this box to include the daemons policy.

Scripts; Selected • All

This allows for reports to be run on only selected or all scripts.

Options tab

Report Options

Report Name

This is where the report name should be entered.

Output Options

Non-compliant

Report on non-compliant entities or attributes only.

Both

Report on all checked entities or attributes.

Show Compliance

This options shows the compliance report.

Show Policy Value

This option shows the policy value report.

Show Server Value

This option shows the server value report.

Email Reports

Add Email

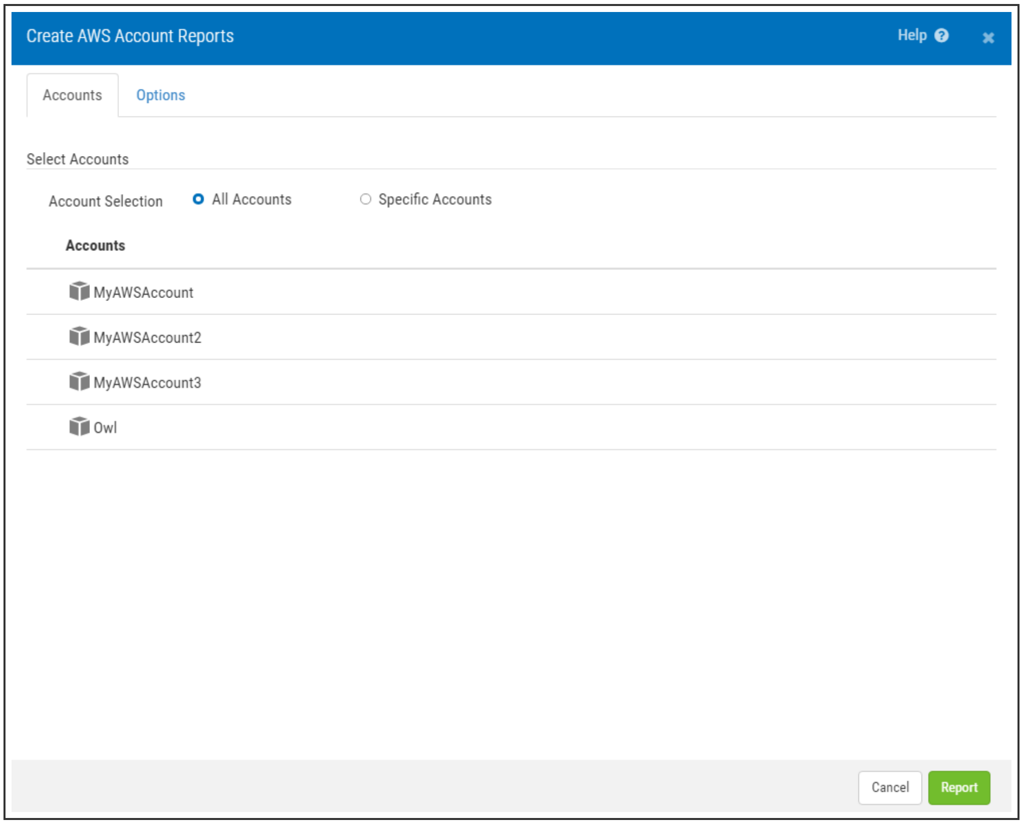
Add an email for the reports to get sent to.

Cancel • Save

Click **Cancel** to dismiss this screen without creating a report. Click **Report** to generate the report based on your settings. You arrive at the View Reports screen where your new report is available for viewing.

Create AWS Account Reports screen

Use this screen to create an AWS Account report.



Select Accounts

Account Selection ● All Accounts ○ Specific Accounts

Accounts

MyAWSAccount

MyAWSAccount2

MyAWSAccount3

Owl

How to get there

Choose **AWS Accounts** > **Create Reports**.

Accounts tab

Select Accounts

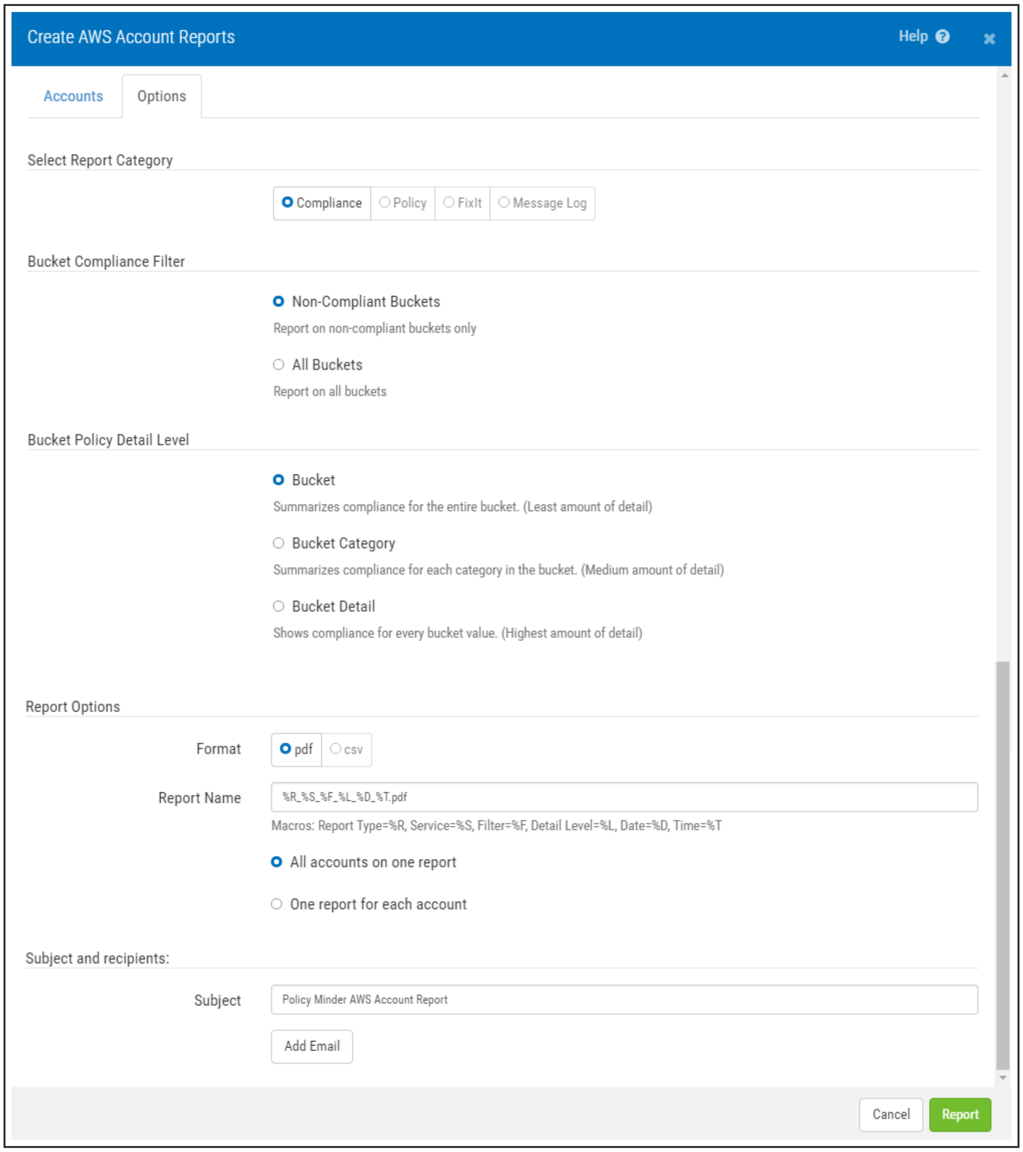
Account Selection; All Accounts • Specific Accounts

Choose **All Accounts** to indicate the report should include data from all AWS accounts. Choose **Specific Accounts** to display a check box next to each account, which allows you to specify the accounts that should be included in the report.

Accounts

This is the list of AWS accounts configured in Security Auditor. See Manage AWS Cloud Service Reports screen.

Options tab



Select Report Category

● Compliance ○ Policy ○ FixIt ○ Message Log

Bucket Compliance Filter

● Non-Compliant Buckets
Report on non-compliant buckets only

○ All Buckets
Report on all buckets

Bucket Policy Detail Level

● Bucket
Summarizes compliance for the entire bucket. (Least amount of detail)

○ Bucket Category
Summarizes compliance for each category in the bucket. (Medium amount of detail)

○ Bucket Detail
Shows compliance for every bucket value. (Highest amount of detail)

Report Options

Format: ● pdf ○ csv

Report Name: %R_%S_%F_%L_%D_%T.pdf
Macros: Report Type=%R, Service=%S, Filter=%F, Detail Level=%L, Date=%D, Time=%T

● All accounts on one report

○ One report for each account

Subject and recipients:

Subject: Policy Minder AWS Account Report

Add Email

Select Report Category

Compliance

This option gives a report on compliance.

Policy

This option gives a report on policy details.

FixIt

This option gives a report on FixIt activity.

Message Log

This report gives a report on the Security Auditor message log.

Bucket Compliance Filter

Non-Compliant Buckets

Choose this option to report only on Buckets that include at least one non-compliant value.

All Buckets

Choose this option to report on both compliant and non-compliant Buckets.

Bucket Policy Detail Level

Bucket

Summarizes compliance for the entire Bucket. This option includes the least amount of detail.

Bucket Category

Summarizes compliance for each category in the Bucket. This option includes a medium amount of detail.

Bucket Detail

Shows compliance for every bucket value. This option includes the highest amount of detail.

Report Options

Format; pdf • csv

This gives the option of receiving the report in pdf or csv format.

> **NOTE:** csv is not currently a supported format.

Report Name; All accounts on one report • One account for each server

This is where the report is named. The Report name macros are:

- Report Type=%R
- Service=%S
- Filter=%F
- Detail Level=%L
- Date=%D
- Time=%T

All accounts can be on one report, or one account can be made for each server.

Subject and Recipients

Use these options to specify details about the emailed report.

Subject

Enter the subject of the email to be sent.

Add Email

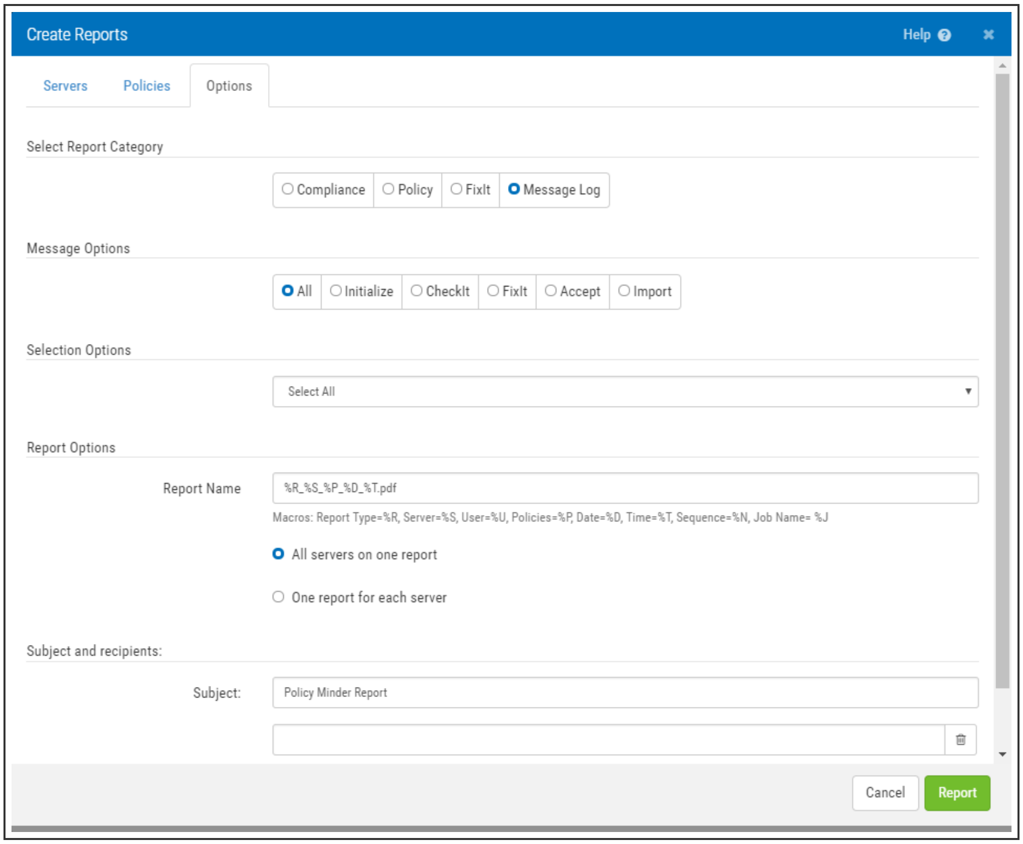
Click this button and enter the email address the report should be sent to. Repeat for additional email addresses.

Cancel • Report

Click **Cancel** to dismiss this screen without creating a report. Click **Report** to generate the report based on your settings. You arrive at the View Reports screen where your new report is available for viewing. Reports are emailed as PDF attachments to the email addresses specified.

Create Reports screen

Use this screen to create a Compliance, Policy, FixIt, or Message Log report.



Select Report Category

○ Compliance ○ Policy ○ FixIt ● Message Log

Message Options

● All ○ Initialize ○ CheckIt ○ FixIt ○ Accept ○ Import

Selection Options

Select All

Report Options

Report Name: %R_%S_%P_%D_%T.pdf

Macros: Report Type=%R, Server=%S, User=%U, Policies=%P, Date=%D, Time=%T, Sequence=%N, Job Name= %J

● All servers on one report

○ One report for each server

Subject and recipients:

Subject: Policy Minder Report

How to get there

Choose **Reports** > **Create Reports**. Or, choose **Servers** > **Create Reports**.

Servers tab

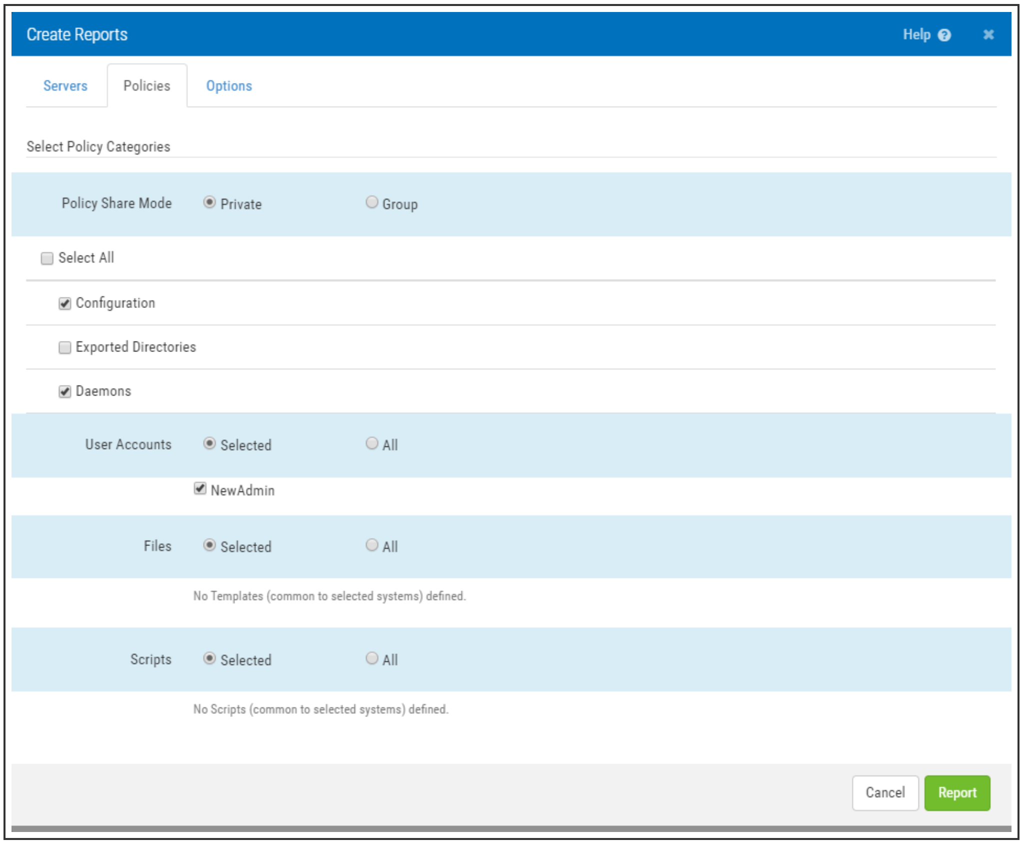
Organize By Groups

Check Organize By Groups to organize the following servers by group.

Select All

Check Select All to select all of the servers.

Policies tab



Select Policy Categories

Policy Share Mode ● Private ○ Group

□ Select All

☑ Configuration

□ Exported Directories

☑ Daemons

User Accounts ● Selected ○ All

☑ NewAdmin

Files ● Selected ○ All

No Templates (common to selected systems) defined.

Scripts ● Selected ○ All

No Scripts (common to selected systems) defined.

Select Policy Categories

Policy Share Mode; Private • Group

Choose **Private** to show Private Policies on the report. Choose **Group** to show Group Policies on the report. See Policy Overview for details on Private and Group Policies.

Select All

Choose this option to select all of the following policy categories.

Configuration

Check this box to include the configuration policy.

Exported Directories

Check this box to include the exported directories policy.

Daemons

Check this box to include the daemons policy.

User Accounts; Selected • All

This function allows for selected or all user accounts to be checked.

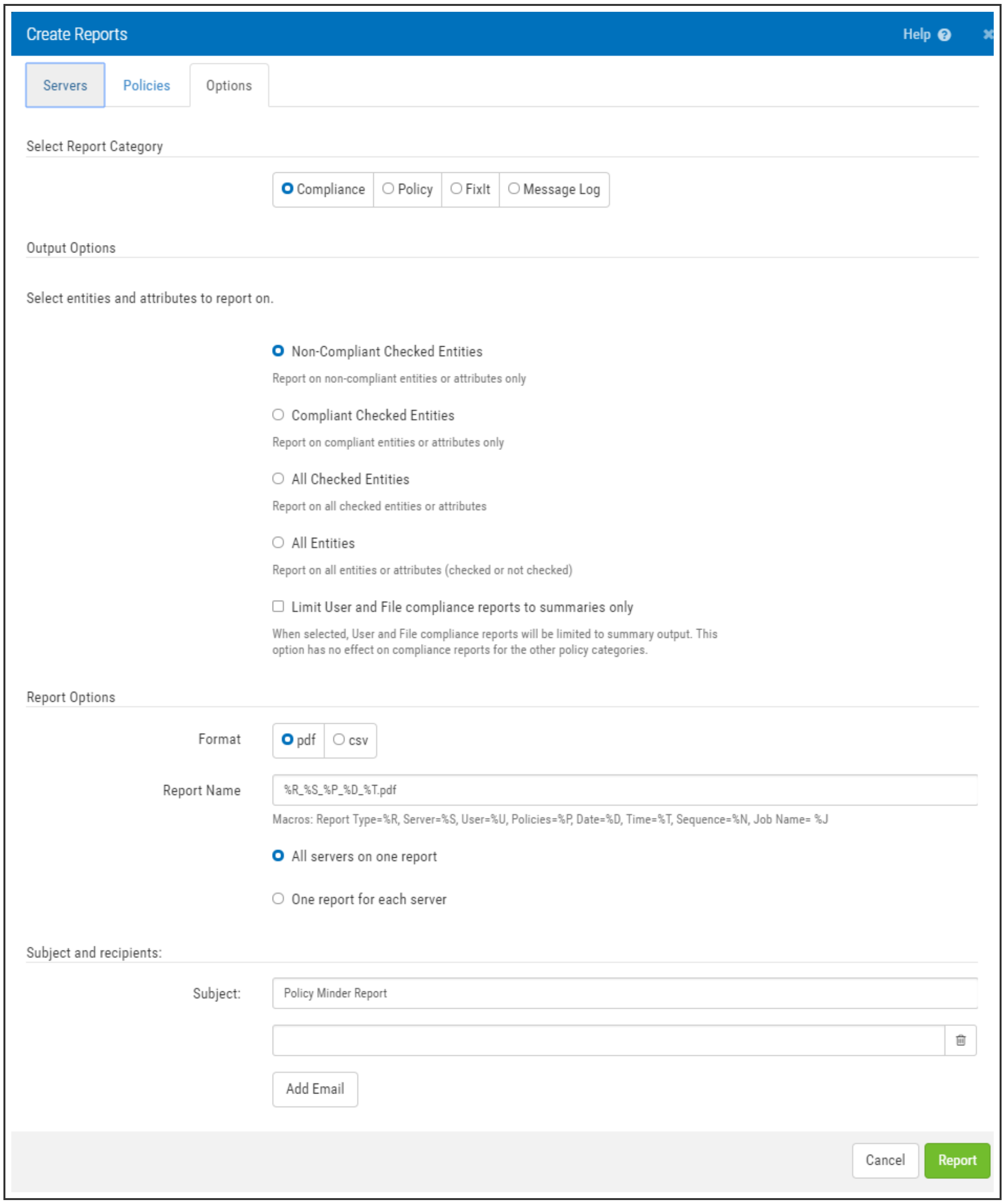
Files; Selected • All

This function allows for selected or all files to be checked.

Scripts; Selected • All

This function allows for selected of all scripts to be checked.

Options tab



Create Reports

Select Report Category

● Compliance ○ Policy ○ FixIt ○ Message Log

Output Options

Select entities and attributes to report on.

● Non-Compliant Checked Entities
Report on non-compliant entities or attributes only

○ Compliant Checked Entities
Report on compliant entities or attributes only

○ All Checked Entities
Report on all checked entities or attributes

○ All Entities
Report on all entities or attributes (checked or not checked)

□ Limit User and File compliance reports to summaries only
When selected, User and File compliance reports will be limited to summary output. This option has no effect on compliance reports for the other policy categories.

Report Options

Format: ● pdf ○ csv

Report Name: %R_%S_%P_%D_%T.pdf

Macros: Report Type=%R, Server=%S, User=%U, Policies=%P, Date=%D, Time=%T, Sequence=%N, Job Name= %J

● All servers on one report

○ One report for each server

Subject and recipients:

Subject: Policy Minder Report

Select Report Category

Compliance

This option gives a report on compliance.

Policy

This option gives a report on policy details.

FixIt

This option gives a report on FixIt activity.

Message Log

This report gives a report on the Security Auditor message log.

Report Options

Format; pdf • csv

This gives the option of receiving the report in pdf or csv format.

Report Name; All servers on one report • One report for each server

This is where the report is named. All servers can be on one report, or one report can be made for each server.

Output Options

When **Compliance** is selected, the following options are available:

- **Summary Only (for Users and Files).** If true, only summaries are reported for Users and Files (and other output options don't apply).
- **Non-Compliant.** Report on non-compliant entities or attributes only.
- **Compliant Checked Entities.** Report on complaint entities or attributes only.
- **All Checked Entities.** Report on all checked entities or attributes.
- **All Entities.** Report on all entities or attributes (checked or not checked).
- **Limit User and File compliance reports to summaries only.** When selected, User and File compliance reports will be limited to summary output. This option has no effect on compliance reports for the other policy categories.

Message Options

When Message Log is selected, the following options appear:

All • Initialize • CheckIt • FixIt • Accept • Import.

Choose All to include all messages on the report. Or, choose one of the available message types to include it on the report.

Selection Options

When **FixIt** is selected, the following options are available:

Date Range; Select All • Date Range

Choose Date Range and specify a 'from' and 'to' date to identify a range of activity to include on the report. Choose Select All to include data without any date restriction.

Report Options

Report Name

Indicate the report name. You can use the following macros: Report Type=%R, Server=%S, User=%U, Policies=%P, Date=%D, Time=%T

Subject and recipients

Use these options to specify details about the emailed report.

Subject

Enter the subject of the email to be sent.

Add Email

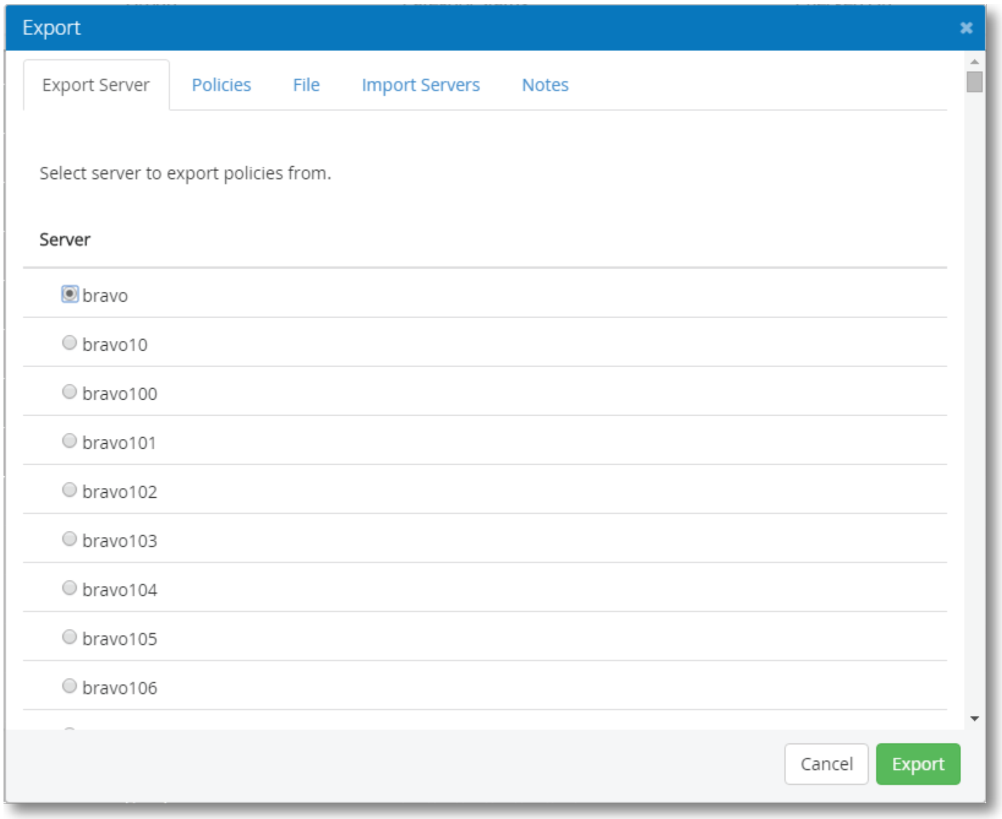
Click this button and enter the email address the report should be sent to. Repeat for additional email addresses.

