ScienceLogic

Skylar Compliance

Version 6.0 Preview, release 2026

Table of Contents

Getting Started with Skylar Compliance **1**

What's New in Version 6.0 2

More Getting Started Information 2

The Skylar Compliance User Interface 2

Editing Views 3

My Account 3

Tasks Pane 4

Working with Skylar Compliance 4

Installing Skylar Compliance **6**

Before You Begin 7

Firewall Requirements 7

Traffic from Clients to Skylar ComplianceSkylar Compliance 7

Traffic from Skylar Compliance to Network Devices 8

Other Traffic Originating from Skylar Compliance 8

Encryption 8

Browser requirements 9

Skylar Compliance Virtual Appliances 9

Amazon Web Services 9

VMware vSphere 6.7 10

Hyper-V 11

Azure 12

Prerequisites 12

Transfer VHDs 12

Deploying a VHD 13

OpenShift 14

Virtual Machine YAML 14

Apache CloudStack 16

IP Address Setup 17

Alternative Method for Setting the IP Address 18

Connecting to Skylar Compliance for the First Time 19

Connecting to Skylar Compliance After a Reboot 23

Prerequisites for Converting Skylar Compliance to Oracle Linux 8 or 9 24
Migration Paths for CentOS Virtual Machines to Oracle Linux 8 or 9 24
CentOS 8 Virtual Machines 24
Converting a Skylar Compliance Hardware Appliance to a Hardware Appliance Running OL8 or OL9 25
Converting a Skylar Compliance Virtual Appliance to a Virtual Appliance Running OL8 or OL9 25
Converting a Skylar Compliance Virtual Appliance to a Hardware Appliance on OL8 or OL9 25
Skylar Compliance Appliance Migration 25
Before you Begin the Migration 26
Migration Paths 26
Partial Migration 26
Full Migration 27
Migration with Agents 28
Updating a Skylar Compliance Appliance 28
Force Check for Upgrade 28
Frequently Asked Questions 29
Known Issues 29
Status **30**
Viewing System Status 31
Reports **33**
Adding a Report 35
Editing a Report 36
Generating a Report 37
Cloning a Report 38
Adding a Report Schedule 39
Editing a Report Schedule 40
Deleting a Report or Report Schedule 40
Viewing Old User Interface Reports 41
Logs **43**
Event Log 44
Syslogs 45
Schedule **46**

Scheduled Tasks ... 47
Postponing Tasks ... 47
Pausing Tasks ... 48
Device List and Discovery ... **49**
Adding Devices to Skylar Compliance ... 50
Adding a New Device Manually ... 50
Importing Multiple Devices Using a CSV File ... 54
Device Discovery ... 55
Discovery Setup ... 55
Discovered Devices ... 56
Ignored Devices ... 58
Device Types ... 58
Automatic Import ... 58
Running a Manual Backup ... 59
Scheduling an Automatic Backup ... 59
Exporting the Device List ... 59
Editing an Existing Device ... 59
Editing Multiple Devices ... 59
Troubleshooting Domain-related Errors ... 61
Deleting an Existing Device ... 61
Device Monitoring ... 61
Enabling Monitoring ... 62
Displaying Monitoring Information ... 62
Viewing the List of Configurations for a Device ... 62
Comparing Device Configurations ... 64
Configuration Baselines ... 67
Backup File Operations ... 68
Backup Failures ... 68
Restoring to an Existing Device ... 68
Restoring to a New Device ... 69
Cloning ... 69
Templates ... **70**

Templates ... 71
Creating and Editing Templates ... 71
Pushing Templates ... 72
Device Control ... **74**
Controlling a Device ... 75
Scheduled Actions ... 76
Lua Functions ... 78
Creating a Lua Function Action ... 78
Error Handling for Lua Functions ... 80
Example: Device Rejected a Command ... 80
Example: Session Failure (Timeout, Connection Error) ... 80
Lua Applets ... 81
Using Parameters ... 81
Software ... **82**
Software ... 83
Uploading and Editing Firmware Images ... 83
Pushing Firmware ... 83
Credential Sets ... **85**
Credential Sets ... 86
Using Credential Sets ... 86
Integrating Skylar Compliance and CyberArk ... 87
Asset Fields ... **90**
Asset Fields ... 91
Labels ... **93**
Using Labels ... 94
Adding a Label from the Device Details Tab ... 94
Adding a Label from the Labels Page ... 95
Global Search ... **97**
Global Search ... 98
Device Policies (Policy Library and Rules Library) ... **100**
Device Policies and Rules ... 101
The Policies Tab ... 101