Cancel • Report

Click **Cancel** to dismiss this screen without creating a report. Click **Report** to generate the report based on your settings. You arrive at the View Reports screen where your new report is available for viewing. Reports are emailed as PDF attachments to the email addresses specified.

Export screen

This screen allows you to export policies from a server.



Select server to export policies from.

Server

- ● bravo
- ○ bravo10
- ○ bravo100
- ○ bravo101
- ○ bravo102
- ○ bravo103
- ○ bravo104
- ○ bravo105
- ○ bravo106

How to get there

Choose **Servers** > **Export**.

Export Server tab

Server

Servers are listed that can have policies exported from.

Policies tab

Select Policy Categories

Select All

Check Select All to select all of the following policy categories.

Configuration

Check this box to include the configuration policy.

Exported Directories

Check this box to include the exported directories policy.

Daemons

Check this box to include the daemons policy.

User Accounts; Selected • All

This function allows for selected or all user accounts to be checked.

Files; Selected • All

This function allows for selected or all files to be checked.

Scripts; Selected • All

This function allows for selected of all scripts to be checked.

File tab

Create output file

This option creates an output file.

There is an exports directory in the installation area:

C:\Program Files (x86)\PowerTech\SecurityAuditor\tomcat\webapps\securityauditor\exports

File Name

This is where the file name is listed. For a list of file macros, see Export Scripts Package.

Import Servers tab

Select the servers to import policies to

Organize By Groups

Check Organize By Groups to organize the following servers by group.

Select All

Check Select All to select all of the following server categories.

Notes tab

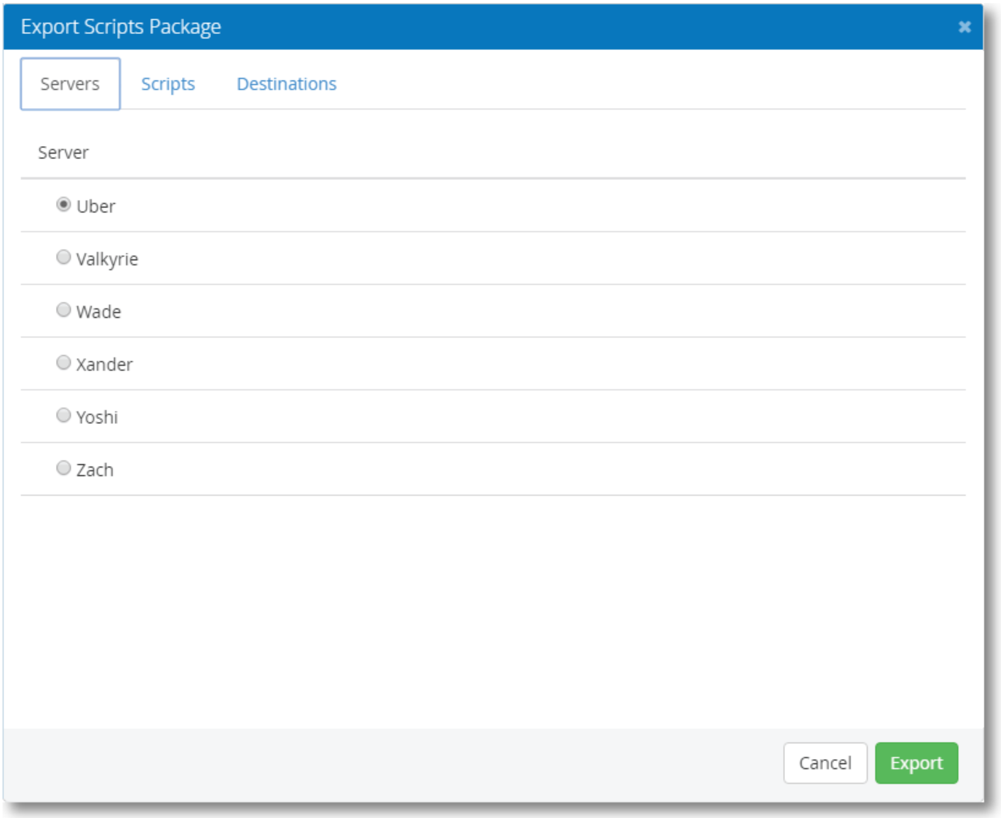
This is an area to add notes.

Cancel • Export

Click **Cancel** to dismiss this screen without exporting. Click **Export** to export the policies based on your settings.

Export Scripts Package

Use this screen to export a scripts package.



Server

● Uber

○ Valkyrie

○ Wade

○ Xander

○ Yoshi

○ Zach

How to Get There

Choose **Admin Tasks** > **Scripts** > **Export Package**

Servers tab

Server

Select the server you would like to export scripts from.

Scripts tab

Select all Scripts Policies you would like to export.

Destinations tab

File Name

Macros:

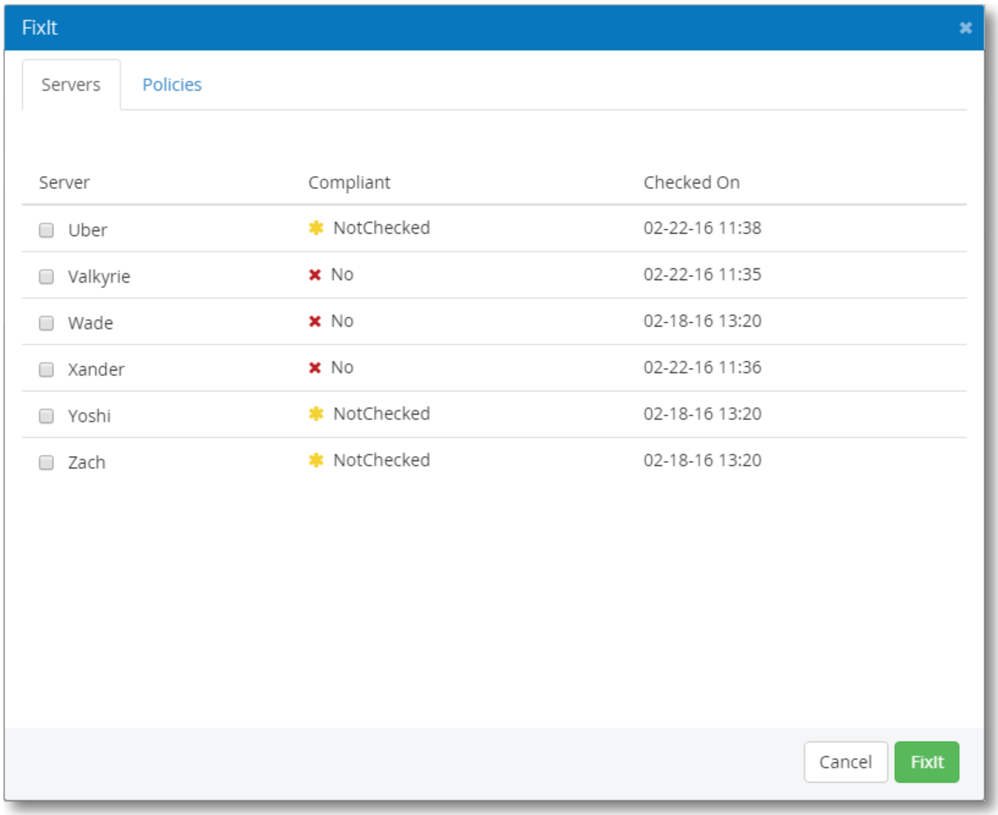
- Report Type=%R
- Server=%S
- User=%U
- Policies=%P
- Date=%D
- Time=%T
- Sequence=%N
- Job Name=%J

Cancel • Export

Click **Cancel** to dismiss this screen without exporting. Click **Export** to export the policies based on your settings.

FixIt Screen

Use this screen to run FixIt.



Server	Compliant	Checked On
□ Uber	✱ NotChecked	02-22-16 11:38
□ Valkyrie	✖ No	02-22-16 11:35
□ Wade	✖ No	02-18-16 13:20
□ Xander	✖ No	02-22-16 11:36
□ Yoshi	✱ NotChecked	02-18-16 13:20
□ Zach	✱ NotChecked	02-18-16 13:20

How to get there

Choose **Servers** > **FixIt**.

Servers tab

Organize By Groups

Check Organize By Groups to organize the following servers by group.

Select Servers

Select All

Check Select All to select all of the following server categories.

Policies tab

Select Policy Categories

Select All

Check Select All to select all of the following policy categories.

Configuration

Check this box to include the configuration policy.

Daemons

Check this box to include the daemons policy.

User Accounts; Selected • All

This function allows for selected or all user accounts to be checked.

Files; Selected • All

This function allows for selected or all files to be checked.

Scripts; Selected • All

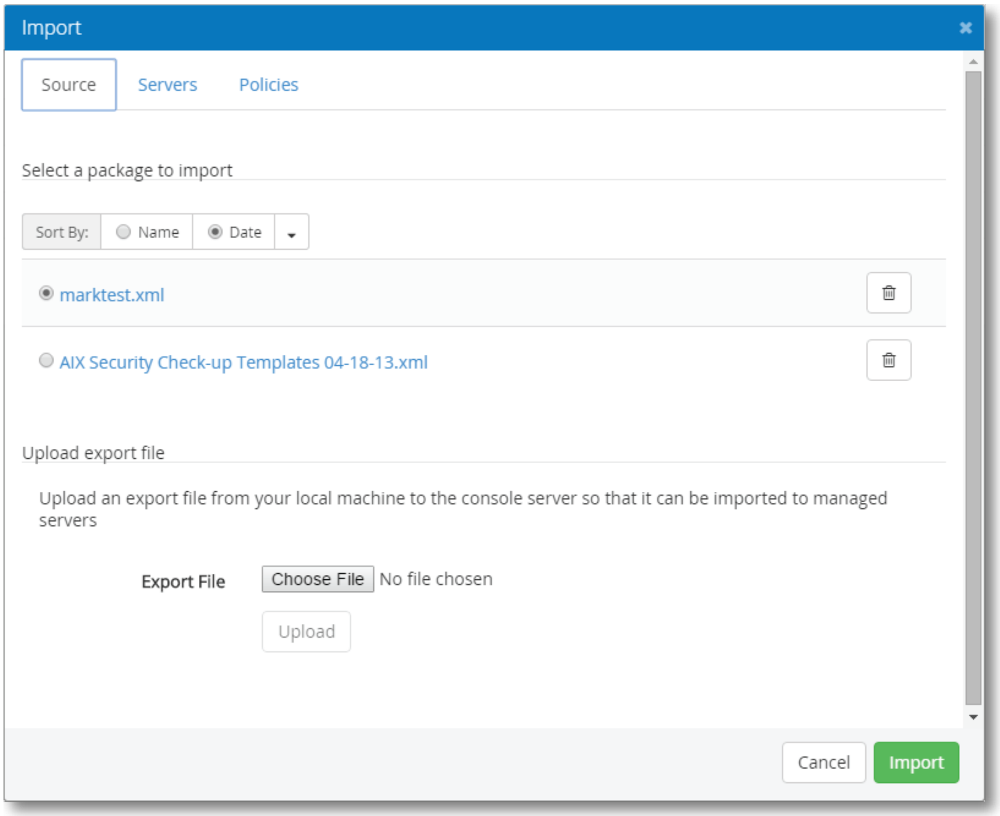
This function allows for selected of all scripts to be checked.

Cancel • FixIt

Choose **Cancel** to dismiss this screen without applying FixIt. Choose **FixIt** to run FixIt based on your settings.

Import screen

Use this screen to import policies.



Select a package to import

Sort By: ○ Name ● Date

● marktest.xml

○ AIX Security Check-up Templates 04-18-13.xml

Upload export file

Upload an export file from your local machine to the console server so that it can be imported to managed servers

Export File: Choose File No file chosen

Upload

How to get there

Choose **Servers > Import**.

Source tab

Select a package to import

Sort By: Name • Date

This allows import packages to be sorted by name or date.

File Name

This is where the file that can be imported are located.

Upload export file

Export File; Choose File • Upload

This is where to choose the files to export and then upload the files.

Servers tab

Select the servers to import policies to

Organize By Groups

Check Organize By Groups to organize the following servers by group.

Select All

Check Select All to select all of the following servers categories.

Policies tab

Select the policy categories to import

Overwrite Policies

If true policies with the same name are replaced, otherwise they are skipped.

Run CheckIt (after import)

If checked CheckIt will be run for imported policies after import.

Select All

Check Select All to select all of the following policy categories.

Configuration

Check this box to include the configuration policy.

User Accounts; Selected • All

This checks for either selected or all of the user account policies listed below.

Files; Selected • All

This checks for either selected or all of the file policies listed below.

Scripts; Selected • All

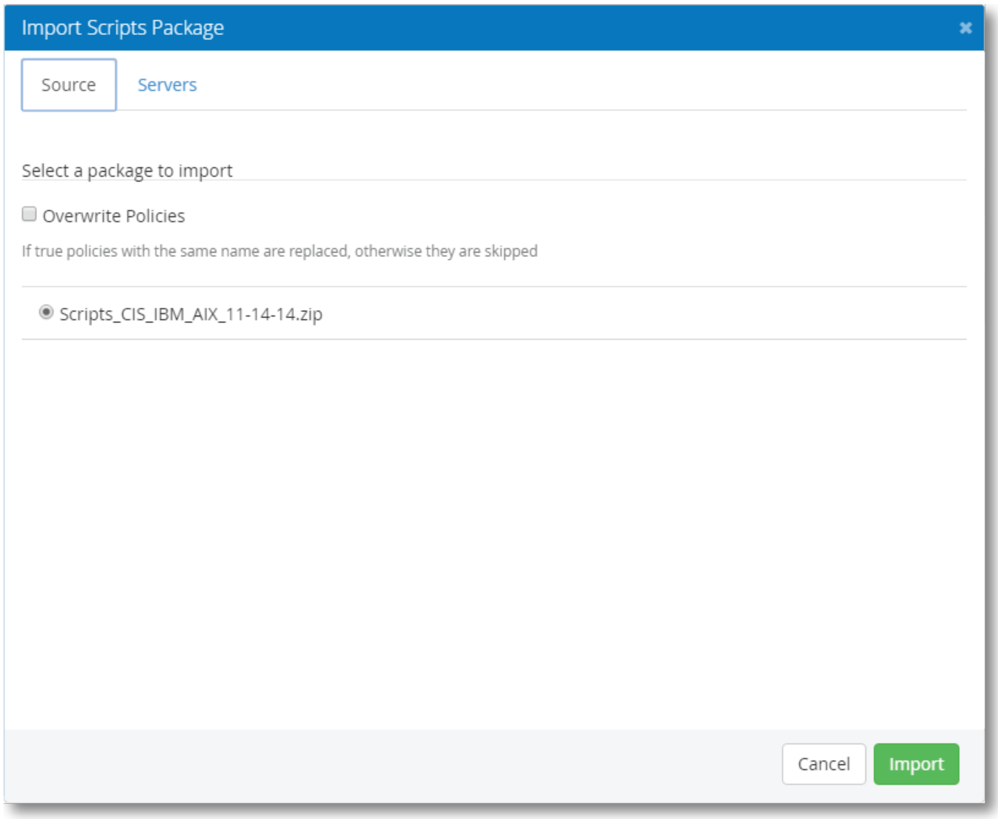
This allows for only selected or all scripts to be defined.

Cancel • Import

Click **Cancel** to dismiss this screen without importing. Click **Import** to import the policies based on your settings.

Import Scripts Package screen

Use this screen to import a policy package.



Import Scripts Package

Select a package to import

□ Overwrite Policies

If true policies with the same name are replaced, otherwise they are skipped

● Scripts_CIS_IBM_AIX_11-14-14.zip

How to get there

Choose **Admin Tasks** > **Scripts** > **Import Package**.

Source tab

Select a package to import

Overwrite policies

If true, policies with the same name are replaced, otherwise they are skipped

Servers tab

Select the servers to import policies to

Organize By Groups

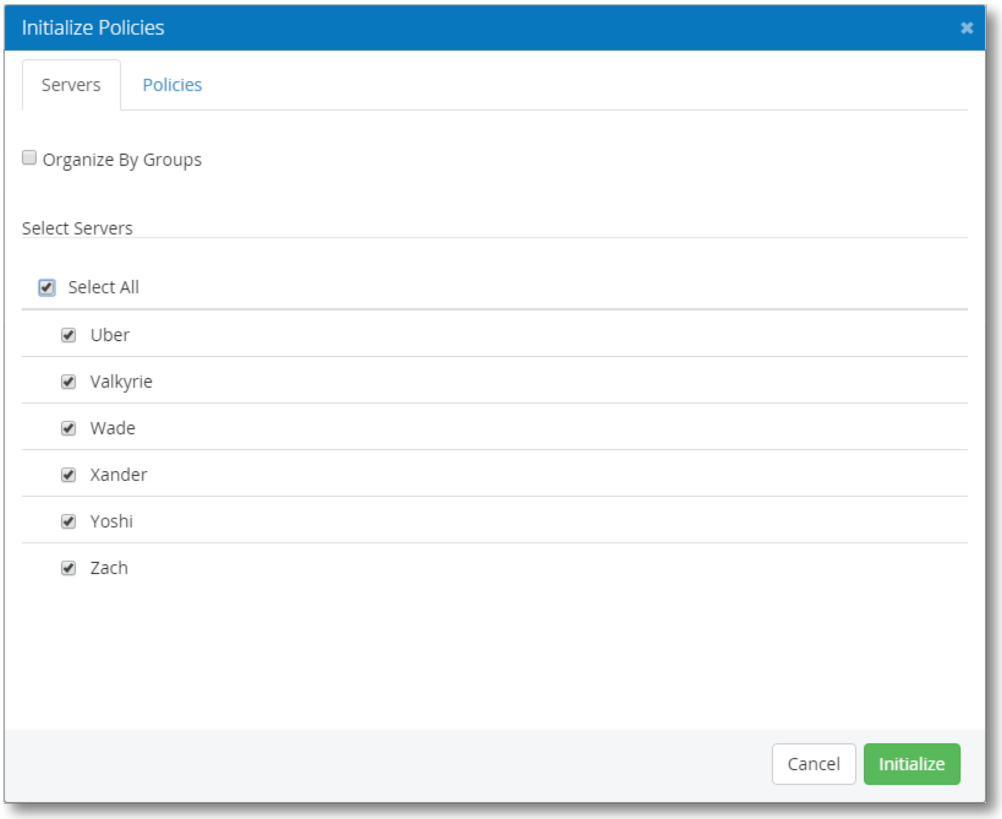
Check Organize By Groups to organize the following servers by group.

Select All

Check Select All to select all of the following server categories.

Initialize Policies screen

Use this screen to identify which servers and policies you want to initialize.



□ Organize By Groups

Select Servers

☑ Select All

☑ Uber

☑ Valkyrie

☑ Wade

☑ Xander

☑ Yoshi

☑ Zach

How to get there

Choose **Servers** > **Initialize Policies**.

Servers tab

Organize By Groups

Check Organize By Groups to organize the following servers by group.

Select Servers

Select All

Check Select All to select all of the following server categories.

Policies tab

Initialization will gather the current values in each category selected and use those settings as your policy settings for that category. Existing policies are replaced.

Select Policy Categories

Select All

Check Select All to select all of the following server categories.

Configuration

Check this box to include the configuration policy.

Exported Directories

Check this box to include the exported directories policy.

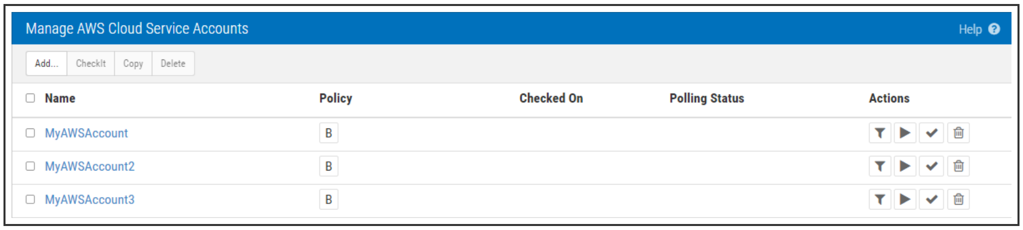
Daemons

Check this box to include the daemons policy.

Cancel • Import

Click **Cancel** to dismiss this screen without initializing. Click **Initialize** to initialize the selected policies on the selected servers.

Manage AWS Cloud Service Accounts



□ Name	Policy	Checked On	Polling Status	Actions
□ MyAWSAccount	B			▼ ▶ ✓ 🗑
□ MyAWSAccount2	B			▼ ▶ ✓ 🗑
□ MyAWSAccount3	B			▼ ▶ ✓ 🗑

How to get there

Choose **AWS Accounts** > **Manage AWS Accounts**.

What it Does

Use the Manage AWS Cloud Service Accounts screen to define an Amazon AWS cloud service account.

Options

Add

Click **Add** to open the Add Cloud Service Account screen, where you can setup a new AWS account with Security Auditor.

CheckIt

Click **CheckIt** to check S3 buckets in the selected AWS accounts for compliance.

Copy

Click **Copy** to create a copy of selected AWS accounts. When you do so, Security Auditor duplicates the name with "_copy#" appended.

Delete

Check one or more accounts and click **Delete** to delete it from Security Auditor.

Column Descriptions

Name

The name of the AWS account.

Policy

Click the "B" button in the Policy column to open the Manage Service Buckets screen for the account. The color of the button depends on the status of the Buckets in the account.

B = Not Checked

B = Not Compliant

B = Compliant

> **NOTE:** See Managing S3 Bucket Policies.

Checked On

The date and time CheckIt was last run on the account.

Polling Status

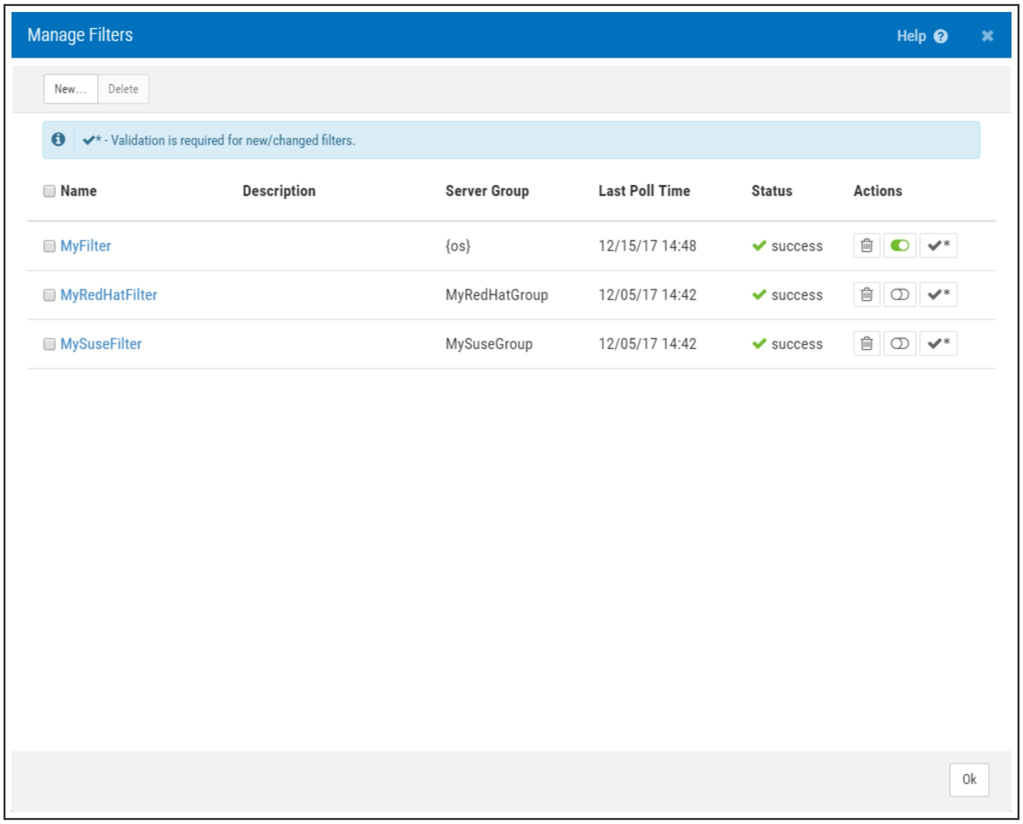
The most recent time the cloud service account was polled. Polling frequency and other polling settings can be configured on the Cloud Services tab of the Preferences screen.

Actions

Use these buttons to perform cloud service account actions.

- Click ⏷ **(Edit Filters)** to open the Manage Filters screen where you can configure cloud service discovery settings.
- Click ▶ **(Poll Service)** to poll the cloud service account using the filter settings specified.
- Click ✓ **(CheckIt)** to check S3 Buckets in the account.
- Click 🗑 **(Delete)** to remove the cloud service account from Security Auditor.

Manage Filters



✓* - Validation is required for new/changed filters.

□ Name	Description	Server Group	Last Poll Time	Status	Actions
□ MyFilter		{os}	12/15/17 14:48	✓ success	🗑 ● ✓*
□ MyRedHatFilter		MyRedHatGroup	12/05/17 14:42	✓ success	🗑 ○ ✓*
□ MySuseFilter		MySuseGroup	12/05/17 14:42	✓ success	🗑 ○ ✓*

How to Get There

On the Manage AWS Cloud Service Accounts screen, click **(Edit Filters)**.

What it Does

Filters allow you to identify the server instances you would like to add automatically during polling and how they are mapped to Groups and Managed Servers within Security Auditor. It does this by creating Managed Servers for the discovered instances.

The information provided here allows you to:

- Identify a subset of servers as part of a policy group.
- Create dynamic names/descriptions used for the Managed Server definitions.
- Customize the attributes that are normally available for the "Add Managed Server" interactive process.

Options

New

Click **New** to open the Add Cloud Service Account screen, where you can setup a new AWS account with Security Auditor.

Delete

Choose an account and click **Delete** to delete the account from Security Auditor.

Name • Description • Type

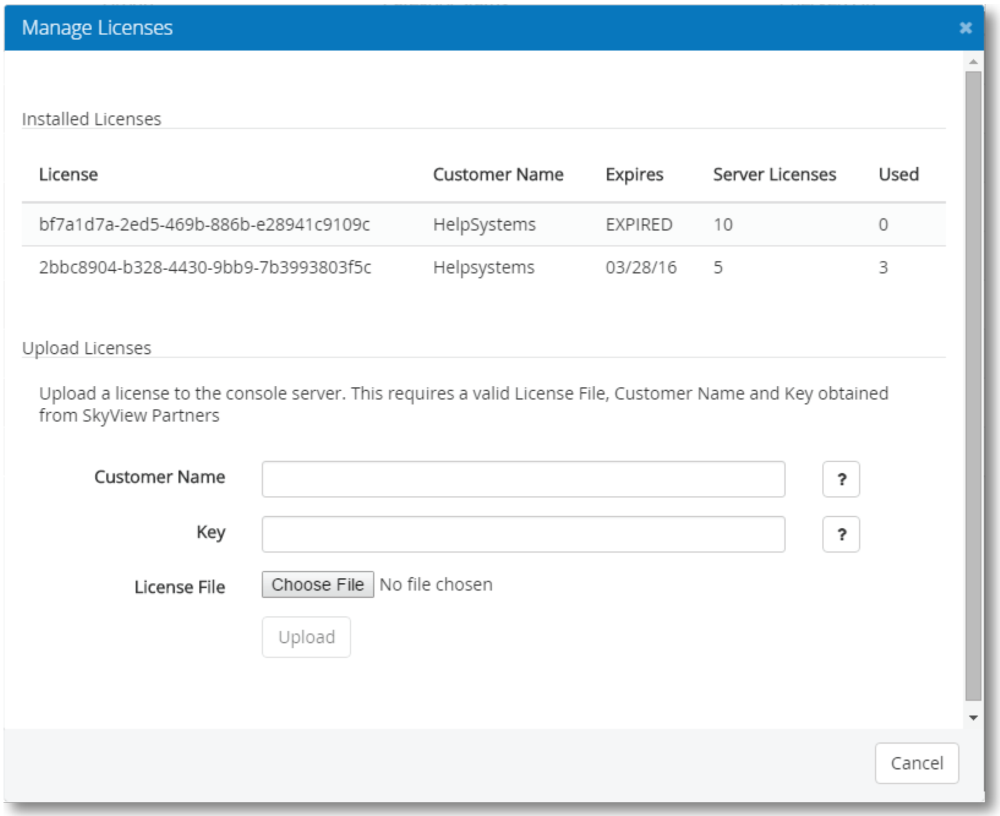
These are the names, descriptions, and type of accounts as specified in the Add/Edit Service Account screen.

[Filter List] Name • Description • Server Group Last Poll Time • Status • Actions

- **Name.** Click an existing filter Name to open the Add/Modify Filter screen where you can edit the filter's settings.
- **Description.** The description of the filter, if specified in the filter settings.
- **Server Group.** The Server Group specified for Server Group Template in the Add/Modify Filter screen for the filter.
- **Last Poll Time.** The most recent time the filter was polled. Polling frequency and other polling settings can be configured on the Cloud Services tab of the Preferences screen.
- **Status.** Lists whether the most recent polling attempt was successful or not, or whether polling is in progress.
- **Actions.** Use these buttons to perform actions on the adjacent filter.
  - Click ✓ **(View Filter)** to display the Validate Filter screen, which displays the server instances yielded by the Filter settings and additional information. No asterisk on the button indicates it will be automatically polled.
  - Click ✓* **(Validate Filter)** to test the filter settings to ensure validity. An asterisk on the button indicates it will not be automatically polled until you accept validation.
  - Click 🗑 **(Delete)** to remove the Filter from the cloud service account.
  - Click ● **(Disable Filter)** or ○ **(Enable Filter)** to turn the filter off or on, respectively. If set to Disable, the Filter will not be included in polling for its cloud service account.

Manage Licenses screen

Use this screen to manage product licenses.



License	Customer Name	Expires	Server Licenses	Used
bf7a1d7a-2ed5-469b-886b-e28941c9109c	HelpSystems	EXPIRED	10	0
2bbc8904-b328-4430-9bb9-7b3993803f5c	Helpsystems	03/28/16	5	3

Upload a license to the console server. This requires a valid License File, Customer Name and Key obtained from SkyView Partners

How to get there

Choose **Admin Tasks > Manage Licenses**.

Installed Licenses

This section lists the licenses that have already been installed, including the customer name, expiration date, number of server licenses available, and the number of server licenses currently used.

Upload Licenses

Customer Name

This must be the exact name given to HelpSystems when the license was obtained.

Key

This must be the key received from HelpSystems along with the license file

License File; Choose File • Upload

This is where to choose a license file to upload.

Cancel

Click **Cancel** to dismiss this screen.

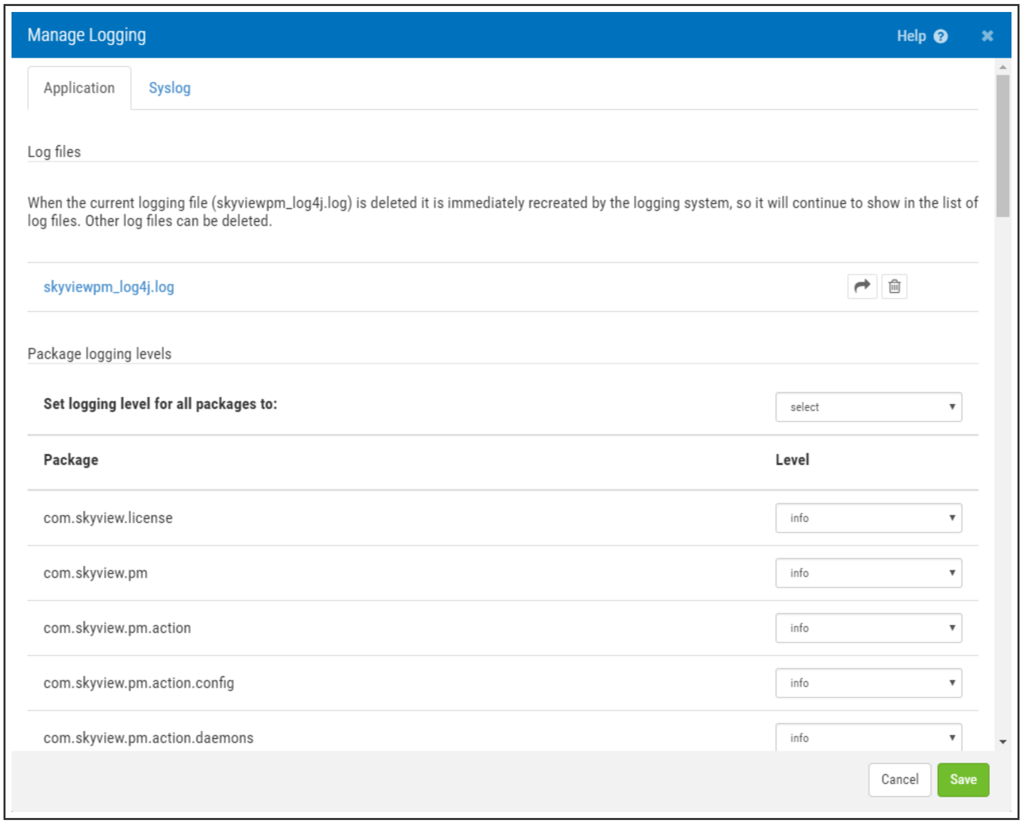
Manage Logging screen

Use this screen to set the logging level for Security Auditor log packages and set syslog options.

How to get there

Choose **Admin Tasks > Manage Logs**.

Application Tab



Log files

When the current logging file (skyviewpm_log4j.log) is deleted it is immediately recreated by the logging system, so it will continue to show in the list of log files. Other log files can be deleted.

skyviewpm_log4j.log

Package logging levels

Set logging level for all packages to: select

Package	**Level**
com.skyview.license	info
com.skyview.pm	info
com.skyview.pm.action	info
com.skyview.pm.action.config	info
com.skyview.pm.action.daemons	info

Log Files

When the current logging file (skyviewpm_log4j.log) is deleted it is immediately recreated by the logging system, so it will continue to show in the list of log files. Other log files can be deleted.

Package logging levels

Set logging level for all packages to:

This is where to set logging levels for packages.

Field Descriptions

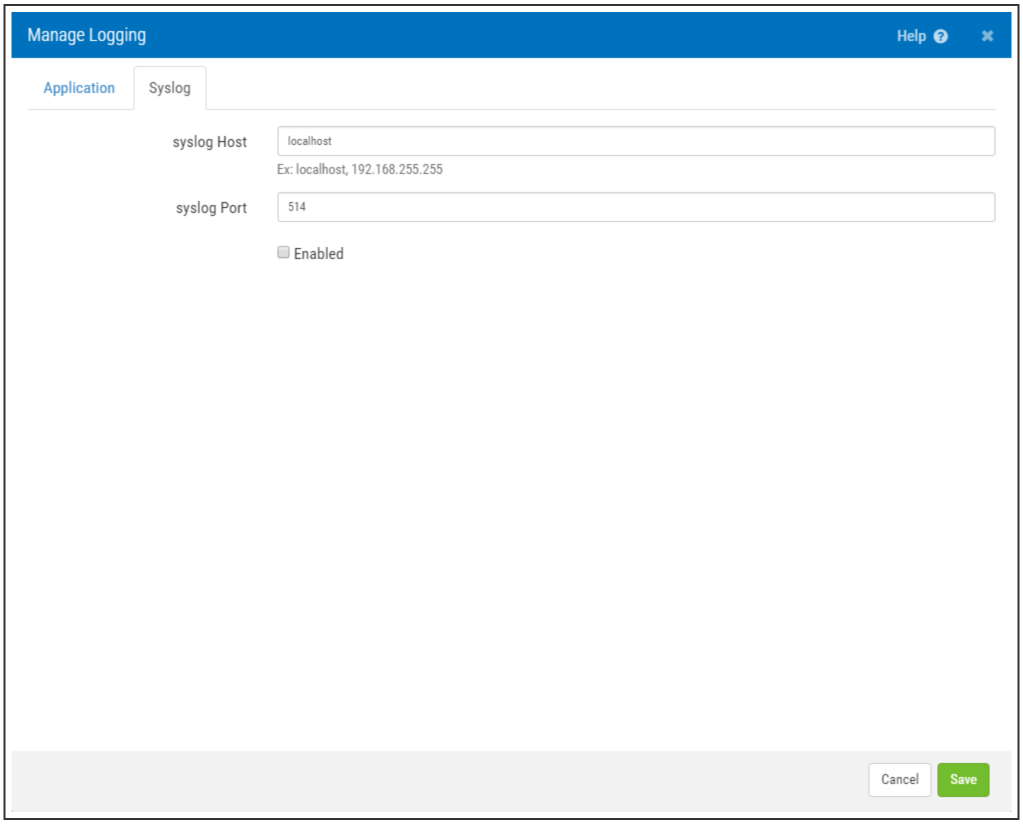
Package

This category shows the log files.

Level

This category is for selecting the level category that corresponds to the file.

Syslog Tab



syslog Host: localhost

Ex: localhost, 192.168.255.255

syslog Port: 514

□ Enabled

Syslog Host

The host of the syslog server.

Syslog Port • Enabled

The port used to communicate with the Syslog server (the default Syslog port is 514). Check **Enabled** to enable syslog messaging.

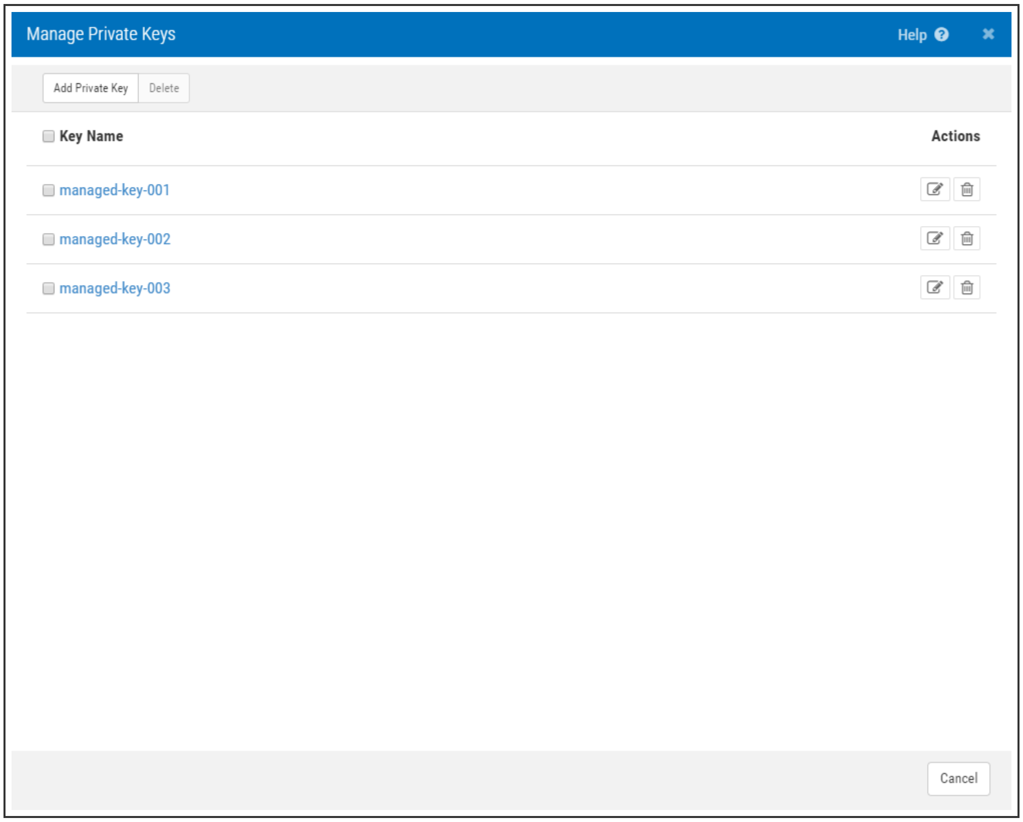
Cancel • Save

Click **Cancel** to dismiss this screen. Click **Save** to save your changes and dismiss the screen.

Manage Private Keys

A password can be used for connecting to managed servers being added to Security Auditor, but Security Auditor also supports connecting to Managed Servers using a private key.

The private key can be provided using direct text entry (copy/paste from clipboard) or by selecting a file from the file system.



□ Key Name	Actions
□ managed-key-001	
□ managed-key-002	
□ managed-key-003	

How to Get There

Choose **Admin Tasks > Manage Private Keys**.

Options

Add Private Key

Click this button to open the Add Private Key screen, where you can add a new private key.

Delete

Check one or more private keys and click this button to remove them.

Field Descriptions

Key Name

This is the name assigned to the private key when it was added.

Actions

✎

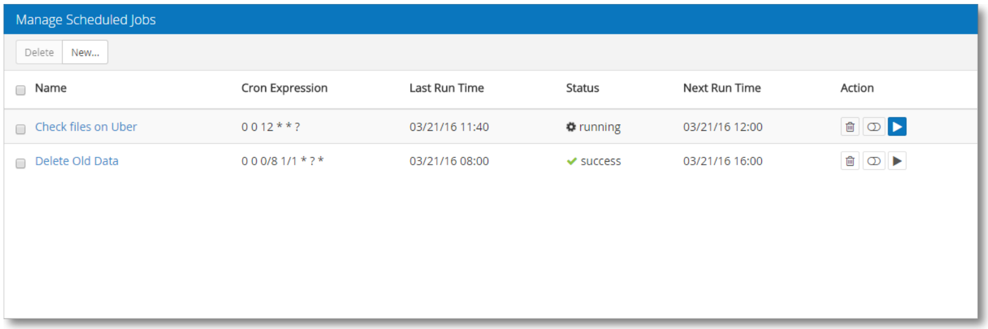
Click this button to open the Modify Private Key screen, where you can specify a new private key.

🗑

Check one or more private keys and click this button to remove them.

Manage Scheduled Jobs screen

Use this screen to create and manage scheduled jobs.



□	Name	Cron Expression	Last Run Time	Status	Next Run Time	Action
□	Check files on Uber	0 0 12 * * ?	03/21/16 11:40	⚙ running	03/21/16 12:00	🗑 ⊂⊃ ▶
□	Delete Old Data	0 0 0/8 1/1 * ? *	03/21/16 08:00	✓ success	03/21/16 16:00	🗑 ⊂⊃ ▶

How to get there

Choose **Admin Tasks > Manage Scheduled Jobs**.

Options

Delete

Click **Delete** to delete selected Scheduled Jobs.

New

Click New to open the Add Scheduled Job screen where you can define and add a Scheduled Job.

Field Descriptions

Name

The name of the scheduled job.

Cron Expression

The cron expression of the scheduled jobs.

Last Run Time

When the job was last run.

Status

Shows the status of the job.

Next Run Time

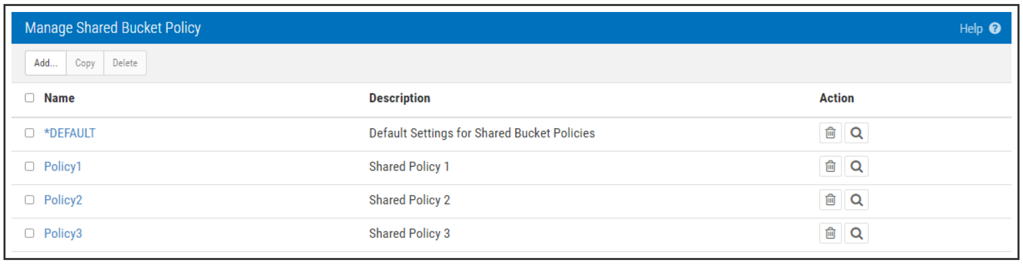
Shows when the job will be run next.

Action

This category allows for three actions:

- Click 🗑 **Delete** to delete the selected job(s).
- Click ◯ **Enable cron job/Disable cron job** to enable or disable the selected job(s).
- Click ▶ **Run job** to run the cron job.

Manage Shared Bucket Policy



□ Name	Description	Action
□ *DEFAULT	Default Settings for Shared Bucket Policies	🗑 🔍
□ Policy1	Shared Policy 1	🗑 🔍
□ Policy2	Shared Policy 2	🗑 🔍
□ Policy3	Shared Policy 3	🗑 🔍

How to get there

Choose **AWS Accounts > Manage Shared Bucket Policy**.

What it Does

Use the Manage Shared Bucket Policy screen to add, copy, or delete a shared AWS bucket policy.

Options

Add

Opens the Add Shared Bucket Policy screen where you can define a new Shared Bucket Policy. See Add/Modify Shared Bucket Policy.

Copy

This option creates a copy of the selected Shared Bucket Policies, appending "_copy#" to new Shared Bucket Policy names.

Delete

This option deletes the selected Shared Bucket Policies. You are prompted with a confirmation screen before the selected Shared Bucket Policies are deleted. A Shared Bucket Policy cannot be deleted when referenced by an Account or Bucket.

Column Descriptions

Name

The name of the Shared Bucket Policy. Click the name to open the Modify Shared Bucket Policy screen.

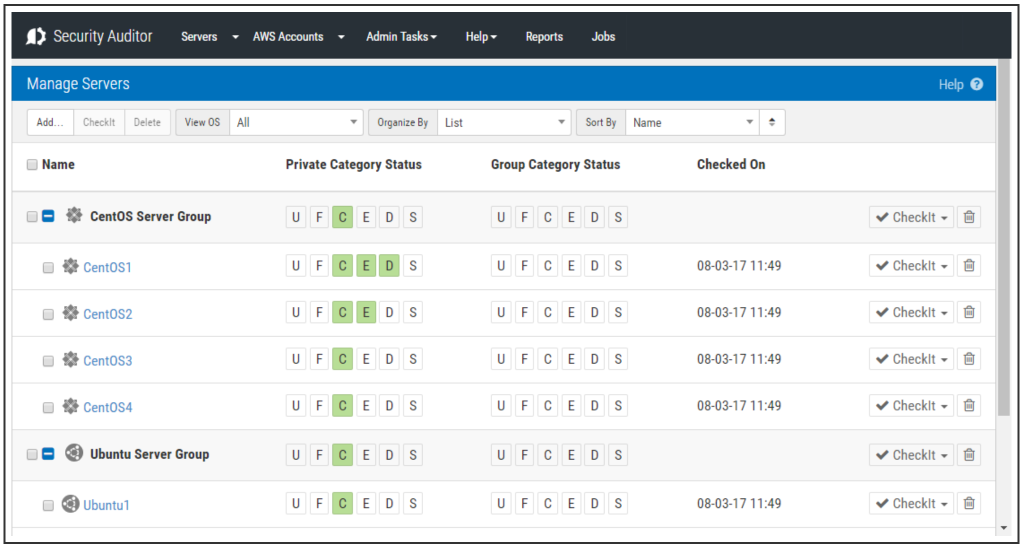
Description

The description of the Shared Bucket Policy.

Action

- Click 🗑 **(Delete)** to remove the Shared Bucket Policy.
- Click 🔍 **(Search)** to open the "Where is *[shared policy]* used" screen, which identifies the buckets used by the policy.

Manage Servers screen



Name	Private Category Status	Group Category Status	Checked On	
CentOS Server Group	U F C E D S	U F C E D S		CheckIt
CentOS1	U F C E D S	U F C E D S	08-03-17 11:49	CheckIt
CentOS2	U F C E D S	U F C E D S	08-03-17 11:49	CheckIt
CentOS3	U F C E D S	U F C E D S	08-03-17 11:49	CheckIt
CentOS4	U F C E D S	U F C E D S	08-03-17 11:49	CheckIt
Ubuntu Server Group	U F C E D S	U F C E D S		CheckIt
Ubuntu1	U F C E D S	U F C E D S	08-03-17 11:49	CheckIt

How to get there

Click **Manage Servers** on the Navigation Pane.

What it Does

Use the Manage Servers screen to add, modify, and check the status of managed servers.

Options

Add

Click **Add** to open the Add a New Server screen where you can add a new managed server.

CheckIt

Select one or more servers and click this button to run CheckIt, which performs a compliance check for the selected attribute(s).

Delete

Select one or more managed servers, and/or Groups, and click this button to delete them.

View OS

Choose this option to display only servers of a particular operating system or distribution.

Organize By: Group • List

Choose Group to order servers by their Group in the list (see Add a New Server screen). Choose List to order servers alphabetically in the list.

Sort By: Name • Group • Checked On • [Ascending/Descending]

When List is selected these options are available. Choose Name to sort the server list by name, group to sort by the server Group, or Checked On to sort chronologically by the date most recently checked (either in ascending or descending order).

Name

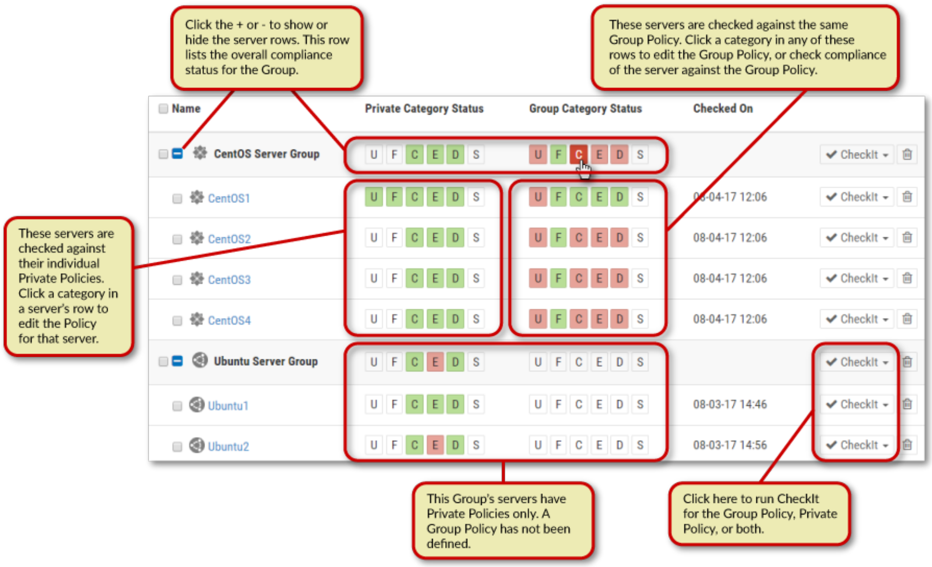
This is the name assigned to the server when it was added (see Add a New Server screen).

Group

This is the Group the server was assigned to when it was added (see Add a New Server screen).

Private Category Status • Group Category Status

These icons are color coded, indicating their compliance status, red for not compliant, green for compliant, and white for not checked. Click a category icon to open its settings. U =User Account Policies, F =Files Policies, C =Configuration Policies, E =Exported Directory Policies, D =Daemon Policies, S =Script Policies. See Servers and Policies screen.



Click the + or - to show or hide the server rows. This row lists the overall compliance status for the Group.

These servers are checked against the same Group Policy. Click a category in any of these rows to edit the Group Policy, or check compliance of the server against the Group Policy.

These servers are checked against their individual Private Policies. Click a category in a server's row to edit the Policy for that server.

□ Name	Private Category Status	Group Category Status	Checked On	
□ ⊟ CentOS Server Group	U F C E D S	U F C E D S		✔ CheckIt ▾ 🗑
□ CentOS1	U F C E D S	U F C E D S	08-04-17 12:06	✔ CheckIt ▾ 🗑
□ CentOS2	U F C E D S	U F C E D S	08-04-17 12:06	✔ CheckIt ▾ 🗑
□ CentOS3	U F C E D S	U F C E D S	08-04-17 12:06	✔ CheckIt ▾ 🗑
□ CentOS4	U F C E D S	U F C E D S	08-04-17 12:06	✔ CheckIt ▾ 🗑
□ ⊟ Ubuntu Server Group	U F C E D S	U F C E D S		✔ CheckIt ▾ 🗑
□ Ubuntu1	U F C E D S	U F C E D S	08-03-17 14:46	✔ CheckIt ▾ 🗑
□ Ubuntu2	U F C E D S	U F C E D S	08-03-17 14:56	✔ CheckIt ▾ 🗑

This Group's servers have Private Policies only. A Group Policy has not been defined.

Click here to run CheckIt for the Group Policy, Private Policy, or both.