Creating a Device Policy 101
Editing a Device Policy 102
The Policy Library Tab 103
Viewing a Library Policy 104
Creating an Instance of a Library Policy 105
Editing an Instance 108
Instance Name and Comments 108
Rules from the Library Policy 109
Cloning an Instance 111
Disabling Rules 112
Cloning a Library Policy 112
Policy Library Updates 113
Reviewing Updates Before You Install Them 115
Turning Off Policy Library Updates 115
How Updates Change Your Instances 116
Packaged Rules in the Rule Library 117
Exporting and Importing Instances 117
The Rule Library Tab 118
Creating a New Rule 118
Remediation 122
Regular Expressions 123
Lua Functions 123
Skylar Compliance Built-in Functions 124
Examples 125
Show Version (Cisco) 125
Show Interface (Cisco) 125
IP Spoofing (ScreenOS) 126
IP Spoofing (Palo Alto) 126
Password Policies and Variable Definitions 128
Password Policies 129
Variable Definitions 130
System Settings 132

The Network Tab 133
Interfaces 133
IP Configuration 134
Network Access 134
Network Address Translation (NAT) 134
Additional IPv4 and/or IPv6 Static Routes 135
Bandwidth Management 135
The Appliance Tab 135
Platform 136
Branding 137
Software Updates 137
Disabling Automatic Updates 138
Manual Updates 138
Offline Updates 138
Date / Time 139
OS Updates 139
The Archive Tab 140
Taking an Archive 140
Restoring from an Archive 141
Workstation DB Archives 142
The Logs / Alerts Tab 142
Logs 143
Compliance Retention Policies 144
Alerts 144
The SNMP Tab 144
The Security Tab 145
Protocol Versions 146
TLS Cipher Options 146
Services 146
HTTPS Certificate 146
Session 147
Admin Allowed Networks 147

Allowed SSH Ciphers 148
Additional SSH Settings 148
Request Settings 148
SSH 148
Known Hosts 148
Key Management 149
Credential Providers 149
Trusted CA Certificates 150
The High Availability (HA) Tab 151
HA Requirements 152
Creating a Cluster 152
The Device Tab 153
Global Devices 154
Plugins 155
Advanced Settings 159
Domains **161**
Skylar Compliance Domains 162
How Domains Work 162
Rules That Govern Domains 162
Domain Permissions 165
Domain Permission Rules 165
Managing Domains 167
Administrator Roles 170
Adding a New Domain User 171
Editing Devices 174
Agents **175**
Agent Firewall Requirements 177
Agent Installation 177
Initial Setup 177
Enabling FIPS 140-3 Mode 179
Adding an Agent to Skylar Compliance 179
Changing the Master IP Address 181

Remote Operations Using Agents ... 182
Managing Agents ... 183
Updating the Operating System for an Agent ... 183
VMware Agent ... 184
Installing and Configuring the VMware Agent ... 184
Amazon Web Services Agent ... 185
Installing and Configuring the AWS Agent ... 185
Azure Agent ... 186
Installing the Azure Agent ... 186
HyperV Agent ... 187
Installing and Configuring the HyperV Agent ... 188
RPM Agent ... 188
RPM Agent Limitations ... 188
Installing and Updating the RPM Agent ... 189
Configuring the RPM Agent ... 189
Optional RPM Agent Configurations ... 190
Device Back-Connection ... 190
Initial Master SSH Connection Port ... 191
Back Connection NAT ... 191
TFTP and FTP Servers ... 191
Disable Strict SSH Host Key Configuration ... 191
System Temporary Directory ... 191
Troubleshooting the RPM Agent ... 192
Docker Agent ... 192
Installing and Configuring the Docker Agent ... 192
Acquiring the API Token ... 192
Configuring rpagent ... 193
Host Networking ... 194
Additional Run Options ... 194
Troubleshooting the Docker Agent ... 195
Configuring CrowdStrike Using Agents ... 195
Users and User Roles ... 196

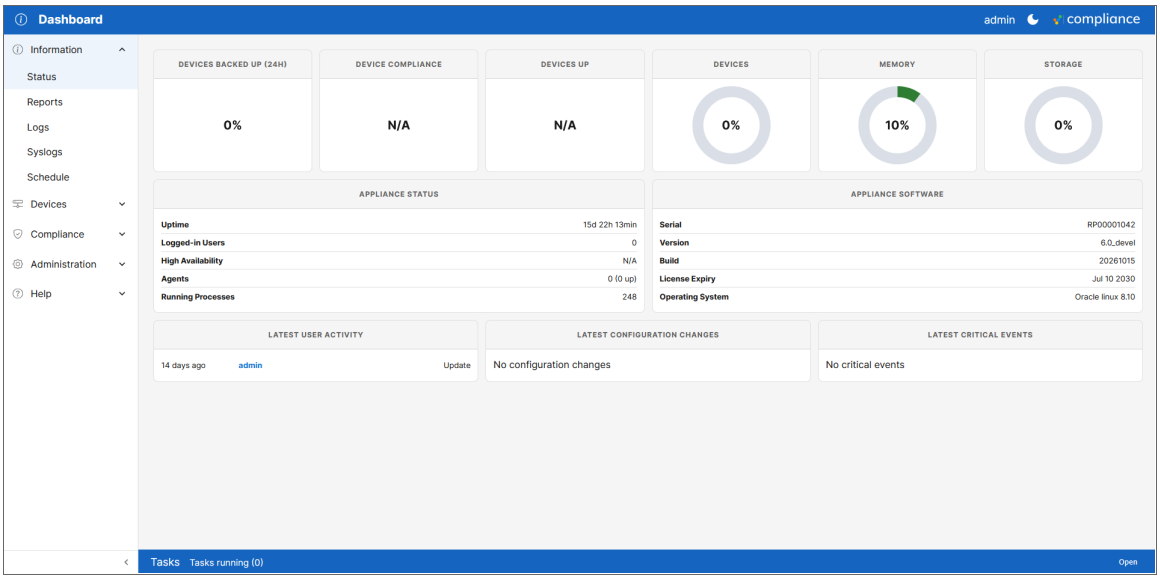
Listing Logged-in Users ... 197
Adding a New User ... 197
Broadcasting to Users ... 199
Editing an Existing User ... 199
Deleting a User ... 200
Password Reset ... 200
Password Recovery Configuration ... 200
Recovery Procedure ... 201
Custom User Roles ... 202
Auth Servers ... 205
RADIUS Authentication ... 206
SAML Authentication ... 206
Adding a SAML Group ... 207
Editing an Existing SAML Group ... 208
Editing an Existing SAML User ... 209
LDAP Authentication ... 210
Storage ... 212
File Servers ... 213
Auto Export ... 213
Data Export ... 214
Data Usage ... 214
Getting Help ... 215
Error Messages ... 216
Errors During Backup Operations ... 216
Other Messages ... 217
Using the System Shell ... 218
Factory Reset ... 219
Skylar Compliance Plugins ... 220
Frequently Asked Questions ... 221
Contacting ScienceLogic Support ... 221

Chapter 1

Getting Started with Skylar Compliance

Overview

Skylar Compliance (formerly Restorepoint) is a Disaster Recovery and Secure Configuration Management appliance for network devices such as routers, switches, proxies, and firewalls. Skylar Compliance can automatically retrieve your network device configurations, detect changes and compliance violations, and report these automatically to network administrators.



Skylar Compliance offers you the ability to add, configure, monitor, and control devices. You can perform these actions through a simple user interface that gives you access to all your devices, stored backups,

user configurations, and activity logs. You can also set the backup frequency for each device individually or as a group.

When your device configurations are stored on Skylar Compliance, you can restore network devices when needed. Your devices are secure as all backups, device configurations, and passwords are encrypted and cannot be accessed by an unauthorized user.

What's New in Version 6.0

The 6.0 release of Skylar Compliance contains the following main features:

- Added the ***Rule Library*** (Compliance > Device Policies > Rule Library tab), a central repository for creating and managing reusable compliance rules that exist independently of any single policy. Administrators can now link these library rules into multiple policies as live instances, ensuring that updates to a base rule automatically propagate across all referencing policies while still allowing for specific field overrides at the policy level. For more details, see *Device Policies (Policy Library and Rules Library)*.
- Added a set of quality-of-life enhancements to the Skylar Compliance user interface, including clearer error messages, improved rule testing tools, and streamlined policy navigation. These updates also feature enhanced editors and metadata filters designed to reduce day-to-day friction for advanced users.
- Added support for the deployment of packaged compliance rules and policies. This enhancement allows pre-built compliance checks, such as those based on configurations or firmware versions, to be pushed to customer appliances in a manner similar to plugin updates, reducing the time and technical expertise required for users to establish compliance monitoring.
- The v3 API replaces the v2 API. Any request to a v2 API is transparently rewritten to v3, but requests can error if the endpoint has received breaking changes.
- This manual was completely reorganized for this release. Chapters were set up based on their location in the Skylar Compliance user interface.

For more information, see the *Skylar Compliance Release Notes*.