Checked On

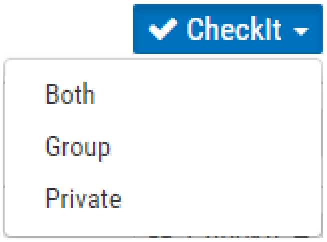
This is the date the policy was most recently checked.

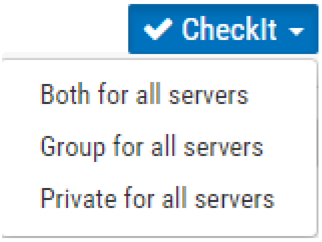
Action ✔ CheckIt ▾ 🗑

Click this button to check a server or Group's policy.

If selected for an individual server, one of the following menu appears:

Server **Group**



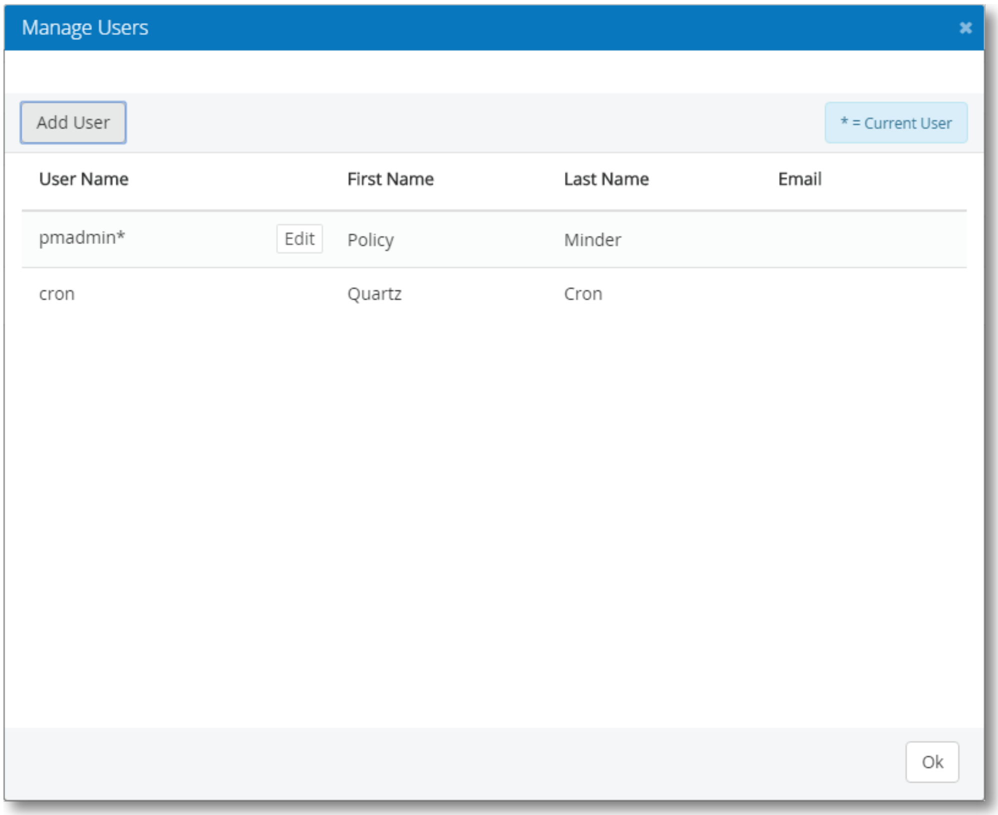


Chose **Group/Group for all servers** to check the Group Policy, **Private/Private for all servers** to check the Private Policy, and **Both/Both for all servers** to check both Policies.

Select 🗑 to delete a server or Group.

Manage Users screen

Use this screen to add and manage Security Auditor users.



User Name	First Name	Last Name	Email
pmadmin*	Policy	Minder	
cron	Quartz	Cron	

Choose **Admin Tasks > Manage Users**.

Add Users

This is the option that is used for adding a user.

Field Descriptions

User Name

This category displays the user names

First Name

This category displays the user's first name.

Last Name

This category displays the user's last name.

Email

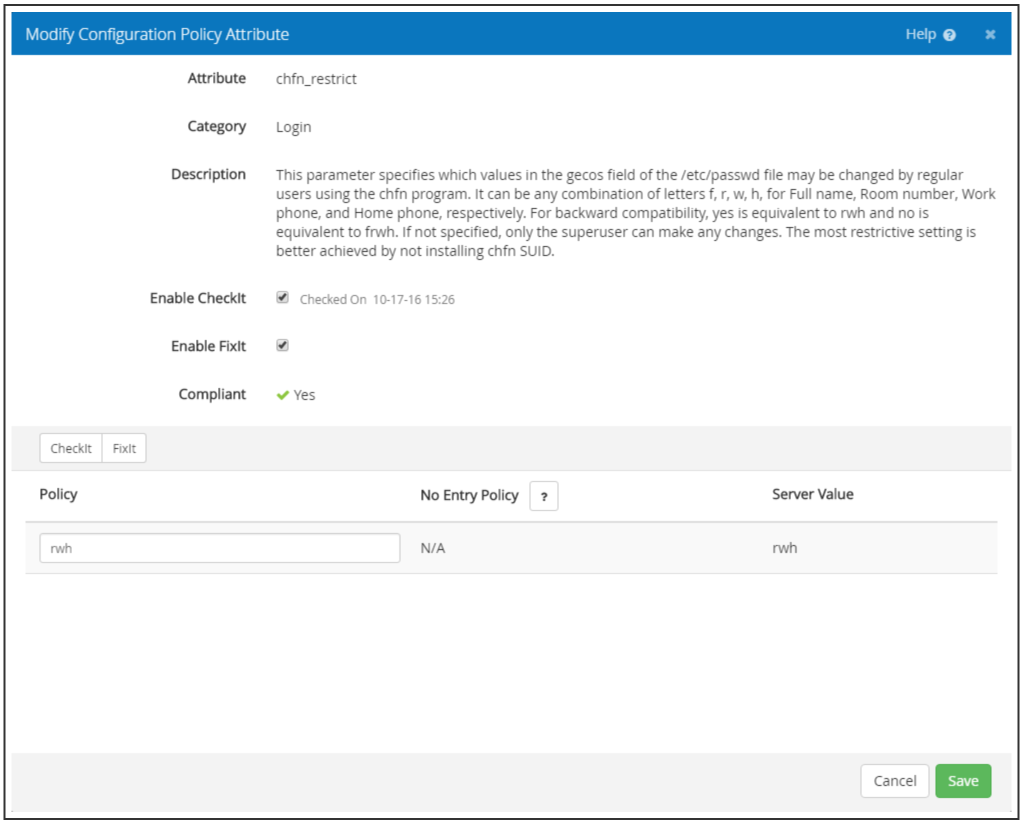
This category displays the user's email.

Ok

Click **Ok** to accept changes and dismiss the Manage Users screen.

Modify Configuration Policy Attribute

This screen allows you to change a Configuration policy attribute.



Attribute chfn_restrict

Category Login

Description This parameter specifies which values in the gecos field of the /etc/passwd file may be changed by regular users using the chfn program. It can be any combination of letters f, r, w, h, for Full name, Room number, Work phone, and Home phone, respectively. For backward compatibility, yes is equivalent to rwh and no is equivalent to frwh. If not specified, only the superuser can make any changes. The most restrictive setting is better achieved by not installing chfn SUID.

Enable CheckIt ☑ Checked On 10-17-16 15:26

Enable FixIt ☑

Compliant ✓ Yes

Policy	No Entry Policy ?	Server Value
rwh	N/A	rwh

How to get there

1. On the menu at the top of the screen choose **Manage Servers**.
2. Choose C for the server you wish to modify.
3. Choose the attribute you wish to modify.

Field Descriptions

Attribute

The name of the policy attribute.

Category

The Category of the Configuration policy attribute.

Description

A description of the Configuration policy attribute.

Enable CheckIt

Check this box to allow Security Auditor to check this value on the server to determine its status.

Enable FixIt

Check this box to allow Security Auditor to fix this value on the server (i.e. change it to match the template value).

Compliant

This column indicates whether the Server Value is compliant with the Policy Value setting.

CheckIt

Click **CheckIt** to perform CheckIt on the selected policy categories.

Policy

The value of the Configuration policy attribute.

No Entry Policy (AIX only)

When true, Security Auditor will monitor (CheckIt) and remove (FixIt) the user stanzas entries in the file etc/security/user for this attribute so that user attributes will not have a value overriding the system default value. This enables the system administrator to control all users by changing the default value.

Server Value

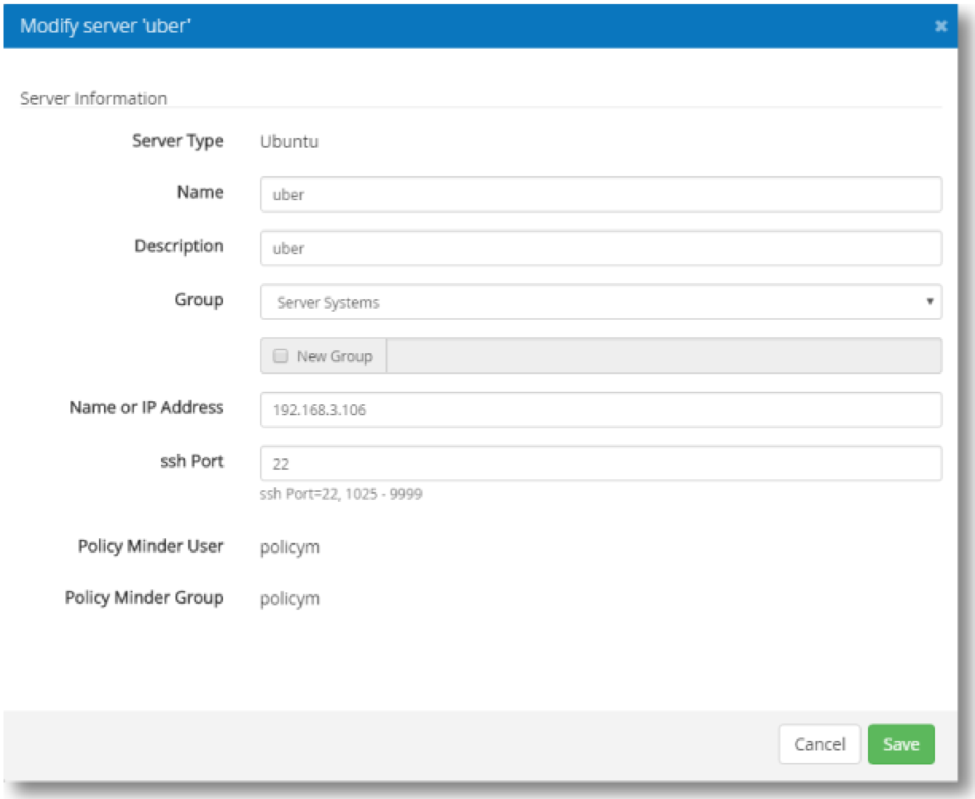
The value on the server for the attribute.

Cancel • Save

Click **Cancel** to dismiss this screen. Click **Save** to save your changes to the policy attribute.

Modify Server screen

Use this screen to modify settings for managed servers.



Modify server 'uber'

Server Information

Server Type: Ubuntu

Name: uber

Description: uber

Group: Server Systems

□ New Group

Name or IP Address: 192.168.3.106

ssh Port: 22

ssh Port=22, 1025 - 9999

Policy Minder User: policym

Policy Minder Group: policym

How to get there

1. On the menu at the top of the screen choose **Manage Servers**.
2. Choose the server you want to modify.

Field Descriptions

Server Type

This lists the OS type of server that has been selected.

Name

The name of the server.

Description

This description of the server.

Group • New Group

This is the group that this server is in. To Make a new group select the new group option.

Name or IP Address

This is the name or IP address of the server.

ssh Port

This is the ssh port of the server.

Security Auditor User

The user associated with the server.

Security Auditor Group

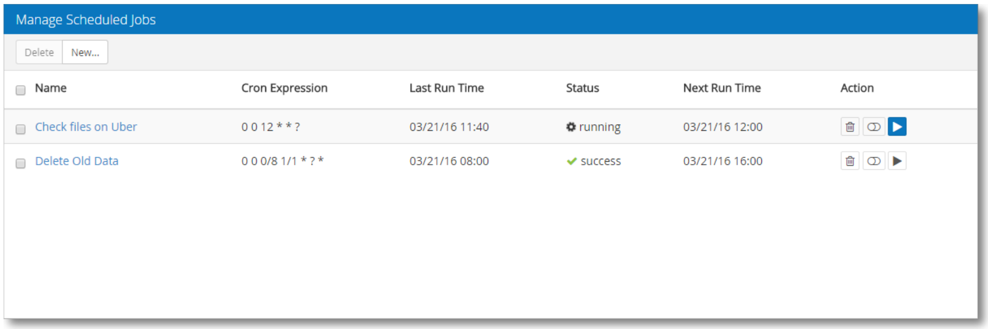
The group associated with the server.

Cancel • Save

Click **Cancel** to dismiss this screen without changing server settings. Click **Save** to save changes to server settings.

Manage Scheduled Jobs screen

Use this screen to create and manage scheduled jobs.



□ Name	Cron Expression	Last Run Time	Status	Next Run Time	Action
□ Check files on Uber	0 0 12 * * ?	03/21/16 11:40	⚙ running	03/21/16 12:00	▶
□ Delete Old Data	0 0 0/8 1/1 * ? *	03/21/16 08:00	✓ success	03/21/16 16:00	▶

How to get there

Choose **Admin Tasks > Manage Scheduled Jobs**.

Options

Delete

Click **Delete** to delete selected Scheduled Jobs.

New

Click New to open the Add Scheduled Job screen where you can define and add a Scheduled Job.

Field Descriptions

Name

The name of the scheduled job.

Cron Expression

The cron expression of the scheduled jobs.

Last Run Time

When the job was last run.

Status

Shows the status of the job.

Next Run Time

Shows when the job will be run next.

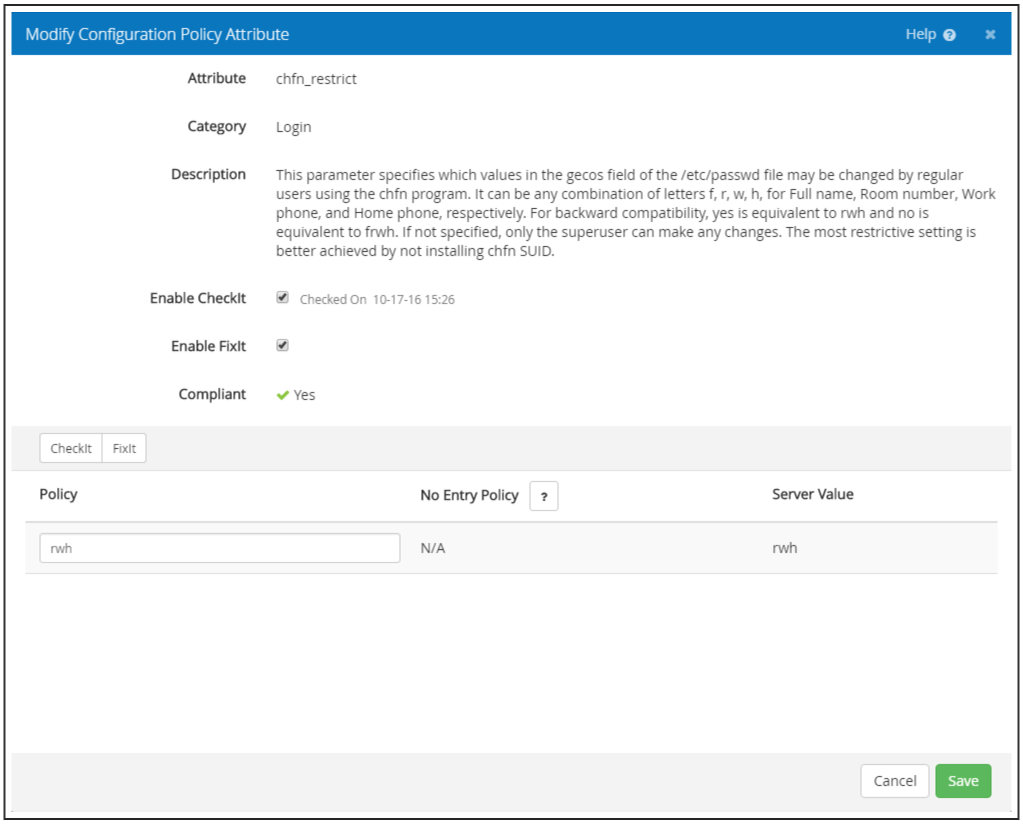
Action

This category allows for three actions:

- Click 🗑 **Delete** to delete the selected job(s).
- Click ◯ **Enable cron job/Disable cron job** to enable or disable the selected job(s).
- Click ▶ **Run job** to run the cron job.

Modify Configuration Policy Attribute

This screen allows you to change a Configuration policy attribute.



Attribute chfn_restrict

Category Login

Description This parameter specifies which values in the gecos field of the /etc/passwd file may be changed by regular users using the chfn program. It can be any combination of letters f, r, w, h, for Full name, Room number, Work phone, and Home phone, respectively. For backward compatibility, yes is equivalent to rwh and no is equivalent to frwh. If not specified, only the superuser can make any changes. The most restrictive setting is better achieved by not installing chfn SUID.

Enable CheckIt ☑ Checked On 10-17-16 15:26

Enable FixIt ☑

Compliant ✓ Yes

Policy	No Entry Policy	Server Value
rwh	N/A	rwh

How to get there

1. On the menu at the top of the screen choose **Manage Servers**.
2. Choose C for the server you wish to modify.
3. Choose the attribute you wish to modify.

Field Descriptions

Attribute

The name of the policy attribute.

Category

The Category of the Configuration policy attribute.

Description

A description of the Configuration policy attribute.

Enable CheckIt

Check this box to allow Security Auditor to check this value on the server to determine its status.

Enable FixIt

Check this box to allow Security Auditor to fix this value on the server (i.e. change it to match the template value).

Compliant

This column indicates whether the Server Value is compliant with the Policy Value setting.

CheckIt

Click **CheckIt** to perform CheckIt on the selected policy categories.

Policy

The value of the Configuration policy attribute.

No Entry Policy (AIX only)

When true, Security Auditor will monitor (CheckIt) and remove (FixIt) the user stanzas entries in the file etc/security/user for this attribute so that user attributes will not have a value overriding the system default value. This enables the system administrator to control all users by changing the default value.

Server Value

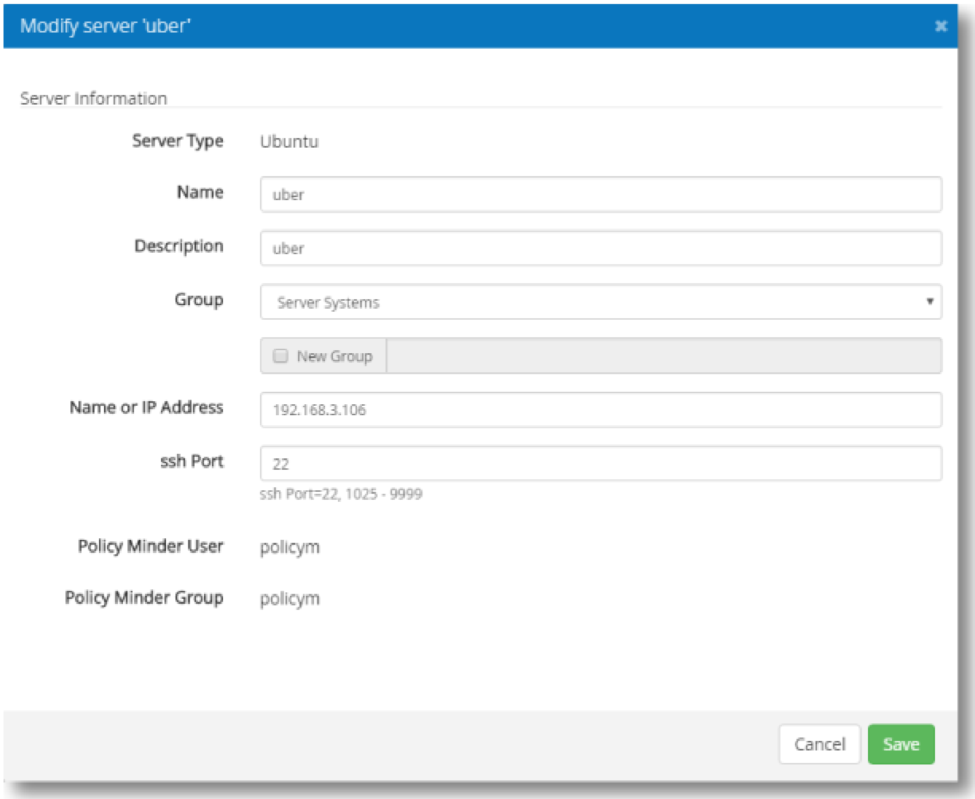
The value on the server for the attribute.

Cancel • Save

Click **Cancel** to dismiss this screen. Click **Save** to save your changes to the policy attribute.

Modify Server screen

Use this screen to modify settings for managed servers.



Modify server 'uber'

Server Information

Server Type: Ubuntu

Name: uber

Description: uber

Group: Server Systems

Name or IP Address: 192.168.3.106

ssh Port: 22

ssh Port=22, 1025 - 9999

Policy Minder User: policym

Policy Minder Group: policym

How to get there

1. On the menu at the top of the screen choose **Manage Servers**.
2. Choose the server you want to modify.

Field Descriptions

Server Type

This lists the OS type of server that has been selected.

Name

The name of the server.

Description

This description of the server.

Group • New Group

This is the group that this server is in. To Make a new group select the new group option.

Name or IP Address

This is the name or IP address of the server.

ssh Port

This is the ssh port of the server.

Security Auditor User

The user associated with the server.

Security Auditor Group

The group associated with the server.

Cancel • Save

Click **Cancel** to dismiss this screen without changing server settings. Click **Save** to save changes to server settings.

Policy Values

When adding a Script Policy, values can be ranges of values for Integers or Dates, or regular expressions for Strings.

Booleans

For booleans, the values can be:

- `true` or `false`
- `yes` or `no`

Integer

Integer values can be a single value, a set of values, a range or a set of ranges and values

- A set of acceptable values are separated by the character ';' like **1;7;11**
- A range of acceptable values are separated by a ':' like **1:20**
- A set of ranges and values are separated by both ';' and ':' like **1:20;25;30:35**

Dates

The date format in Security Auditor must match the format used on the server.

> **EXAMPLE:**
> If the date value on the server is `05/31/2020`, the Policy format must be *`mm/dd/yyyy`*.

String

Summary of regular-expression constructs.

Construct	Matches
Characters	
x	The character x
`\\`	The backslash character
`\0`*`n`*	The character with octal value `0`*`n`* (0 <= *n* <= 7)
`\0`*`nn`*	The character with octal value `0`*`nn`* (0 <= *n* <= 7)
`\0`*`mnn`*	The character with octal value `0`*`mnn`* (0 <= *m* <= 3, 0 <= *n* <= 7)
`\x`*`hh`*	The character with hexadecimal value `0x`*`hh`*

Construct	Matches
Characters	
`\uhhhh`	The character with hexadecimal value `0xhhhh`
`\t`	The tab character (`'\u0009'`)
`\n`	The newline (line feed) character (`'\u000A'`)
`\r`	The carriage-return character (`'\u000D'`)
`\f`	The form-feed character (`'\u000C'`)
`\a`	The alert (bell) character (`'\u0007'`)
`\e`	The escape character (`'\u001B'`)
`\cx`	The control character corresponding to `x`

Character classes	
`[abc]`	`a`, `b`, or `c` (simple class)
`[^abc]`	Any character except `a`, `b`, or `c` (negation)
`[a-zA-Z]`	`a` through `z` or `A` through `Z`, inclusive (range)
`[a-d[m-p]]`	`a` through `d`, or `m` through `p`: `[a-dm-p]` (union)
`[a-z&&[def]]`	`d`, `e`, or `f` (intersection)
`[a-z&&[^bc]]`	`a` through `z`, except for `b` and `c`: `[ad-z]` (subtraction)
`[a-z&&[^m-p]]`	`a` through `z`, and not `m` through `p`: `[a-lq-z]` (subtraction)

Predefined character classes	
`.`	Any character (may or may not match line terminators)
`\d`	A digit: `[0-9]`
`\D`	A non-digit: `[^0-9]`
`\s`	A whitespace character: `[ \t\n\x0B\f\r]`
`\S`	A non-whitespace character: `[^\s]`
`\w`	A word character: `[a-zA-Z_0-9]`

Predefined character classes	
\W	A non-word character: [^\w]

POSIX character classes (US-ASCII only)	
\p{Lower}	A lower-case alphabetic character: [a-z]
\p{Upper}	An upper-case alphabetic character: [A-Z]
\p{ASCII}	All ASCII: [\x00-\x7F]
\p{Alpha}	An alphabetic character: [\p{Lower}\p{Upper}]
\p{Digit}	A decimal digit: [0-9]
\p{Alnum}	An alphanumeric character: [\p{Alpha}\p{Digit}]
\p{Punct}	Punctuation: One of !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
\p{Graph}	A visible character: [\p{Alnum}\p{Punct}]
\p{Print}	A printable character: [\p{Graph}\x20]
\p{Blank}	A space or a tab: [\t]
\p{Cntrl}	A control character: [\x00-\x1F\x7F]
\p{XDigit}	A hexadecimal digit: [0-9a-fA-F]
\p{Space}	A whitespace character: [\t\n\x0B\f\r]

java.lang.Character classes (simple java character type)	
\p{javaLowerCase}	Equivalent to java.lang.Character.isLowerCase()
\p{javaUpperCase}	Equivalent to java.lang.Character.isUpperCase()
\p{javaWhitespace}	Equivalent to java.lang.Character.isWhitespace()
\p{javaMirrored}	Equivalent to java.lang.Character.isMirrored()

Classes for Unicode blocks and categories	
\p{InGreek}	A character in the Greek block (simple block)
\p{Lu}	An uppercase letter (simple category)

Classes for Unicode blocks and categories	
`\p{Sc}`	A currency symbol
`\P{InGreek}`	Any character except one in the Greek block (negation)
`[\p{L}&&[^\p{Lu}]]`	Any letter except an uppercase letter (subtraction)

Boundary matchers	
`^`	The beginning of a line
`$`	The end of a line
`\b`	A word boundary
`\B`	A non-word boundary
`\A`	The beginning of the input
`\G`	The end of the previous match
`\Z`	The end of the input but for the final terminator, if any
`\z`	The end of the input

Greedy quantifiers	
`X?`	*X*, once or not at all
`X*`	*X*, zero or more times
`X+`	*X*, one or more times
X{*n*}	*X*, exactly *n* times
X{*n*,}	*X*, at least *n* times
X{*n*,*m*}	*X*, at least *n* but not more than *m* times

Reluctant quantifiers	
`X??`	*X*, once or not at all
`X*?`	*X*, zero or more times
`X+?`	*X*, one or more times

Reluctant quantifiers	
`X{n}?`	*X*, exactly *n* times
`X{n,}?`	*X*, at least *n* times
`X{n,m}?`	*X*, at least *n* but not more than *m* times

Possessive quantifiers	
`X?+`	*X*, once or not at all
`X*+`	*X*, zero or more times
`X++`	*X*, one or more times
`X{n}+`	*X*, exactly *n* times
`X{n,}+`	*X*, at least *n* times
`X{n,m}+`	*X*, at least *n* but not more than *m* times

Logical operators	
`XY`	*X* followed by *Y*
`X|Y`	Either *X* or *Y*
`(X)`	X, as a capturing group

Back references	
`\n`	Whatever the *n* th capturing group matched

Quotation	
`\`	Nothing, but quotes the following character
`\Q`	Nothing, but quotes all characters until `\E`
`\E`	Nothing, but ends quoting started by `\Q`

Special constructs (non-capturing)	
`(?:X)`	*X*, as a non-capturing group
`(?idmsux-idmsux)`	Nothing, but turns match flags idmsux on - off
`(?idmsux-idmsux:X)`	*X*, as a non-capturing group with the given flags idmsux on - off
(?=*X*)	*X*, via zero-width positive lookahead
(?!*X*)	X, via zero-width negative lookahead
(?<=*X*)	X, via zero-width positive lookbehind
(?<!*X*)	X, via zero-width negative lookbehind
(?>*X*)	X, as an independent, non-capturing group

Backslashes, escapes, and quoting

The backslash character ('\') serves to introduce escaped constructs, as defined in the table above, as well as to quote characters that otherwise would be interpreted as unescaped constructs. Thus the expression \\ matches a single backslash and \{ matches a left brace.

It is an error to use a backslash prior to any alphabetic character that does not denote an escaped construct; these are reserved for future extensions to the regular-expression language. A backslash may be used prior to a non-alphabetic character regardless of whether that character is part of an unescaped construct.

Backslashes within string literals in Java source code are interpreted as required by the Java Language Specification as either Unicode escapes or other character escapes. It is therefore necessary to double backslashes in string literals that represent regular expressions to protect them from interpretation by the Java bytecode compiler. The string literal "\b", for example, matches a single backspace character when interpreted as a regular expression, while "\\b" matches a word boundary. The string literal "\(hello\)" is illegal and leads to a compile-time error; in order to match the string (hello) the string literal "\\(hello\\)" must be used.

Character Classes

Character classes may appear within other character classes, and may be composed by the union operator (implicit) and the intersection operator (&&). The union operator denotes a class that contains every character that is in at least one of its operand classes. The intersection operator denotes a class that contains every character that is in both of its operand classes.

The precedence of character-class operators is as follows, from highest to lowest:

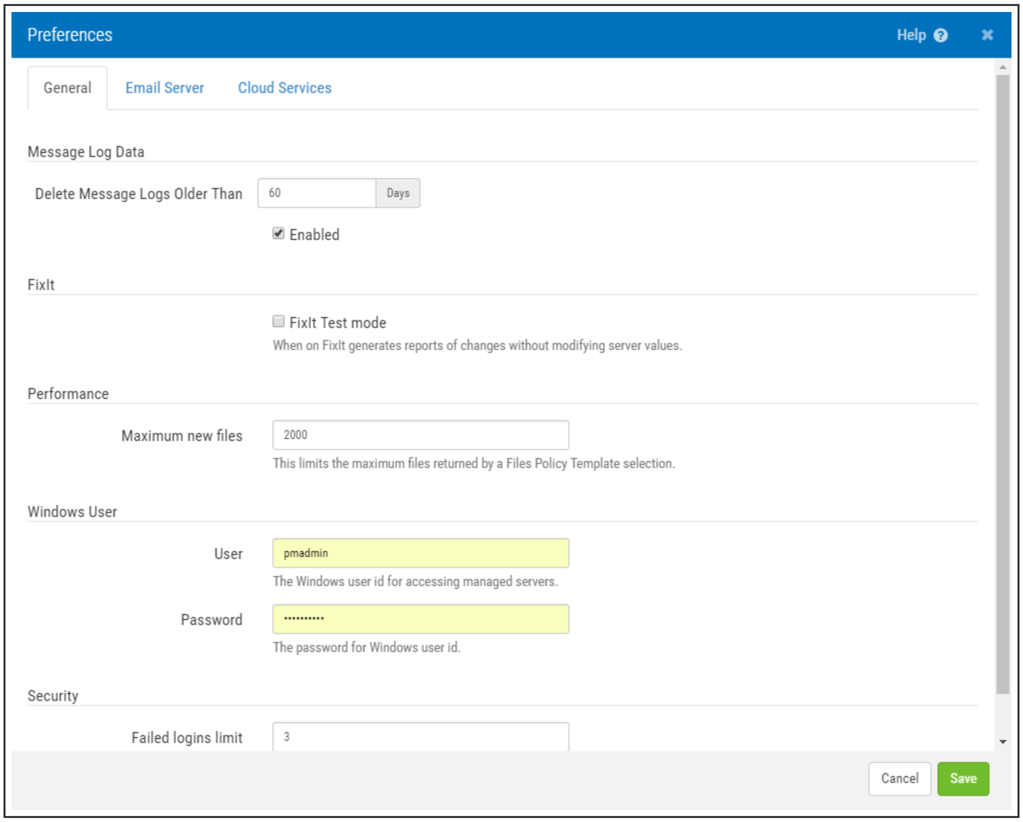
1	Literal escape	`\x`

2	Grouping	`[...]`
3	Range	`a-z`
4	Union	`[a-e][i-u]`
5	Intersection	`[a-z&&[aeiou]]`

Note that a different set of metacharacters are in effect inside a character class than outside a character class. For instance, the regular expression . loses its special meaning inside a character class, while the expression - becomes a range forming metacharacter.

Preferences screen

Use this screen to make changes to Security Auditor's general and email server preferences.



Message Log Data

Delete Message Logs Older Than 60 Days

☑ Enabled

FixIt

□ FixIt Test mode

When on FixIt generates reports of changes without modifying server values.

Performance

Maximum new files 2000

This limits the maximum files returned by a Files Policy Template selection.

Windows User

User pmadmin

The Windows user id for accessing managed servers.

Password ••••••••••

The password for Windows user id.

Security

Failed logins limit 3

How to get there

Choose **Admin Tasks** > **Preferences**.

General tab

Message Log Data

Delete Message Logs Older Than _ Days • Enabled

Enter a value here to automatically delete message logs older than the number of days specified. Check **Enabled** to activate this feature.

> **NOTE:** This feature clears an internal message log and not the logs displayed in the Manage Logging screen (Admin Tasks > Manage Logging).

FixIt

FixIt Test mode

When on FixIt generates reports of changes without modifying server values.

Performance

Maximum new files

This limits the maximum files returned by a Files Policy Template selection. See Files.

Windows User

These are the credentials used for logging in to a server when **Default User and Password** is chosen for "Connection Option" in the Add a New Server screen.

User

The Windows user ID for accessing managed servers.

Password

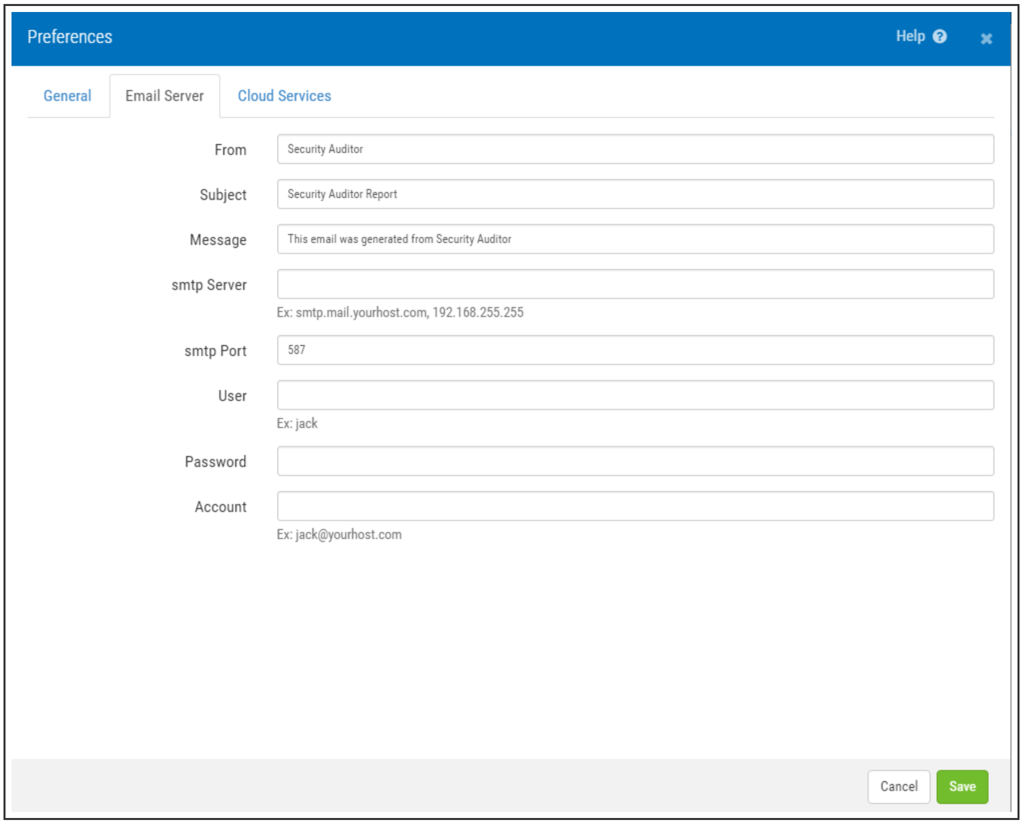
The password for Windows user ID.

Security

Failed Logins Limit

This sets the maximum number of failed logins before a user's account is disabled.

Email Server tab



From: Security Auditor

Subject: Security Auditor Report

Message: This email was generated from Security Auditor

smtp Server:

Ex: smtp.mail.yourhost.com, 192.168.255.255

smtp Port: 587

User:

Ex: jack

Password:

Account:

Ex: jack@yourhost.com

From

This text will appear in the "from" field of the email message.

Subject

This text will appear in the subject of the email message.

Message

This text will appear in the body of the email message.

smtp Server

This is the smtp server name or ip address.

> **EXAMPLE:**
> `smtp.mail.yourhost.com` or `192.168.255.255`

> **NOTE:** The "Default" SMTP server option of earlier versions of this software is no longer available. In order to send email from Security Auditor you need to define an SMTP server.

smtp Port

Mail clients generally submit outgoing emails to mail servers on port 587, which is the Security Auditor default setting.

User

The user name for the account on the specified smtp server (e.g. Jack).

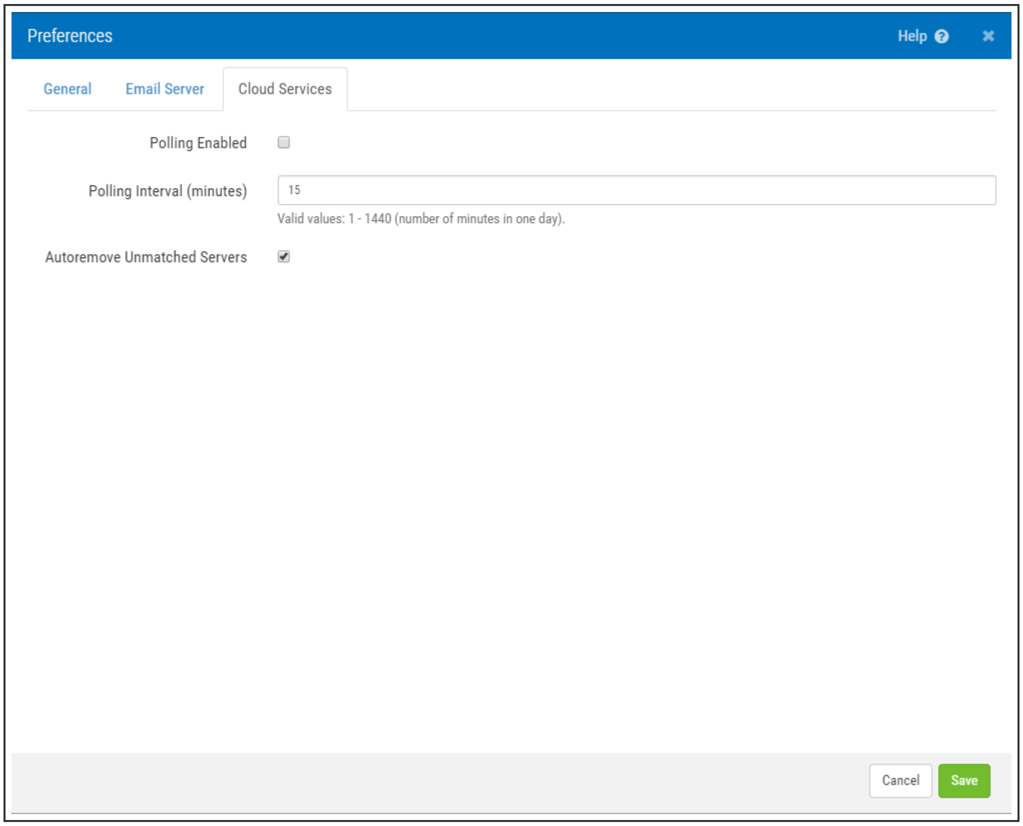
Password

The password for the specified user.

Account

The email account to use (e.g. jack@yourhost.com).

Cloud Services tab



Polling Enabled □

Polling Interval (minutes) 15

Valid values: 1 - 1440 (number of minutes in one day).

Autoremove Unmatched Servers ☑

Polling Enabled

Check this box to enable polling. Cloud services polling monitors services like Amazon AWS to identify new server definitions. When it finds one, Security Auditor can automatically create new managed server definitions and link the servers to shared policy definitions for quick and easy setup. The monitored cloud services are defined on the Manage AWS Cloud Service Accounts screen.

Polling Interval (minutes)

Specify the frequency of queries to the service, in number of minutes.

Autoremove Unmatched Servers

Check this box to delete Managed Servers that were previously discovered/added for a Cloud Service Account when any of the following changes occur:

- The server instance is deleted/removed from the cloud service.
- The originating Cloud Service Account is deleted from Security Auditor.
- The originating Filter is deleted from the Cloud Service Account in Security Auditor.
- The server instance no longer matches the originating Instance Filter selection criteria (only for enabled filters).
- The Filter selection/omission criteria has changed.
- The server instance attributes have changed in the Cloud Service Account so the selection/omission no longer includes the server.
- The Specific Regions selections processed by the filter have changed and does not include the region for server.

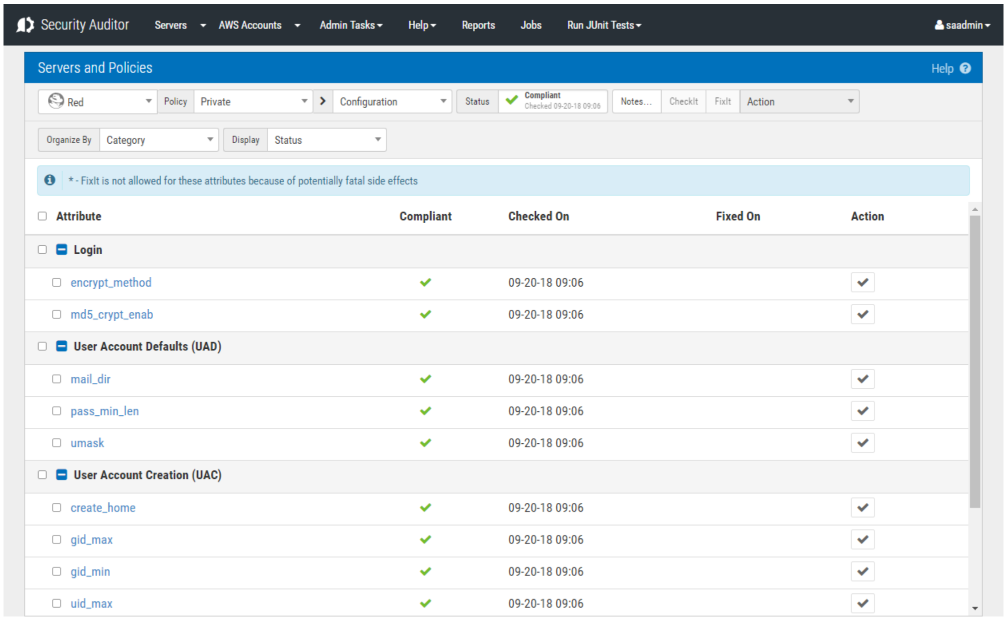
> **WARNING:** When a Managed Server is automatically deleted, its accompanying Private Policy will also be deleted, if one exists. Shared Group Policies are retained by the Group definition.

Cancel • Save

Choose **Cancel** to dismiss the screen without making changes. Choose **Save** to save your settings.

Servers and Policies - Configuration

Use this screen to configure and manage Configuration Policy Templates. When you initialize the Configuration category, Security Auditor identifies your current server configuration settings and lists them as Compliant. You can check these settings in the future to identify settings that have changed, or update the Configuration template to modify your security policy's configuration settings. Many administrators are comfortable with the current settings for these configuration settings and want to make sure that they remain set that way. The way to use Security Auditor to ensure they remain the same is to start by initializing the Security Auditor Configuration category. Go to **Servers > Initialize Policies** and choose to initialize the Configuration category.



Servers and Policies

Red | Policy: Private | Configuration | Status: ✓ Compliant, Checked 09-20-18 09:06 | Notes... | CheckIt | FixIt | Action

Organize By: Category | Display: Status

* - FixIt is not allowed for these attributes because of potentially fatal side effects

Attribute	Compliant	Checked On	Fixed On	Action
Login				
encrypt_method	✓	09-20-18 09:06		✓
md5_crypt_enab	✓	09-20-18 09:06		✓
User Account Defaults (UAD)				
mail_dir	✓	09-20-18 09:06		✓
pass_min_len	✓	09-20-18 09:06		✓
umask	✓	09-20-18 09:06		✓
User Account Creation (UAC)				
create_home	✓	09-20-18 09:06		✓
gid_max	✓	09-20-18 09:06		✓
gid_min	✓	09-20-18 09:06		✓
uid_max	✓	09-20-18 09:06		✓

How to get there

In the Manage Servers screen, choose C for a server.

What it Does

The Configuration page of the Servers and Policies screen displays an overview of the status of Configuration policy templates.

Status

Displays the status of the Policies and when they were last checked.

Notes

Choose this option to open the Configuration Policy Notes screen where you can record any notes related to the Policy. Notes appear in reports and provide a place to explain the intent of defined policies.

CheckIt

Use this button to run CheckIt, which performs a compliance check for the selected attribute(s).

FixIt

Use this button to run FixIt, which changes the value on the server to match that of Security Auditor.

Action; Enable CheckIt • Disable CheckIt • Enable FixIt • Disable FixIt

Use these options to enable/disable CheckIt and/or FixIt for selected attributes.

Organize By; Category • List

Choose Category to organize the attributes by category (Login, User Account Defaults (UAD), User Account Creation (UAC), and UAC (Password)). Choose List to display the Sort By drop-down menu, where you can choose the method to sort the selected attributes.

Sort By

Choose List in the 'Organize By' drop-down menu to activate this menu, which you can use to select how you want to sort the attributes.

Linux Attributes (RHEL, CentOS, Oracle)

Display; Status • Policy

Choose **Status** to view each Attribute's Category, Compliance status, and Checked On/Fixed On date and time. Choose **Policy** to replace the Category and Checked On/Fixed On columns with the Policy Value and Server Value columns, which show the exact values for each attribute on the server compared to the value in Security Auditor.

Login

Default attributes applied when a user logs in

encrypt_method

This defines the system default encryption algorithm for encrypting passwords (if no algorithm are specified on the command line). It can take one of these values:

- **DES (default)**
- **MD5**
- **SHA256**
- **SHA512. Note: this parameter overrides the MD5_CRYPT_ENAB variable.**

md5_crypt_enab

This variable is deprecated. You should use ENCRYPT_METHOD. Indicate if passwords must be encrypted using the MD5—based algorithm. If set to yes, new passwords will be encrypted using the MD5—based algorithm compatible with the one used by recent releases of FreeBSD. It supports passwords of unlimited length and longer salt strings. Set to no if you need to copy encrypted passwords to other systems which do not understand the new algorithm. Default is no. This variable is superseded by the ENCRYPT__METHOD variable or by any command line option used to configure the encryption algorithm.

User Account Defaults (UAD)

mail_dir

The mail spool directory. This is needed to manipulate the mailbox when its corresponding user account is modified or deleted. If not specified, a compile-time default is used.

pass_min_len

Minimum acceptable password length.

unmask

Determines file permissions at time of creation: the default is 022.

User Account Creation (UAC)

uid_min

Minimum range of user IDs used for the creation of regular users by useradd or newusers.

uid_max

Maximum range of user IDs used for the creation of reqular users by useradd or newusers.

gid_min

Minimum range of group IDs used for the creation of regular groups by useradd, groupadd, or newusers.

gid_max

Maximum range of group IDs used for the creation of regular groups by useradd, groupadd, or newusers.

userdel_cmd

If defined, this command is run when removing a user. It should remove any at/cron/printjobs etc. owned by the user to be removed (passed as the first argument).

create_home

Indicate if a home directory should be created by default for new users. This setting does not apply to system users, and can be overriden on the command line.

usergroups_enab

This enables userdel to remove user groups if no members exist.

UAC Password

pass_max_days

The maximum number of days a password may be used. If the password is older than this, a password change will be forced. If not specified, -1 will be assumed (which disables the restriction). (PASS_MAX_

DAYS, PASS_MIN_DAVS and PASS_WARN_AGE are only used at the time of account creation. Any changes to these settings won't affect existing accounts).

pass_min_days

The minimum number of days allowed between password changes. Any password changes attempted sooner than this will be rejected. If not specified, -1 will be assumed (which disables the restriction). (PASS_MAX_DAYS, PASS_MIN_DAYS and PASS_WARN_AGE are only used at the time of account creation. Any changes to these settings won't affect existing accounts).

pass_warn_age

The number of days warning given before a password expires. A zero means warning is given only upon the day of expiration, a negative value means no warning is given. If not specified, no warning will be provided. (PASS_MAX_DAVS, PASS_MIN_DAVS and PASS_WARN_A6E are only used at the time of account creation. Any changes to these settings won't affect sting accounts).

Linux Attributes (Ubuntu)

Login

Default attributes applied when a user logs in

encrypt_method

This defines the system default encryption algorithm for encrypting passwords (if no algorithm are specified on the command line). It can take one of these values:

- **DES (default)**
- **MD5**
- **SHA256**
- **SHA512. Note: this parameter overrides the MD5_CRYPT_ENAB variable.**

md5_crypt_enab

This variable is deprecated. You should use ENCRYPT_METHOD. Indicate if passwords must be encrypted using the MD5—based algorithm. If set to yes, new passwords will be encrypted using the MD5—based algorithm compatible with the one used by recent releases of FreeBSD. It supports passwords of unlimited length and longer salt strings. Set to no if you need to copy encrypted passwords to other systems which do not understand the new algorithm. Default is no. This variable is superseded by the ENCRYPT__METHOD variable or by any command line option used to configure the encryption algorithm.

chfn_restrict

This parameter specifies which values in the gecos field of the /etc/passwd file may be changed by regular users using the chfn program. It can be any combination of letters f, r, w, h, for Full name, Room number, Work phone, and Home phone, respectively. For backward compatibility, yes is equivalent to rwh and no is equivalent to frwh. If not specified, only the superuser can make any changes. The most restrictive setting is better achieved by not installing chfn SUID.

default_home

Indicate if login is allowed if we cant cd to the home directory. Default in no. If set to yes, the user will login in the root (/) directory if it is not possible to cd to her home directory.

env_path

If set, it will be used to define the PATH environment variable when a regular user login. The value can be preceded by PATH=, or a colon separated list of paths (for example /bin:/usr/bin). The default value is PATH=/bin:/usr/bin.

env_supath

If set, it will be used to define the PATH environment variable when the superuser login. The value can be preceded by PATH=, or a colon separated list of paths (for example /sbin:/bin:/usr/sbin:/usr/bin). The default value is PATH=/sbin:/bin:/usr/sbin:/usr/bin.

erasechar

Terminal ERASE character (010 = backspace, 0177 = DEL). The value can be prefixed "0" for an octal value, or "0x" for an hexadecimal value.

faillog_enab

Enable logging and display of /var/log/faillog login failure info. This option conflicts with the pam_tally PAM module.

ftmp_file

If defined, login failures will be logged in this file in a utmp format. last, when invoked as lastb, will read /var/log/btmp

hushlogin_file

If defined, this file can inhibit all the usual chatter during the login sequence. If a full pathname is specified, then hushed mode will be enabled if the users name or shell are found in the file. If not a full pathname, then hushed mode will be enabled if the file exists in the users home directory.

killchar

Terminal KILL character (025 = CTRL/U). The value can be prefixed "0" for an octal value, or "0x" for an hexadecimal value.

login_retries

Maximum number of login retries in case of bad password. This will most likely be overridden by PAM, since the default pam_unix module has its own built in of 3 retries. However, this is a safe fallback in case you are using an authentication module that does not enforce PAM_MAXTRIES.

login_timeout

Max time in seconds for login.

log_ok_logins

Enable logging of successful logins.

log_unkfail_enab

Enable display of unknown usernames when login failures are recorded. Note: logging unknown usernames may be a security issue if an user enter her password instead of her login name.

su_name

If defined, the command name to display when running "su -". For example, if this is defined as "su" then a "ps" will display the command is "-su". If not defined, then "ps" would display the name of the shell actually being run, e.g. something like "-sh".

syslog_sg_enab

Enable syslog logging of sg activity.

syslog_su_enab

Enable "syslog" logging of su activity - in addition to sulog file logging.

ttygroup

The terminal permissions: the login tty will be owned by the TTYGROUP group, and the permissions will be set to TTYPERM. By default, the ownership of the terminal is set to the users primary group and the permissions are set to 0600. TTYGROUP can be either the name of a group or a numeric group identifier. If you have a write program which is "setgid" to a special group which owns the terminals, define TTYGROUP to the group number and TTYPERM to 0620. Otherwise leave TTYGROUP commented out and assign TTYPERM to either 622 or 600.

ttyperm

The terminal permissions: the login tty will be owned by the TTYGROUP group, and the permissions will be set to TTYPERM. By default, the ownership of the terminal is set to the users primary group and the permissions are set to 0600. TTYGROUP can be either the name of a group or a numeric group identifier. If you have a write program which is "setgid" to a special group which owns the terminals, define TTYGROUP to the group number and TTYPERM to 0620. Otherwise leave TTYGROUP commented out and assign TTYPERM to either 622 or 600.

User Account Defaults (UAD)

mail_dir

The mail spool directory. This is needed to manipulate the mailbox when its corresponding user account is modified or deleted. If not specified, a compile-time default is used.

unmask

Determines file permissions at time of creation: the default is 022.

User Account Creation (UAC)

uid_min

Minimum range of user IDs used for the creation of regular users by useradd or newusers.

uid_max

Maximum range of user IDs used for the creation of reqular users by useradd or newusers.

gid_min

Minimum range of group IDs used for the creation of regular groups by useradd, groupadd, or newusers.

gid_max

Maximum range of group IDs used for the creation of regular groups by useradd, groupadd, or newusers.

usergroups_enab

This enables userdel to remove user groups if no members exist.

dshell

The dshell variable specifies the default login shell on your system.

dhome

The dhome variable specifies the directory containing users home directories.

grouphomes

If grouphomes is yes, then the home directories will be created as /home/groupname/user.

letterhomes

If letterhomes is yes, then the created home directories will have an extra directory - the first letter of the user name. For example: /home/u/user.

skel

The skel variable specifies the directory containing skeletal user files; in other words, files such as a sample .profile that will be copied to the new users home directory when it is created.

first_system_uid

first_system_[gu]id to last_system_[gu]id inclusive is the range for UIDs for dynamically allocated administrative and system accounts/groups. Please note that system software, such as the users allocated by the base-passwd package, may assume that UIDs less than 100 are unallocated.

last_system_uid

first_system_[gu]id to last_system_[gu]id inclusive is the range for UIDs for dynamically allocated administrative and system accounts/groups. Please note that system software, such as the users allocated by the base-passwd package, may assume that UIDs less than 100 are unallocated.

first_system_gid

first_system_[gu]id to last_system_[gu]id inclusive is the range for UIDs for dynamically allocated administrative and system accounts/groups. Please note that system software, such as the users allocated by the base-passwd package, may assume that UIDs less than 100 are unallocated.

last_system_gid

first_system_[gu]id to last_system_[gu]id inclusive is the range for UIDs for dynamically allocated administrative and system accounts/groups. Please note that system software, such as the users allocated by the base-passwd package, may assume that UIDs less than 100 are unallocated.

first_uid

first_[gu]id to last_[gu]id inclusive is the range of UIDs of dynamically allocated user accounts/groups.

last_uid

first_[gu]id to last_[gu]id inclusive is the range of UIDs of dynamically allocated user accounts/groups.

first_gid

first_[gu]id to last_[gu]id inclusive is the range of UIDs of dynamically allocated user accounts/groups.

last_gid

first_[gu]id to last_[gu]id inclusive is the range of UIDs of dynamically allocated user accounts/groups.

usergroups

The usergroups variable can be either yes or no. If yes each created user will be given their own group to use as a default. If "no", each created user will be placed in the group whose gid is USERS_GID (see below).

users_gid

If usergroups is no, then users_gid should be the GID of the group users (or the equivalent group) on your system.

dir_mode

If dir_mode is set, directories will be created with the specified mode. Otherwise the default mode 0755 will be used.

quotauser

If quotauser is set, a default quota will be set from that user with `edquota -p quotauser newuser

skel_ignore_regex

If skel_ignore_regex is set, adduser will ignore files matching this regular expression when creating a new home directory.

UAC Password

pass_max_days

The maximum number of days a password may be used. If the password is older than this, a password change will be forced. If not specified, -1 will be assumed (which disables the restriction). (PASS_MAX_DAYS, PASS_MIN_DAVS and PASS_WARN_AGE are only used at the time of account creation. Any changes to these settings won't affect existing accounts).

pass_min_days

The minimum number of days allowed between password changes. Any password changes attempted sooner than this will be rejected. If not specified, -1 will be assumed (which disables the restriction). (PASS_MAX_DAYS, PASS_MIN_DAYS and PASS_WARN_AGE are only used at the time of account creation. Any changes to these settings won't affect existing accounts).

pass_warn_age

The number of days warning given before a password expires. A zero means warning is given only upon the day of expiration, a negative value means no warning is given. If not specified, no warning will be provided. (PASS_MAX_DAVS, PASS_MIN_DAVS and PASS_WARN_A6E are only used at the time of account creation. Any changes to these settings won't affect sting accounts).

Linux Attributes (SLES)

Login

chfn_restrict

This parameter specifies which values in the gecos field of the /etc/passwd file may be changed by regular users using the chfn program. It can be any combination of letters f, r, w, h, for Full name, Room number, Work phone, and Home phone, respectively. For backward compatibility, yes is equivalent to rwh and no is equivalent to frwh. If not specified, only the superuser can make any changes. The most restrictive setting is better achieved by not installing chfn SUID.

Console

If defined, either full pathname of a file containing device names or a ":" delimited list of device names. Root logins will be allowed only upon these devices.

console_groups

List of groups to add to the users supplementary group set when logging in on the console (as determined by the CONSOLE setting). Default is none.

default_home

Indicate if login is allowed if we cant cd to the home directory. Default is no. If set to yes, the user will login in the root (/) directory if it is not possible to cd to her home directory.

encrypt_method

This defines the system default encryption algorithm for encrypting passwords (if no algorithm are specified on the command line). It can take one of these values: DES (default), MD5, SHA256, SHA512.

Note: this parameter overrides the MD5_CRYPT_ENAB variable.

encrypt_method_nis

This defines the system default encryption algorithm for encrypting passwords for NIS systems (if no algorithm are specified on the command line). It can take one of these values: DES (default), MD5, SHA256, SHA512.

env_path

If set, it will be used to define the PATH environment variable when a regular user login. The value can be preceded by PATH=, or a colon separated list of paths (for example /bin:/usr/bin). The default value is PATH=/bin:/usr/bin.

env_rootpath

The default PATH settings for root (used by login)

env_supath

If set, it will be used to define the PATH environment variable when the superuser login. The value can be preceded by PATH=, or a colon separated list of paths (for example /sbin:/bin:/usr/sbin:/usr/bin). The default value is PATH=/sbin:/bin:/usr/sbin:/usr/bin.

erasechar

Terminal ERASE character

fail_delay

Delay in seconds before being allowed another attempt after a login failure.

hushlogin_file

If defined, this file can inhibit all the usual chatter during the login sequence. If a full pathname is specified, then hushed mode will be enabled if the users name or shell are found in the file. If not a full pathname, then hushed mode will be enabled if the file exists in the users home directory.

killchar

Terminal KILL character (025 = CTRL/U). The value can be prefixed "0" for an octal value, or "0x" for an hexadecimal value.

log_ok_logins

Enable logging of successful logins.

log_unkfail_enab

Enable display of unknown usernames when login failures are recorded. Note: logging unknown usernames may be a security issue if an user enter her password instead of her login name.

login_retries

Maximum number of login retries in case of bad password. This will most likely be overridden by PAM, since the default pam_unix module has its own built in of 3 retries. However, this is a safe fallback in case you are using an authentication module that does not enforce PAM_MAXTRIES.

login_timeout

Max time in seconds for login.

motd_file

If defined, ":" delimited list of "message of the day" files to be displayed upon login.

sha_crypt_max_rounds

Only works if ENCRYPT_METHOD is set to SHA256 or SHA512. Define the number of SHA rounds. With a lot of rounds, it is more difficult to brute forcing the password. But note also that it more CPU resources will be needed to authenticate users. If not specified, the libc will choose the default number of rounds (5000). The values must be inside the 1000-999999999 range. If only one of the MIN or MAX values is set, then this value will be used. If MIN > MAX, the highest value will be used.

sha_crypt_min_rounds

Only works if ENCRYPT_METHOD is set to SHA256 or SHA512. Define the number of SHA rounds. With a lot of rounds, it is more difficult to brute forcing the password. But note also that it more CPU resources will be needed to authenticate users. If not specified, the libc will choose the default number of rounds (5000). The values must be inside the 1000-999999999 range. If only one of the MIN or MAX values is set, then this value will be used. If MIN > MAX, the highest value will be used.

sulog_file

If defined, all su activity is logged to this file.

syslog_sg_enab

Enable syslog logging of sg activity.

syslog_su_enab

Enable "syslog" logging of su activity - in addition to sulog file logging.

ttygroup

The terminal permissions: the login tty will be owned by the TTYGROUP group, and the permissions will be set to TTYPERM. By default, the ownership of the terminal is set to the users primary group and the permissions are set to 0600. TTYGROUP can be either the name of a group or a numeric group identifier. If you have a write program which is "setgid" to a special group which owns the terminals, define TTYGROUP to the group number and TTYPERM to 0620. Otherwise leave TTYGROUP commented out and assign TTYPERM to either 622 or 600.

ttyperm

The terminal permissions: the login tty will be owned by the TTYGROUP group, and the permissions will be set to TTYPERM. By default, the ownership of the terminal is set to the users primary group and the permissions are set to 0600. TTYGROUP can be either the name of a group or a numeric group identifier. If you have a write program which is "setgid" to a special group which owns the terminals, define TTYGROUP to the group number and TTYPERM to 0620. Otherwise leave TTYGROUP commented out and assign TTYPERM to either 622 or 600.

ttytype_file

If defined, file which maps tty line to TERM environment parameter. Each line of the file is in a format something like "vt100 tty01".

User Account Defaults (UAD)

groupadd_cmd

If defined, this command is run when adding a group.

umask

Determines file permissions at time of creation; the default is 022.

create_home

Indicate if a home directory should be created by default for new users. This setting does not apply to system users, and can be overriden on the command line.

gid_max

Maximum range of group IDs used for the creation of regular groups by useradd, groupadd, or newusers.

gid_min

Minimum range of group IDs used for the creation of regular groups by useradd, groupadd, or newusers.

max_members_per_group

If set to a non-nul number, the shadow utilities will make sure that groups never have more than this number of users on one line. This permits support to split groups (groups split into multiple lines, with the same group ID, to avoid limitation of the line length in the group file). 0 is the default value and disables this feature.

sys_gid_max

(SUSE 12) SYS_GID_MIN to SYS_GID_MAX inclusive is the range for GIDs for dynamically allocated administrative and system groups.

sys_gid_min

(SUSE 12) SYS_GID_MIN to SYS_GID_MAX inclusive is the range for GIDs for dynamically allocated administrative and system groups.

sys_uid_max

(SUSE 12) SYS_UID_MIN to SYS_UID_MAX inclusive is the range for UIDs for dynamically allocated administrative and system accounts.

sys_uid_min

(SUSE 12) SYS_UID_MIN to SYS_UID_MAX inclusive is the range for UIDs for dynamically allocated administrative and system accounts.

uid_max

Maximum range of user IDs used for the creation of regular users by useradd or newusers.

uid_min

Minimum range of user IDs used for the creation of regular users by useradd or newusers.

useradd_cmd

If defined, this command is run when adding a user.

userdel_cmd

If defined, this command is run when removing a user. It should remove any at/cron/print jobs etc. owned by the user to be removed (passed as the first argument).

userdel_postcmd

If defined, this command is run after removing a user.

userdel_precmd

UserAccountCreationMisc

usergroups_enab

This enables userdel to remove user groups if no members exist.

UAC (Password)

pass_max_days

The maximum number of days a password may be used. If the password is older than this, a password change will be forced. -1 value means the restriction is disabled. If not specified, -1 will be assumed. (PASS_MAX_DAYS, PASS_MIN_DAYS and PASS_WARN_AGE are only used at the time of account creation. Any changes to these settings will not affect existing accounts).

pass_min_days

The minimum number of days allowed between password changes. Any password changes attempted sooner than this will be rejected. -1 value means the restriction is disabled. If not specified, -1 will be assumed. (PASS_MAX_DAYS, PASS_MIN_DAYS and PASS_WARN_AGE are only used at the time of account creation. Any changes to these settings will not affect existing accounts).

pass_warn_age

The number of days warning given before a password expires. A zero means warning is given only upon the day of expiration. -1 value means no warning is given. If not specified, -1 will be assumed (which disables the warning). (PASS_MAX_DAYS, PASS_MIN_DAYS and PASS_WARN_AGE are only used at the time of account creation. Any changes to these settings will not affect existing accounts).

AIX Attributes

Auditing

binmode

Controls whether bin collection, as defined in the bin stanza, is used.

streammode

Controls whether stream data collection, as defined in the file specified in the stream stanza, is configured at the start up of the audit system.

trail

Specifies the path name of the audit trail file.

bin1

Specifies the path name that the auditbin daemon uses for its primary bin file.

bin2

Specifies the path name that the auditbin daemon uses for its secondary bin file.

binsize

Specifies a decimal integer string that defines the threshold size (in bytes) of each audit bin.

bincmds

Specifies the path name of the file that contains the audit backend commands called by the auditbin daemon.

freespace

Specifies a decimal integer string that defines the recommended number of 512-byte free blocks in the file system where the audit trail file is located.

streamcmds

To enable the auditbin daemon to set up stream collection, add lines to the start and stream stanzas of the /etc/security/audit/config file.

Login

auth_type *

Defines the route through which all users will be authenticated (in supported applications).

dist_uniqid

Defines the system configuration for resolving ID collision for creating/modifying user/group accounts among registries.

logintimeout

Defines the time (in seconds) the user is given to type the login name and the password.

maxlogins

Defines the maximum number of simultaneous logins to the system.

maxroles

Defines the maximum number of roles that each session allows.

mkhomeatlogin

Specifies whether to create a home directory at login if the home directory does not already exist.

shells

Defines the valid shells on the system.

pwd_algorithm *

Defines the loadable password algorithm to use when you store user passwords.

User Account Defaults (UAD)

admin

Defines the administrative status of the user. Possible values are: (1) true - The user is an administrator. Only the root user can change the attributes of users defined as administrators. (2) false- The user is not an administrator. This is the default value.

admgroups

Lists the groups the user administrates. The value parameter is a comma-separated list of group names.

auth1 *

Primary auth method (Deprecated: use SYSTEM), Lists the primary methods for authenticating the user.

auth2 *

Lists the secondary methods for authenticating the user.

SYSTEM *

Defines the system authentication mechanism for the user.

capabilities

Defines the system privileges (capabilities) which are granted to a user by the login or su commands.

default_roles *

Specifies the default roles for the user; can only contain roles assigned to the user in the roles attribute. You can use the ALL keyword to signify that the default roles for the user are all their assigned roles.

rcmds

Controls the remote execution of the r-commands (rsh, rexec, rcp); Possible values are allow (default), deny, and hostlogincontrol, which specifies that the ability of remote command execution is determined by the hostsallowedlogin and hostsdeniedlogin attributes. The user is only allowed to execute remote commands on a target system if the user (or target user) is allowed to log in the target system.

roles *

Lists the administrative roles for this user. The Value parameter is a list of role names, separated by commas.

su

Indicates whether another user can switch to the specified user account with the su command - true (default) or false.

sugroups

Lists the groups that can use the su command to switch to the specified user account; a value of ALL indicates all groups. An ! (exclamation point) in front of a group name excludes that group. If this attribute is not specified, all groups can switch to this user account with the su command.

umask

Determines file permissions at time of creation; the default is 022.

AUD (Password)

dictionlist *

Defines the password dictionaries used when creating new passwords.

histexpire

Defines the period of time (in weeks) that a user cannot reuse a password. The value is a decimal integer string. The default is 0, indicating that no time limit is set. Only an administrative user can change this attribute.

histsize

Defines the number of previous passwords a user cannot reuse. The value is a decimal integer string. The default is 0. Only an administrative user can change this attribute.

maxage

Defines the maximum age in weeks of a password. The password must be changed by this time. The value is a decimal integer string. The default is a value of 0, indicating no maximum age. Range: 0 to 52

maxexpired

Defines the maximum time in weeks beyond maxage that a user can change an expired password. After this defined time, only an administrative user can change the password. The value is a decimal integer string. The default is -1, which means the user can always change their expired password regardless of how many weeks have passed. If the maxexpired attribute is 0, the password expires when the maxage value is met. If the maxage attribute is 0, the maxexpired attribute is ignored. Range: 0 to 52 (a root user is exempt from maxexpired)

maxrepeats

Defines the maximum number of times a character can be repeated in a new password. Since a value of 0 is meaningless, the default value of 8 indicates that there is no maximum number. The value is a decimal integer string. Range: 0 to 8

minage

Defines the minimum age (in weeks) a password must be before it can be changed. The value is a decimal integer string. The default is a value of 0, indicating no minimum age. Range: 0 to 52

minalpha

Defines the minimum number of alphabetic characters that must be in a new password. The value is a decimal integer string. The default is a value of 0, indicating no minimum number. Range: 0 to 8

mindiff

Defines the minimum number of characters required in a new password that were not in the old password. The value is a decimal integer string. The default is a value of 0, indicating no minimum number. Range: 0 to 8

minlen

Defines the minimum length of a password. The value is a decimal integer string. The default is a value of 0, indicating no minimum length. The maximum value allowed is 8. This attribute is determined by by minlen and/or minalpha + minother, whichever is greater. minalpha + minother should never be greater than 8. If minalpha + minother is greater than 8, then the effective value for minother is reduced to 8 - minalpha.

minother

Defines the minimum number of non-alphabetic characters that must be in a new password. The value is a decimal integer string. The default is a value of 0, indicating no minimum number. Range: 0 to 8

pwdchecks *

Defines the password restriction methods enforced on new passwords. The value is a list of comma-separated method names and is evaluated from left to right. A method name is either an absolute path name or a path name relative to /usr/lib of an executable load module.

pwdwarntime

Defines the number of days before the system issues a warning that a password change is required. The value is a decimal integer string. A zero or negative value indicates that no message is issued. The value must be less than the difference of the maxage and minage attributes. Values greater than this difference are ignored and a message is issued when the minage value is reached.

UAD (Login)

account_locked *

Indicates if the user account is locked - yes, true, and always are equivalent; no, false, and never are equivalent.

expires

Identifies the expiration date of the account. The Value parameter is a 10-character string in the MMDDhhmmYY form, where MM = month, DD = day, hh = hour, mm = minute, and YY = last 2 digits of the years 1939 through 2038. All characters are numeric. If the Value parameter is 0, the account does not expire. The default is 0.

login

Indicates if the user can log into the system with the login command - true (default) or false.

logindelay

The time in seconds between login prompts. This will be multiplied with the number of failed attempts; for example, 5,10,15,20 seconds when 5 is the initial value.

logindisable

Disable login on this terminal after logintimes consecutive failed attempts.

loginreenable

Re-enable the terminal after it was automatically disabled after specified minutes.

loginretries

Defines the number of unsuccessful login attempts allowed after the last successful login before the system locks the account; A zero or negative value indicates that no limit exists.

logininterval

Terminal will be disabled when the specified invalid attempts have been made within specified seconds.

logintimes

Defines the days and times that the user is allowed to access the system.

maxulogs

Defines the maximum number of logins for the user. If the concurrent login number for a user exceeds the maximum number of allowed logins, the login is denied.

rlogin *

Indicates if the user can access the account remotely with the telnet or rlogin commands - true (default) or false.

sak_enabled

Values for the sak_enabled attribute are: true - SAK processing is enabled, so the key sequence establishes a trusted path for the port: false - SAK processing is not enabled, so a trusted path cannot be established. This is the default value.

User Account Creation (UAC)

admgroups

Lists the groups the user administrates. The value parameter is a comma-separated list of group names.

auth1 *

Primary auth method (Deprecated: use SYSTEM), Lists the primary methods for authenticating the user.

auth2 *

Lists the secondary methods for authenticating the user.

SYSTEM *

Defines the system authentication mechanism for the user.

capabilities

Defines the system privileges (capabilities) which are granted to a user by the login or su commands.

default_roles *

Specifies the default roles for the user; can only contain roles assigned to the user in the roles attribute. You can use the ALL keyword to signify that the default roles for the user are all their assigned roles.

home

Full path name of the home directory of the user. The $USER macro can be used for defining policy, e.g. /home/$USER.

rcmds

Controls the remote execution of the r-commands (rsh, rexec, rcp); Possible values are allow (default), deny, and hostlogincontrol, which specifies that the ability of remote command execution is determined by the hostsallowedlogin and hostsdeniedlogin attributes. The user is only allowed to execute remote commands on a target system if the user (or target user) is allowed to log in the target system.

roles *

Lists the administrative roles for this user. The Value parameter is a list of role names, separated by commas.

shell

Defines the program run for the user at session initiation - full path name.

su

Indicates whether another user can switch to the specified user account with the su command - true (default) or false.

sugroups

Lists the groups that can use the su command to switch to the specified user account; a value of ALL indicates all groups. An ! (exclamation point) in front of a group name excludes that group. If this attribute is not specified, all groups can switch to this user account with the su command.

umask

Determines file permissions at time of creation; the default is 022.

User Account Creation (UAC)

admgroups

Lists the groups the user administrates. The value parameter is a comma-separated list of group names.

auth1 *

Primary auth method (Deprecated: use SYSTEM), Lists the primary methods for authenticating the user.

auth2 *

Lists the secondary methods for authenticating the user.

SYSTEM *

Defines the system authentication mechanism for the user.

capabilities

Defines the system privileges (capabilities) which are granted to a user by the login or su commands.

default_roles *

Specifies the default roles for the user; can only contain roles assigned to the user in the roles attribute. You can use the ALL keyword to signify that the default roles for the user are all their assigned roles.

home

Full path name of the home directory of the user. The $USER macro can be used for defining policy, e.g. /home/$USER.

rcmds

Controls the remote execution of the r-commands (rsh, rexec, rcp); Possible values are allow (default), deny, and hostlogincontrol, which specifies that the ability of remote command execution is determined by the hostsallowedlogin and hostsdeniedlogin attributes. The user is only allowed to execute remote commands on a target system if the user (or target user) is allowed to log in the target system.

roles *

Lists the administrative roles for this user. The Value parameter is a list of role names, separated by commas.

shell

Defines the program run for the user at session initiation - full path name.

su

Indicates whether another user can switch to the specified user account with the su command - true (default) or false.

sugroups

Lists the groups that can use the su command to switch to the specified user account; a value of ALL indicates all groups. An ! (exclamation point) in front of a group name excludes that group. If this attribute is not specified, all groups can switch to this user account with the su command.

umask

Determines file permissions at time of creation; the default is 022.

UAC (Auditing)

auditclasses *

Lists the users audit classes. The Value parameter is a list of comma-separated classes, or a value of ALL to indicate all audit classes.

UAC (Group)

pgrp

Identifies the users primary group - value cannot be null. The $USER macro can be used for defining policy, e.g. $USER.

groups

Identifies the groups the user belongs to. The $USER macro can be used for defining policy, e.g. $USER group2 group3.

UAC (Password)

dictionlist *

Defines the password dictionaries used when creating new passwords.

histexpire

Defines the period of time (in weeks) that a user cannot reuse a password. The value is a decimal integer string. The default is 0, indicating that no time limit is set. Only an administrative user can change this attribute.

histsize

Defines the number of previous passwords a user cannot reuse. The value is a decimal integer string. The default is 0. Only an administrative user can change this attribute.

maxage

Defines the maximum age in weeks of a password. The password must be changed by this time. The value is a decimal integer string. The default is a value of 0, indicating no maximum age. Range: 0 to 52

maxexpired

Defines the maximum time in weeks beyond maxage that a user can change an expired password. After this defined time, only an administrative user can change the password. The value is a decimal integer string. The default is -1, which means the user can always change their expired password regardless of how many weeks have passed. If the maxexpired attribute is 0, the password expires when the maxage value is met. If the maxage attribute is 0, the maxexpired attribute is ignored. Range: 0 to 52 (a root user is exempt from maxexpired)

maxrepeats

Defines the maximum number of times a character can be repeated in a new password. Since a value of 0 is meaningless, the default value of 8 indicates that there is no maximum number. The value is a decimal integer string. Range: 0 to 8

minage

Defines the minimum age (in weeks) a password must be before it can be changed. The value is a decimal integer string. The default is a value of 0, indicating no minimum age. Range: 0 to 52

minalpha

Defines the minimum number of alphabetic characters that must be in a new password. The value is a decimal integer string. The default is a value of 0, indicating no minimum number. Range: 0 to 8

mindiff

Defines the minimum number of characters required in a new password that were not in the old password. The value is a decimal integer string. The default is a value of 0, indicating no minimum number. Range: 0 to 8

minlen

Defines the minimum length of a password. The value is a decimal integer string. The default is a value of 0, indicating no minimum length. The maximum value allowed is 8. This attribute is determined by by minlen and/or minalpha + minother, whichever is greater. minalpha + minother should never be greater than 8. If minalpha + minother is greater than 8, then the effective value for minother is reduced to 8 - minalpha.

minother

Defines the minimum number of non-alphabetic characters that must be in a new password. The value is a decimal integer string. The default is a value of 0, indicating no minimum number. Range: 0 to 8

pwdchecks *

Defines the password restriction methods enforced on new passwords. The value is a list of comma-separated method names and is evaluated from left to right. A method name is either an absolute path name or a path name relative to /usr/lib of an executable load module.

pwdwarntime

Defines the number of days before the system issues a warning that a password change is required. The value is a decimal integer string. A zero or negative value indicates that no message is issued. The value must be less than the difference of the maxage and minage attributes. Values greater than this difference are ignored and a message is issued when the minage value is reached.

UAC (Login)

account_locked *

Indicates if the user account is locked - yes, true, and always are equivalent; no, false, and never are equivalent.

expires

Identifies the expiration date of the account. The Value parameter is a 10-character string in the MMDDhhmmYY form, where MM = month, DD = day, hh = hour, mm = minute, and YY = last 2 digits of the years 1939 through 2038. All characters are numeric. If the Value parameter is 0, the account does not expire. The default is 0.

login

Indicates if the user can log into the system with the login command - true (default) or false

loginretries

DDefines the number of unsuccessful login attempts allowed after the last successful login before the system locks the account; A zero or negative value indicates that no limit exists.

maxulogs

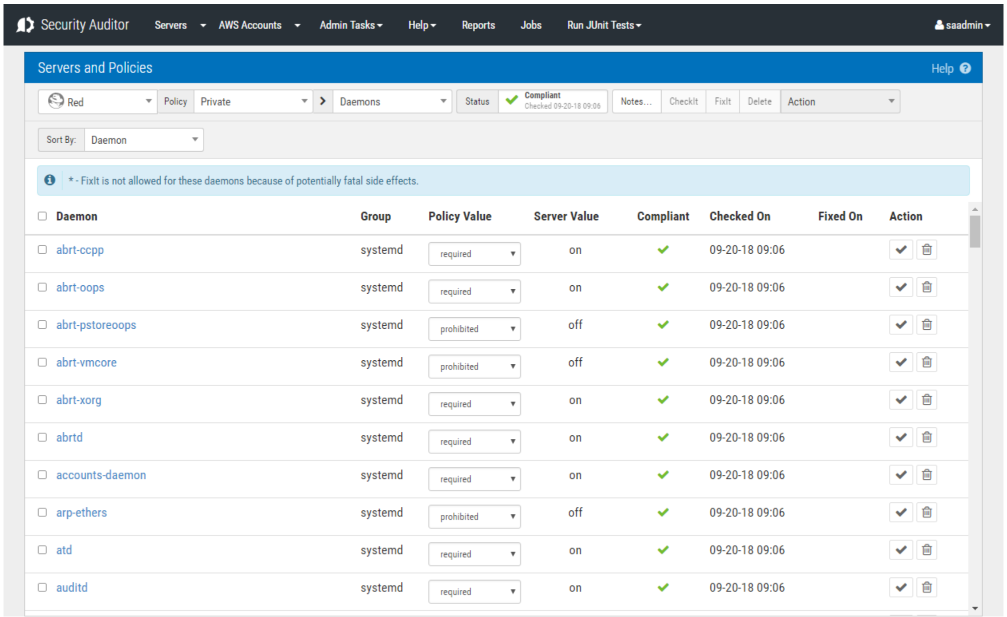
Defines the maximum number of logins for the user. If the concurrent login number for a user exceeds the maximum number of allowed logins, the login is denied.

rlogin *

Indicates if the user can access the account remotely with the telnet or rlogin commands - true (default) or false.

Servers and Policies - Daemons

Use this screen to configure and manage Daemon Policy Templates. Security Auditor allows you to define your policy for daemons – whether they are required to be running, restricted from (should not be) running or it doesn't matter whether they're running or not. To initialize the Security Auditor Daemon category, go to **Servers > Initialize Policies** and choose to initialize the Daemon category. Daemons that are running appear in this list. See Daemons.



* - FixIt is not allowed for these daemons because of potentially fatal side effects.

□ Daemon	Group	Policy Value	Server Value	Compliant	Checked On	Fixed On	Action
□ abrt-ccpp	systemd	required	on	✓	09-20-18 09:06		
□ abrt-oops	systemd	required	on	✓	09-20-18 09:06		
□ abrt-pstoreoops	systemd	prohibited	off	✓	09-20-18 09:06		
□ abrt-vmcore	systemd	prohibited	off	✓	09-20-18 09:06		
□ abrt-xorg	systemd	required	on	✓	09-20-18 09:06		
□ abrtd	systemd	required	on	✓	09-20-18 09:06		
□ accounts-daemon	systemd	required	on	✓	09-20-18 09:06		
□ arp-ethers	systemd	prohibited	off	✓	09-20-18 09:06		
□ atd	systemd	required	on	✓	09-20-18 09:06		
□ auditd	systemd	required	on	✓	09-20-18 09:06		

How to get there

In the Manage Servers screen, choose D for a server.

What it Does

The Daemons page of the Servers and Policies screen displays an overview of the status of Daemons policy templates.

Status

Displays the status of the Policies and when they were last checked.

Notes

Choose this option to open the Daemons Policy Notes screen where you can record any notes related to the Policy. Notes appear in reports and provide a place to explain the intent of defined policies.

CheckIt

Use this button to run CheckIt, which performs a compliance check for the selected attribute(s).

FixIt

Use this button to run FixIt, which changes the value on the server to match that of Security Auditor.

Delete

Use this button to delete the selected attribute(s).

Action; Enable CheckIt • Disable CheckIt • Enable FixIt • Disable FixIt • Accept as Policy

Use these options to enable/disable CheckIt and/or FixIt for selected attributes. Choose Accept as Policy to redefine the policy to match the server value for selected attributes.

Organize By; Category • List

Choose Category to organize the attributes by category (Login, User Account Defaults (UAD), User Account Creation (UAC), and UAC (Password)). Choose List to display the Sort By drop-down menu, where you can choose the method to sort the selected attributes.

Sort By

Use this drop-down menu to choose how you want to organize the list of Daemons.

Field Descriptions

Daemon

The list of daemons on the server. Use the Sort By drop-down menu above to adjust the sort order of this list.

Group

The group of the daemon.

Policy Value

This column indicates Security Auditor's Policy Value. Once initialized, you can alter the daemon settings to indicate whether they are Required (must be running), Prohibited (cannot be running) or Allowed (can be running or stopped).

Server Value

This column indicates the daemon's value on the server.

Compliant

This column indicates whether the Server Value is compliant with the Policy Value setting.

Checked On

This column indicates date and time the Server Value was checked against the Policy Value.

Fixed On

This column indicates date and time the Server Value was fixed to match the Policy Value.

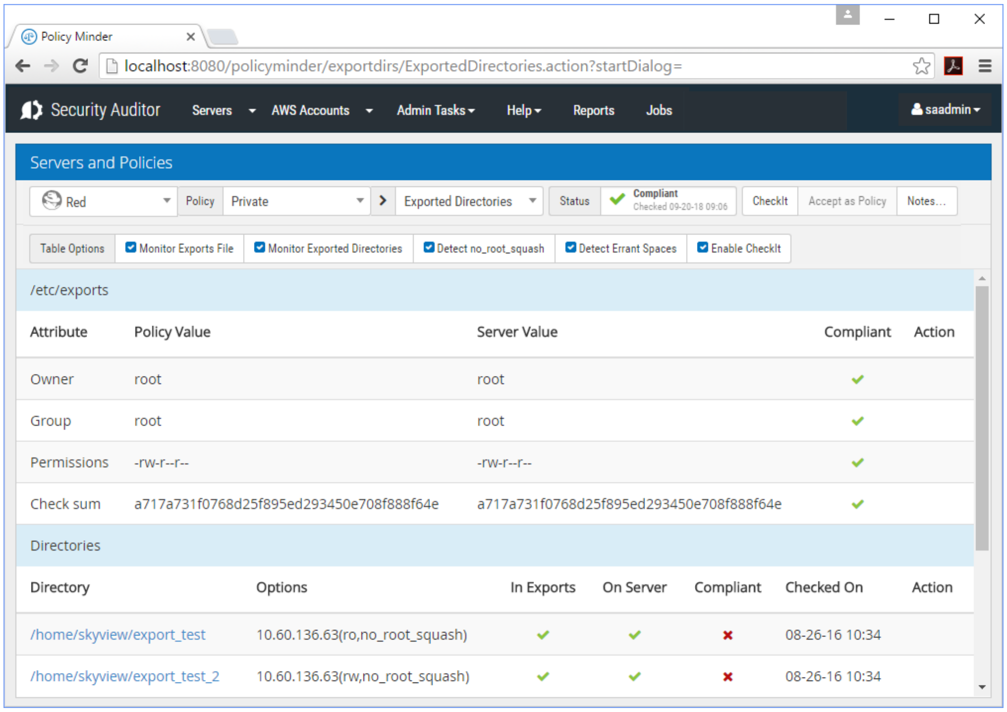
Action

Click ✓ to run CheckIt on the daemon.

Click 🗑 to delete the daemon from Security Auditor. This does NOT delete the daemon from the server – only from the policy and subsequent compliance checks.

Servers and Policies - Exported Directories

Use this screen to configure and manage Exported Directory Policy Templates.



/etc/exports

Attribute	Policy Value	Server Value	Compliant	Action
Owner	root	root	✓	
Group	root	root	✓	
Permissions	-rw-r--r--	-rw-r--r--	✓	
Check sum	a717a731f0768d25f895ed293450e708f888f64e	a717a731f0768d25f895ed293450e708f888f64e	✓	

Directories

Directory	Options	In Exports	On Server	Compliant	Checked On	Action
/home/skyview/export_test	10.60.136.63(ro,no_root_squash)	✓	✓	✗	08-26-16 10:34	
/home/skyview/export_test_2	10.60.136.63(rw,no_root_squash)	✓	✓	✗	08-26-16 10:34	

How to get there

In the Manage Servers screen, choose E for a server.

What it Does

The Exported Directories page of the Servers and Policies screen displays an overview of the status of Exported Directories policy templates.

Monitor Exports File

Establish file attributes baseline and monitor for correct values over time.

Monitor Exported Directories

Establish directory attributes baseline and monitor for correct values over time.

Detect no_root_squash

If no_root_squash is set for a directory, a root user from a client system will become a root user on the server system.

Detect Errant Spaces

If there is an errant space between the export host and the first parenthesis around options the meaning of the export definition changes.

Enable CheckIt

Enable CheckIt for the policy.

CheckIt

Access server to discover new entities defined by policy and monitor attributes of entities in policy

Accept as Policy

Accept entities and values last found on server as current policy.

Notes

Add a description of the policy. This description is included in reports.

Table Options

Monitor Exports File

Establish File attributes baseline and monitor for correct values over time.

Monitor Exported Directories

Establish Directory attributes baseline and monitor for correct values over time.

Detect no_root_squash

If no_root_squash is set for a directory, a root user from a client system will become a root user on the server system.

Detect Errant Spaces

If there is an errant space between the export host and the first parenthesis around options, the meaning of the export definition changes.

Enable CheckIt

Check this box to enable CheckIt for Exported Directories.

Field Descriptions

/etc/exports

Attribute

The policy attribute.

Policy Value

The value of the attribute defined by Security Auditor.

> **NOTE:** The 'Check sum' attribute is always ignored when testing Group Policy compliance of Exported Directories. This is because any insignificant difference (e.g. an extra space character) in the "/etc/exports" file on any server will cause its check sum to not match and be non-compliant.

Server Value

The value of the attribute on the server.

Compliant

The status of the Exported Directories Policy template for the directory. Not checked ✱, Not Compliant ✖ , or Compliant ✔.

Action

If there is a change on the server, the Set as Policy button ☑ appears under the Actions column. Click ☑ **Set as Policy** to set your policy to match the server.

Directories

Directory

The path of the exported directory.

Options

This column lists options used on the exported directory. Examples can be found on the IBM Knowledge Center under Exports File for NFS.

In Exports • On Server • Compliant

The status of the exported directory. Not checked ✱, Not Compliant ✖ , or Compliant ✔.

Checked On

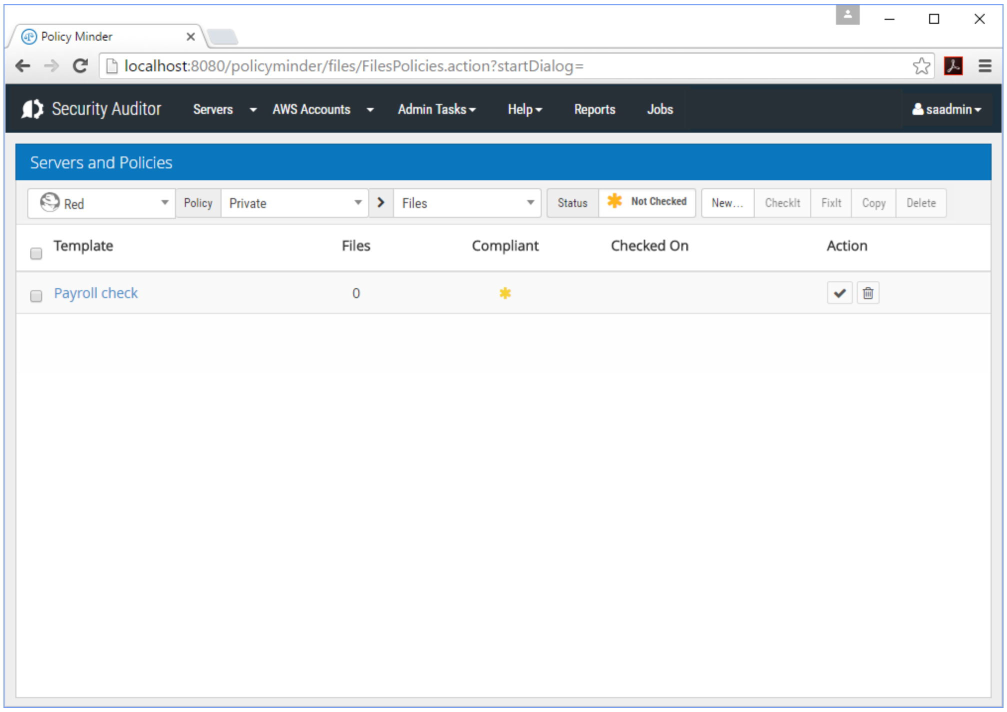
The date and time the directory was last checked.

Action

If there is a change on the server, the Set as Policy button ☑ appears under the Actions column. Click ☑ **Set as Policy** to set your policy to match the server.

Servers and Policies - Files

Use this screen to configure and manage initialized File Policy Templates.



localhost:8080/policyminder/files/FilesPolicies.action?startDialog=

□ Template	Files	Compliant	Checked On	Action
□ Payroll check	0	*		✓ 🗑

How to get there

In the Manage Servers screen, choose F for a server.

What it Does

The Files page of the Servers and Policies screen displays an overview of the status of Files policy templates.

Status

Displays the status of the Policies and when they were last checked.

New

Use this button to add a new policy Template.

CheckIt

Use this button to run CheckIt, which performs a compliance check for the selected attribute(s).

FixIt

Use this button to run FixIt, which changes the value on the server to match that of Security Auditor.

Copy

Use this button to copy the selected attribute(s), in order to copy to a different server.

Delete

Use this button to delete the selected attribute(s).

Field Descriptions

Template

The name of the policy template.

Files

Number of files included in the policy template.

Compliant

Indicates whether the server is compliant with the policy.

Checked On

Indicates the date and time the policy was last checked.

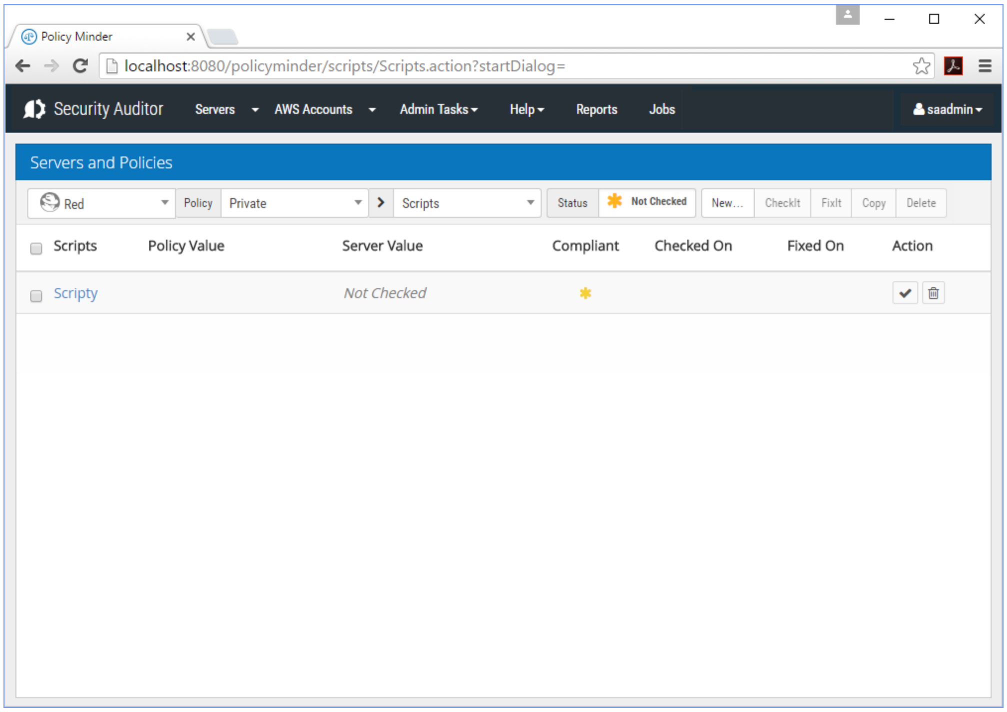
Action

Click ✓ to run CheckIt on the policy.

Click 🗑 to delete the policy from Security Auditor.

Servers and Policies - Scripts

Use this screen to configure and manage Script Policy Templates. The Scripts category makes it possible for you to upload scripts into the Security Auditor console and run them as part of your compliance checks. See Scripts and Add a New Script Policy screen.



Red | Policy: Private > Scripts | Status: ✱ Not Checked

□	Scripts	Policy Value	Server Value	Compliant	Checked On	Fixed On	Action
□	Scripty		*Not Checked*	✱			✓ 🗑

How to get there

In the Manage Servers screen, choose S for a server.

What it Does

The Scripts page of the Servers and Policies screen displays an overview of the status of Script policy templates.

New

Use this button to add a new policy Template.

CheckIt

Use this button to run CheckIt, which performs a compliance check for the selected attribute(s).

FixIt

Use this button to run FixIt, which changes the value on the server to match that of Security Auditor.

Copy

Use this button to copy the selected Template(s), in order to copy to a different server.

Delete

Use this button to delete the selected Template(s).

Field Descriptions

Scripts

The name of the script on the server.

Policy Value

The value of the script defined by Security Auditor.

Server Value

The value of the script on the server.

Compliant

The status of the Scripts Policy template for the script. Not checked ✱, Not Compliant ✖ , or Compliant ✓.

Checked On

The date and time the script was last checked.

Fixed On

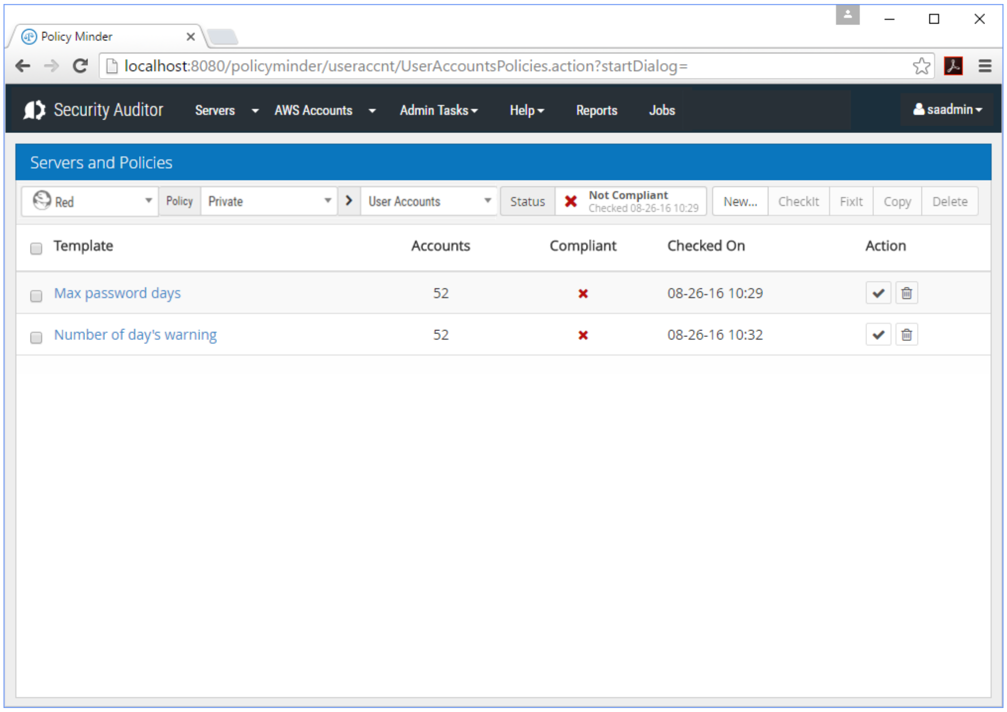
The date and time the script was fixed.

Action

If there is a change on the server, the Set as Policy button ✓ appears under the Actions column. Click ✓ **Set as Policy** to set your policy to match the server.

Servers and Policies - User Accounts

Use this screen to configure and manage initialized User Account Policy Templates.



Not Compliant
Checked 08-26-16 10:29

□	Template	Accounts	Compliant	Checked On	Action
□	Max password days	52	✗	08-26-16 10:29	✓ 🗑
□	Number of day's warning	52	✗	08-26-16 10:32	✓ 🗑

How to get there

In the Manage Servers screen, choose U for a server.

What it Does

The User Account page of the Servers and Policies screen displays an overview of the status of User Account policy templates.

Status

Displays the status of the Policies and when they were last checked.

New

Use this button to add a new policy Template. See Add a New User Accounts Policy Template.

CheckIt

Use this button to run CheckIt, which performs a compliance check for the selected attribute(s).

FixIt

Use this button to run FixIt, which changes the value on the server to match that of Security Auditor.

Copy

Use this button to copy the selected Template(s), in order to copy to a different server.

Delete

Use this button to delete the selected Template(s).

Field Descriptions

Template

The user account policy template name.

Accounts

The number of user accounts in the policy.

Compliant

The status of the template. Not checked ✱, Not Compliant ✖ , or Compliant ✔.

Checked On

Lists the date and time this template was most recently checked.

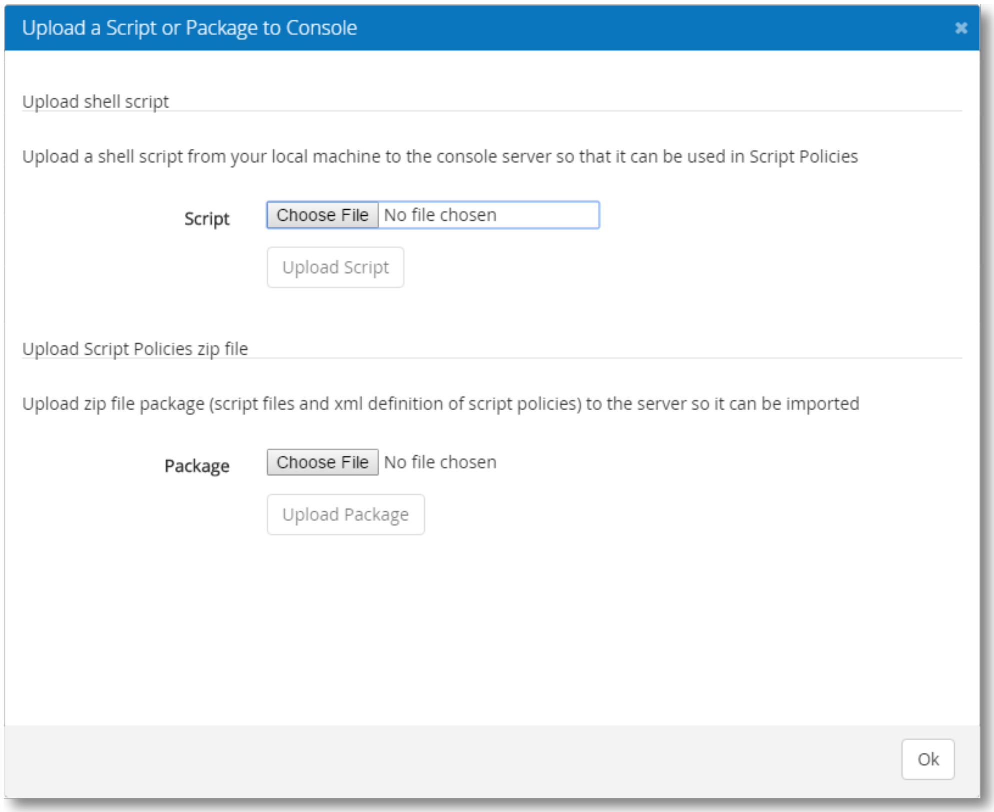
Action

Click ✓ to run CheckIt on the policy.

Click 🗑 to delete the policy from Security Auditor.

Upload a Script or Package to Console

This screen allows you to upload a shell script or script policies zip file.



Upload a Script or Package to Console

Upload shell script

Upload a shell script from your local machine to the console server so that it can be used in Script Policies

Script: No file chosen

Upload Script Policies zip file

Upload zip file package (script files and xml definition of script policies) to the server so it can be imported

Package: No file chosen

How to get there

Choose **Admin Tasks** > **Scripts** > **Upload**.

Upload shell script

Upload a shell script from your local machine to the console server so that it can be used in Script Policies

Script; Choose File • Upload Script

Choose a script file to upload to Security Auditor.

Upload Script Policies zip file

Upload zip file package (script files and xml definition of script policies) to the server so it can be imported

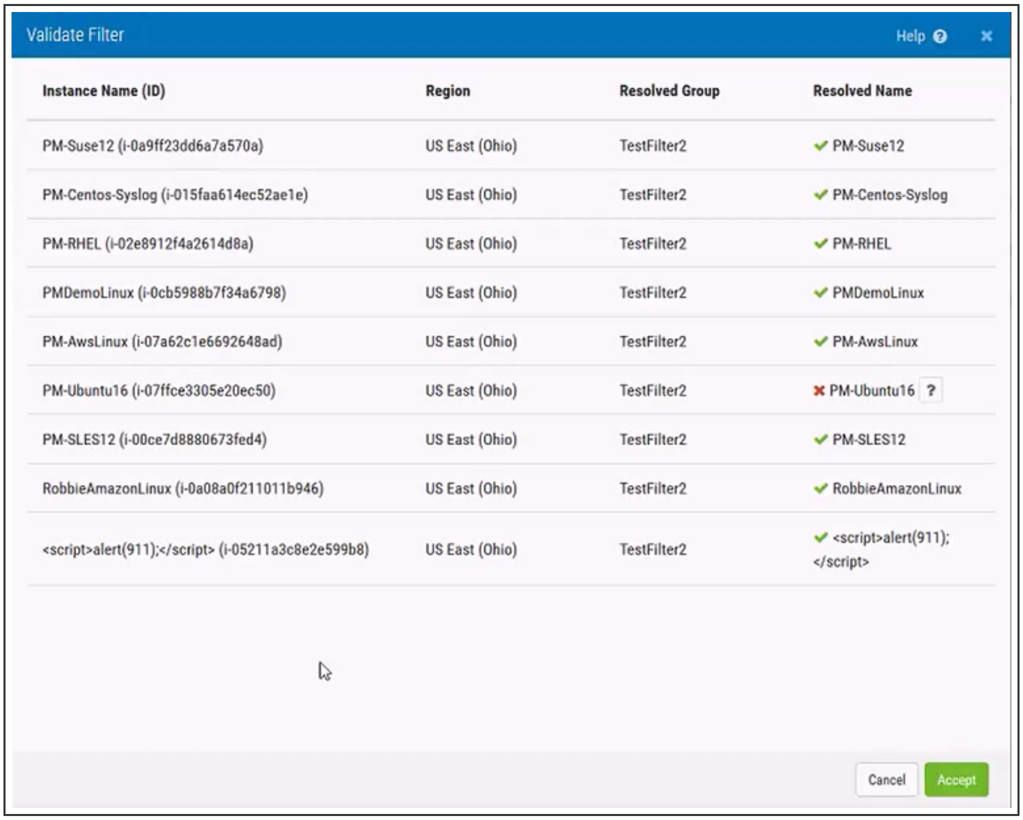
Package; Choose File • Upload Package

Choose a package file to upload to Security Auditor.

Ok

Click **Ok** to dismiss the screen.

Validate Filter screen



Instance Name (ID)	Region	Resolved Group	Resolved Name
PM-Suse12 (i-0a9ff23dd6a7a570a)	US East (Ohio)	TestFilter2	✓ PM-Suse12
PM-Centos-Syslog (i-015faa614ec52ae1e)	US East (Ohio)	TestFilter2	✓ PM-Centos-Syslog
PM-RHEL (i-02e8912f4a2614d8a)	US East (Ohio)	TestFilter2	✓ PM-RHEL
PMDemoLinux (i-0cb5988b7f34a6798)	US East (Ohio)	TestFilter2	✓ PMDemoLinux
PM-AwsLinux (i-07a62c1e6692648ad)	US East (Ohio)	TestFilter2	✓ PM-AwsLinux
PM-Ubuntu16 (i-07ffce3305e20ec50)	US East (Ohio)	TestFilter2	✗ PM-Ubuntu16 ?
PM-SLES12 (i-00ce7d8880673fed4)	US East (Ohio)	TestFilter2	✓ PM-SLES12
RobbieAmazonLinux (i-0a08a0f211011b946)	US East (Ohio)	TestFilter2	✓ RobbieAmazonLinux
<script>alert(911);</script> (i-05211a3c8e2e599b8)	US East (Ohio)	TestFilter2	✓ <script>alert(911);</script>

How to Get There

In the Manage Filters screen, click ✓ **Validate Filter** or ✓ **View Filter** for a Filter.

What it Does

This screen allows you to see the server instances yielded by the Filter settings you have configured for any given Filter.

Column Descriptions

Instance Name

The name of the AWS sever instance.

Region

The Region assigned to the AWS server instance.

Resolved Group

The Group the server belongs to in Security Auditor.

Resolved Name

A ✓ next to the Resolved Name indicates the server has been added.

An ✖ next to the Resolved Name indicates the server instance already exists and will not be added.

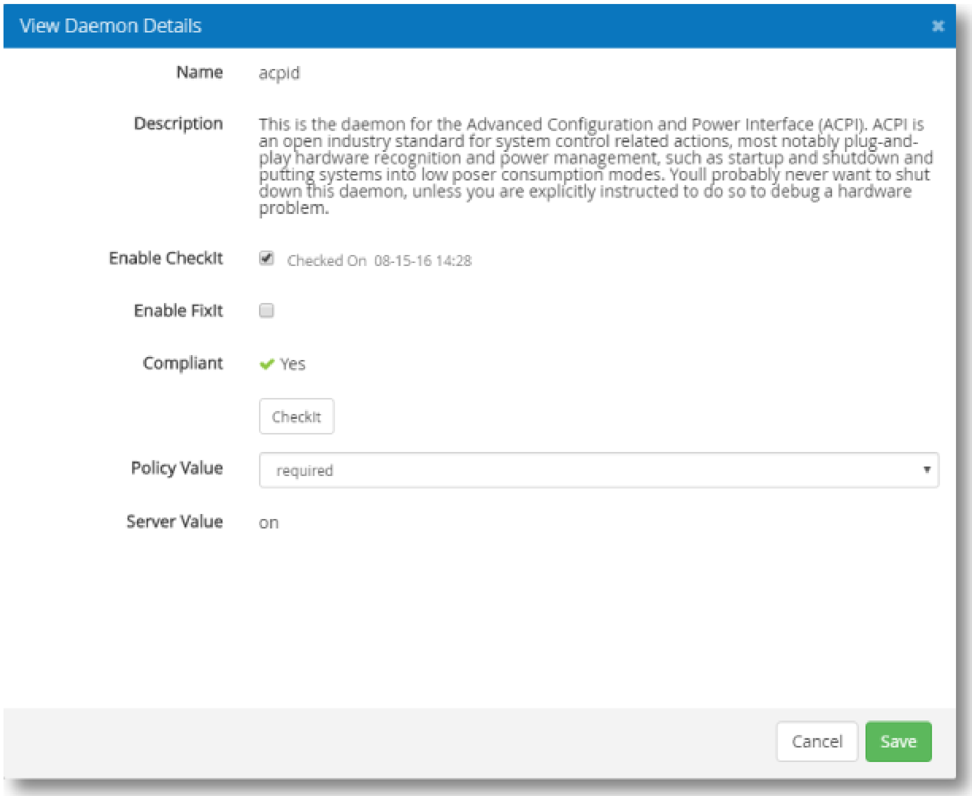
Cancel • Accept

Click **Cancel** to dismiss the screen without making changes. Click **Accept** to validate the Filter and begin automatic polling.

> **NOTE:** Automatic polling can be enabled and disabled on the Preferences screen.

View Daemon Details screen

This screen displays Daemon Policy information and allows you to edit the Policy for a Daemon.



Name: acpid

Description: This is the daemon for the Advanced Configuration and Power Interface (ACPI). ACPI is an open industry standard for system control related actions, most notably plug-and-play hardware recognition and power management, such as startup and shutdown and putting systems into low poser consumption modes. Youll probably never want to shut down this daemon, unless you are explicitly instructed to do so to debug a hardware problem.

Enable CheckIt: ☑ Checked On 08-15-16 14:28

Enable FixIt: □

Compliant: ✓ Yes

Policy Value: required ▾

Server Value: on

How to get there

1. On the menu at the top of the screen choose **Manage Servers**.
2. Choose D for the server you want details about.
3. Choose the daemon you want details about.

Field Descriptions

Name

The selected Daemon's name.

Description

The selected Daemon's description.

Enable CheckIt

Check this box to allow Security Auditor to check this value on the daemon to determine its status.

Enable FixIt

Check this box to allow Security Auditor to fix this value on the daemon (i.e. change it to match the template value).

Compliant

Indicates whether the selected Daemon is compliant.

CheckIt

Choose **CheckIt** to run the CheckIt process on this Daemon in order to check its compliance status.

Policy Value

This drop-down menu allows you to indicate whether the policy value is allowed, required, or prohibited.

- **Allowed:** Choose this option to indicate the server is compliant regardless of whether the Daemon is on or off.
- **Required:** Choose this option to indicate the Daemon must be on in order to be compliant.
- **Prohibited:** Choose this option to indicate the Daemon must be off in order to be compliant.

Server Value

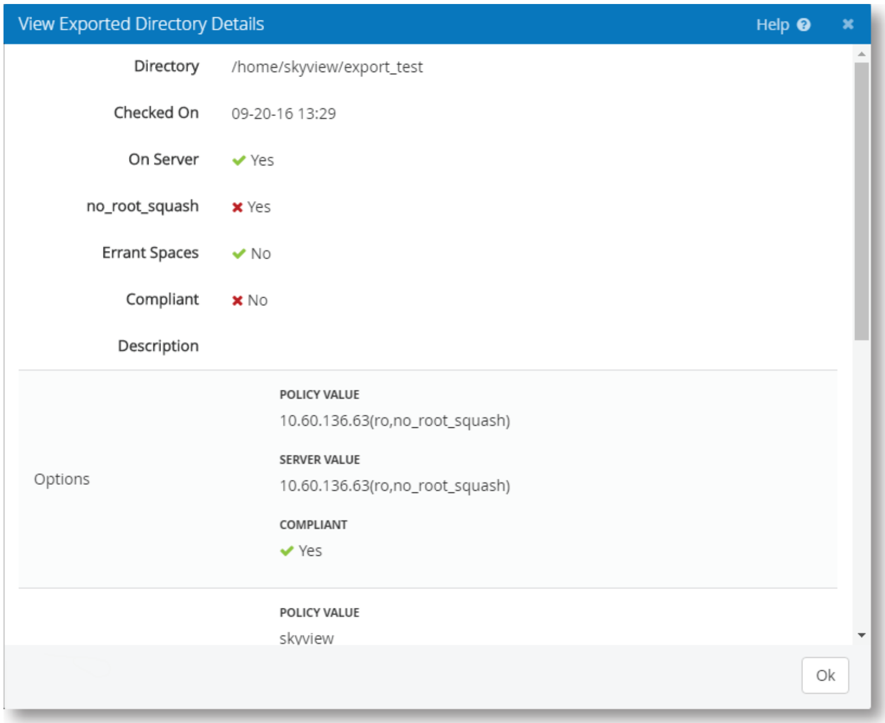
This indicates what the value of the server is.

Cancel • Save

Click **Cancel** to dismiss this screen. Click **Save** to save your changes and dismiss the screen.

View Exported Directory Details screen

Use the View Exported Directory Details screen to access additional information about the Exported Directory.



Directory	/home/skyview/export_test
Checked On	09-20-16 13:29
On Server	✓ Yes
no_root_squash	✗ Yes
Errant Spaces	✓ No
Compliant	✗ No
Description	
Options	POLICY VALUE 10.60.136.63(ro,no_root_squash) SERVER VALUE 10.60.136.63(ro,no_root_squash) COMPLIANT ✓ Yes
	POLICY VALUE skyview

How to get there

Choose **Admin Tasks** > **Scripts** > **Export Package**.

Field Descriptions

Directory

The path of the Exported Directory.

Checked On

The date and time CheckIt was last run on the Exported Directory.

On Server

The server of the Exported Directory.

no_root_squash

Indicates whether no_root_squash is set for the directory.

Errant Spaces

Indicates whether there is an errant space between the export host and the first parenthesis around options.

Compliance

Indicates the compliance status of the directory.

Description

This is the comment after your exported directory entry in the /etc/exports file.

For example:

```
/user/export 10.60.136.63(ro,no_root_squash) #comment here
```

Options • Owner • Group • Permissions

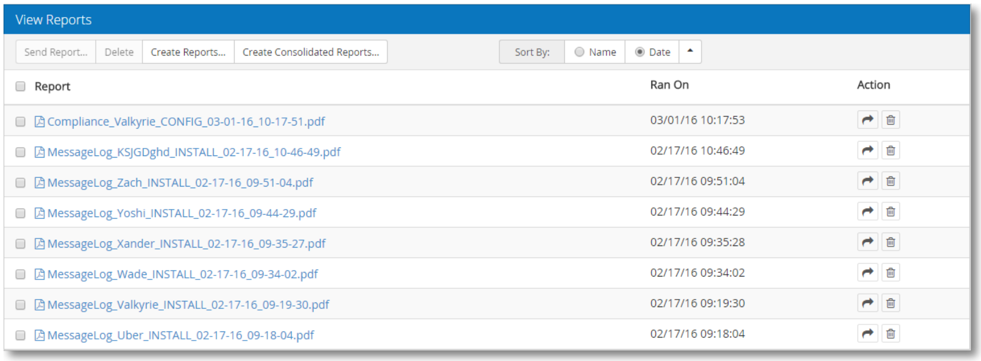
These fields list the Exported Directory's Options, Owner, Group, and Permissions settings, including the policy value, the server value, and whether or not the Exported Directory is compliant.

Ok

Click **Ok** to dismiss the View Exported Directories screen.

View Reports screen

Use this screen to view and manage reports.



□ Report	Ran On	Action
□ Compliance_Valkyrie_CONFIG_03-01-16_10-17-51.pdf	03/01/16 10:17:53	↷ 🗑
□ MessageLog_KSJGDghd_INSTALL_02-17-16_10-46-49.pdf	02/17/16 10:46:49	↷ 🗑
□ MessageLog_Zach_INSTALL_02-17-16_09-51-04.pdf	02/17/16 09:51:04	↷ 🗑
□ MessageLog_Yoshi_INSTALL_02-17-16_09-44-29.pdf	02/17/16 09:44:29	↷ 🗑
□ MessageLog_Xander_INSTALL_02-17-16_09-35-27.pdf	02/17/16 09:35:28	↷ 🗑
□ MessageLog_Wade_INSTALL_02-17-16_09-34-02.pdf	02/17/16 09:34:02	↷ 🗑
□ MessageLog_Valkyrie_INSTALL_02-17-16_09-19-30.pdf	02/17/16 09:19:30	↷ 🗑
□ MessageLog_Uber_INSTALL_02-17-16_09-18-04.pdf	02/17/16 09:18:04	↷ 🗑

How to get there

Choose **Servers** > **Reports** > **View Reports**.

Options

Send Report

Select one or more reports and click this button to send the report as an email attachment.

Delete

Select one or more reports and click this button to delete the report(s).

Create Reports

Click **Create Reports** to open the Create Reports screen where you can create a new report.

Create Consolidated Reports

Click **Create Consolidated Reports** to open the Create Consolidated Reports screen where you can create a consolidated report.

Sort By: Name • Date • ▾ or ▴

Choose Name to sort by the report's name and Date to sort by the report's creation date. Click **Sort** ▾ to change the sort order from ascending to descending or vice versa.

Field Descriptions

Report

Lists each report by filename.

Ran On

Lists the date and time the report was created.

Action

Select **Send Report in email** ↪ to send the report as an email attachment. Select **Delete** 🗑 to remove the report from Security Auditor.

Appendix: Configuring Security Auditor for SSL Mode

These instructions show you how to configure Security Auditor to run in secure sockets layer (SSL) mode. Additional information is available on the Apache Tomcat® website.

If you wish to use trusted certificate authority (CA) certificates, go to a CA website for information on generating the correct keys for a Tomcat server.

> **WARNING:** If you upgrade or update Security Auditor while it is running in SSL Mode, the existing "server.xml" file will be renamed to include a timestamp ("server.timestamp.xml") and a new standard "server.xml" will be installed. As such, you will need to re-apply the changes to the "server.xml" to make Security Auditor run in SSL Mode again.

Generating a Self-Signed Certificate

If you use a self-signed certificate, modern browsers will warn you that the connection is not secure. Users of the web server will need to follow their browser's prompts to allow the use of a self-signed certificate.

You must first generate or obtain a .keystore file. Make sure to note the password you enter, as you'll need this later.

1. From a command shell, set your working directory to a location where you would like to create a .keystore file.
2. The JAVA_HOME environment variable must be set to the location of a valid JVM. Then, issue one of the following commands from a command prompt:
   - For Windows: **"%JAVA_HOME%\bin\keytool" -keysize 2048 -genkey -validity 365 -alias ptsaweb -keyalg RSA -keystore ptsaweb.keystore**
   - For AIX/Linux: **$JAVA_HOME/bin/keytool -keysize 2048 -genkey -validity 365 -alias ptsaweb -keyalg RSA -keystore ptsaweb.keystore**
3. After creating a password, you'll be prompted for additional information.
   - When prompted for First Name and Last Name, enter the web server's computer name.
   - Provide other prompt answers per your environment.

   The resulting **ptsaweb.keystore** file is located in your working directory.

Enabling the Certificate

1. Stop the Security Auditor web server. See Stopping the Security Auditor web server.
2. Copy the **ptsaweb.keystore** file into the installation directory for the correct system below:

Environment	Location
Windows	C:\Program Files(x86)\Powertech\SecurityAuditor\tomcat\conf\
AIX/Linux	.../Powertech/SecurityAuditor/tomcat/conf/

3. Open and edit the server.xml file as follows. This file's location depends on the directory where the Security Auditor server is installed (see step 2).

> **NOTE:** This <!-- is a comment --> and this < is not a comment /> in the xml.

a. The initially shipped "Connector" definition looks like this:

```
<Connector port="8080" protocol="HTTP/1.1"
       connectionTimeout="20000"
       redirectPort="8443" />
```

Comment the above code out.

b. Uncomment the shipped connector definition and modify it with your password from above:

```
<Connector
          port="8443"

protocol="org.apache.coyote.http11.Http11NioProtocol"
          SSLEnabled="true"
          connectionTimeout="20000"
          scheme="https"
          secure="true"
          keystoreFile="conf/ptsaweb.keystore"
          keystorePass="yourpassword"
          sslProtocol="TLS"
          sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"
/>
```

Additionally, you can specify a "ciphers" parameter with a list of specific ciphers appropriate for your environment:

Example:

ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA"

c. There should also be an active connector definition for protocol=”AJP/1.3” like this:

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443"
/>
```

4. Save your changes to **server.xml**.
5. Start the Security Auditor Server to complete the configuration process:
    - On Windows, to start both the database and Tomcat go to **Start > Powertech Security Auditor > Start Security Auditor**.
    - On AIX or Linux, navigate to the directory where the console was installed and run the startpm.sh script.

After You Are Done

The links created in your Start menu during the install will be broken. To correct...

1. Change your browser links to use https (instead of http) and the correct port (8443).
2. The browser link should look like this: `https://`*`yourserver`*`:8443/securityauditor`, where *`yourserver`* is the name or IP address of your Security Auditor server.

Policy Values

When adding a Script Policy, values can be ranges of values for Integers or Dates, or regular expressions for Strings.

Booleans

For booleans, the values can be:

- `true` or `false`
- `yes` or `no`

Integer

Integer values can be a single value, a set of values, a range or a set of ranges and values

- A set of acceptable values are separated by the character ';' like **1;7;11**
- A range of acceptable values are separated by a ':' like **1:20**
- A set of ranges and values are separated by both ';' and ':' like **1:20;25;30:35**

Dates

The date format in Security Auditor must match the format used on the server.

> **EXAMPLE:**
> If the date value on the server is `05/31/2020`, the Policy format must be *`mm/dd/yyyy`*.

String

Summary of regular-expression constructs.

Construct	Matches
Characters	
x	The character x
\\	The backslash character
\\0*n*	The character with octal value 0*n* (0 <= *n* <= 7)
\\0*nn*	The character with octal value 0*nn* (0 <= *n* <= 7)
\\0*mnn*	The character with octal value 0*mnn* (0 <= *m* <= 3, 0 <= *n* <= 7)
\\x*hh*	The character with hexadecimal value 0x*hh*

Construct	Matches
Characters	
`\uhhhh`	The character with hexadecimal value `0xhhhh`
`\t`	The tab character (`'\u0009'`)
`\n`	The newline (line feed) character (`'\u000A'`)
`\r`	The carriage-return character (`'\u000D'`)
`\f`	The form-feed character (`'\u000C'`)
`\a`	The alert (bell) character (`'\u0007'`)
`\e`	The escape character (`'\u001B'`)
`\cx`	The control character corresponding to `x`

Character classes	
`[abc]`	`a`, `b`, or `c` (simple class)
`[^abc]`	Any character except `a`, `b`, or `c` (negation)
`[a-zA-Z]`	`a` through `z` or `A` through `Z`, inclusive (range)
`[a-d[m-p]]`	`a` through `d`, or `m` through `p`: `[a-dm-p]` (union)
`[a-z&&[def]]`	`d`, `e`, or `f` (intersection)
`[a-z&&[^bc]]`	`a` through `z`, except for `b` and `c`: `[ad-z]` (subtraction)
`[a-z&&[^m-p]]`	`a` through `z`, and not `m` through `p`: `[a-lq-z]` (subtraction)

Predefined character classes	
`.`	Any character (may or may not match line terminators)
`\d`	A digit: `[0-9]`
`\D`	A non-digit: `[^0-9]`
`\s`	A whitespace character: `[ \t\n\x0B\f\r]`
`\S`	A non-whitespace character: `[^\s]`
`\w`	A word character: `[a-zA-Z_0-9]`

Predefined character classes	
\W	A non-word character: [^\w]

POSIX character classes (US-ASCII only)	
\p{Lower}	A lower-case alphabetic character: [a-z]
\p{Upper}	An upper-case alphabetic character: [A-Z]
\p{ASCII}	All ASCII: [\x00-\x7F]
\p{Alpha}	An alphabetic character: [\p{Lower}\p{Upper}]
\p{Digit}	A decimal digit: [0-9]
\p{Alnum}	An alphanumeric character: [\p{Alpha}\p{Digit}]
\p{Punct}	Punctuation: One of !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
\p{Graph}	A visible character: [\p{Alnum}\p{Punct}]
\p{Print}	A printable character: [\p{Graph}\x20]
\p{Blank}	A space or a tab: [\t]
\p{Cntrl}	A control character: [\x00-\x1F\x7F]
\p{XDigit}	A hexadecimal digit: [0-9a-fA-F]
\p{Space}	A whitespace character: [\t\n\x0B\f\r]

java.lang.Character classes (simple java character type)	
\p{javaLowerCase}	Equivalent to java.lang.Character.isLowerCase()
\p{javaUpperCase}	Equivalent to java.lang.Character.isUpperCase()
\p{javaWhitespace}	Equivalent to java.lang.Character.isWhitespace()
\p{javaMirrored}	Equivalent to java.lang.Character.isMirrored()

Classes for Unicode blocks and categories	
\p{InGreek}	A character in the Greek block (simple block)
\p{Lu}	An uppercase letter (simple category)

Classes for Unicode blocks and categories	
`\p{Sc}`	A currency symbol
`\P{InGreek}`	Any character except one in the Greek block (negation)
`[\p{L}&&[^\p{Lu}]]`	Any letter except an uppercase letter (subtraction)

Boundary matchers	
`^`	The beginning of a line
`$`	The end of a line
`\b`	A word boundary
`\B`	A non-word boundary
`\A`	The beginning of the input
`\G`	The end of the previous match
`\Z`	The end of the input but for the final terminator, if any
`\z`	The end of the input

Greedy quantifiers	
`X?`	*X*, once or not at all
`X*`	*X*, zero or more times
`X+`	*X*, one or more times
`X{n}`	*X*, exactly *n* times
`X{n,}`	*X*, at least *n* times
`X{n,m}`	*X*, at least *n* but not more than *m* times

Reluctant quantifiers	
`X??`	*X*, once or not at all
`X*?`	*X*, zero or more times
`X+?`	*X*, one or more times

Reluctant quantifiers	
`X{n}?`	*X*, exactly *n* times
`X{n,}?`	*X*, at least *n* times
`X{n,m}?`	*X*, at least *n* but not more than *m* times

Possessive quantifiers	
`X?+`	*X*, once or not at all
`X*+`	*X*, zero or more times
`X++`	*X*, one or more times
`X{n}+`	*X*, exactly *n* times
`X{n,}+`	*X*, at least *n* times
`X{n,m}+`	*X*, at least *n* but not more than *m* times

Logical operators	
`XY`	*X* followed by *Y*
`X|Y`	Either *X* or *Y*
`(X)`	X, as a capturing group

Back references	
`\n`	Whatever the *n* th capturing group matched

Quotation	
`\`	Nothing, but quotes the following character
`\Q`	Nothing, but quotes all characters until `\E`
`\E`	Nothing, but ends quoting started by `\Q`

Special constructs (non-capturing)	
`(?:X)`	*X*, as a non-capturing group
`(?idmsux-idmsux)`	Nothing, but turns match flags idmsux on - off
`(?idmsux-idmsux:X)`	*X*, as a non-capturing group with the given flags idmsux on - off
(?=*X*)	*X*, via zero-width positive lookahead
(?!*X*)	X, via zero-width negative lookahead
(?<=*X*)	X, via zero-width positive lookbehind
(?<!*X*)	X, via zero-width negative lookbehind
(?>*X*)	X, as an independent, non-capturing group

Backslashes, escapes, and quoting

The backslash character ('\') serves to introduce escaped constructs, as defined in the table above, as well as to quote characters that otherwise would be interpreted as unescaped constructs. Thus the expression \\ matches a single backslash and \{ matches a left brace.

It is an error to use a backslash prior to any alphabetic character that does not denote an escaped construct; these are reserved for future extensions to the regular-expression language. A backslash may be used prior to a non-alphabetic character regardless of whether that character is part of an unescaped construct.

Backslashes within string literals in Java source code are interpreted as required by the Java Language Specification as either Unicode escapes or other character escapes. It is therefore necessary to double backslashes in string literals that represent regular expressions to protect them from interpretation by the Java bytecode compiler. The string literal "\b", for example, matches a single backspace character when interpreted as a regular expression, while "\\b" matches a word boundary. The string literal "\(hello\)" is illegal and leads to a compile-time error; in order to match the string (hello) the string literal "\\(hello\\)" must be used.

Character Classes

Character classes may appear within other character classes, and may be composed by the union operator (implicit) and the intersection operator (&&). The union operator denotes a class that contains every character that is in at least one of its operand classes. The intersection operator denotes a class that contains every character that is in both of its operand classes.

The precedence of character-class operators is as follows, from highest to lowest:

1	Literal escape	`\x`

2	Grouping	`[...]`
3	Range	`a-z`
4	Union	`[a-e][i-u]`
5	Intersection	`[a-z&&[aeiou]]`

Note that a different set of metacharacters are in effect inside a character class than outside a character class. For instance, the regular expression . loses its special meaning inside a character class, while the expression - becomes a range forming metacharacter.