More Getting Started Information

To install Skylar Compliance, see *Installing Skylar Compliance*.

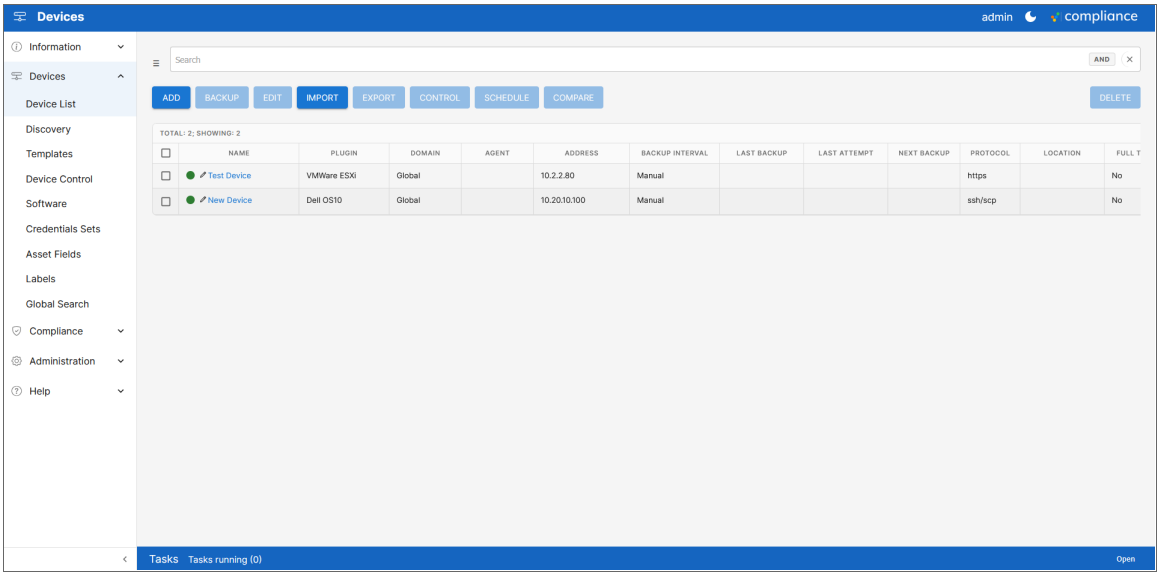
You can find a list of devices that are currently supported by Skylar Compliance in the **Plugin Guide** (Help > Plugin Guide) on the Skylar Compliance website and on the *Plugins* page.

Skylar Compliance also has its own RESTful API that allows you to trigger all of Skylar Compliance's operations automatically. For more information, see the *Skylar Compliance API Documentation*.

The Skylar Compliance User Interface

The Skylar Compliance user interface pages share some common features. These features include:

- A menu bar at the top of the page, for navigating between the different functions
- The username of the logged in user at the top right-hand side of the screen



You can change column widths by clicking and dragging the heading separators. You can change the sorting criterion by clicking on a column heading. You can also perform a full text search by typing in the ***Search*** field.

Editing Views

In addition to the built-in views, every data table in Skylar Compliance can have multiple customized views. You can access these by clicking on the menu icon (☰) at the top left of a table. You can use this icon to reorder columns by clicking the up/down arrows and selecting the checkbox to show/hide columns.

You can define a name and save column orders, widths, and display settings using the **[Save]** button. You can delete saved views using the **[Delete]** button.

> **NOTE:** Views stored in your browser's local storage are only available on the browser and workstation where they were set. If you clear your browser storage, you will clear any saved views.

My Account

You can hover over the username on the top of the user interface and two options appear. A **Logout** option that features a clock that shows how many minutes until a user is automatically logged out, and the **My Account** option that allows you to edit the following user settings:

- **Full Name**
- **Email**

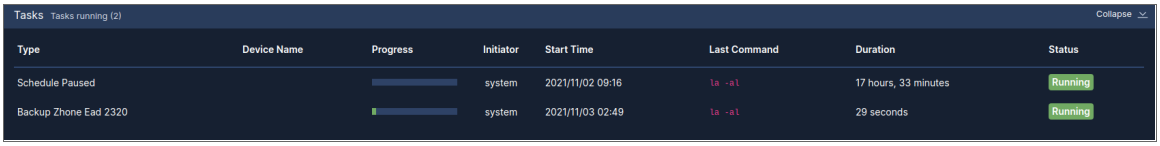
- **New Password**
- **Encryption Password**
- **Recovery Question**
- **Recovery Answer**

> **NOTE:** To change a password, you need to specify the **Old Password**.

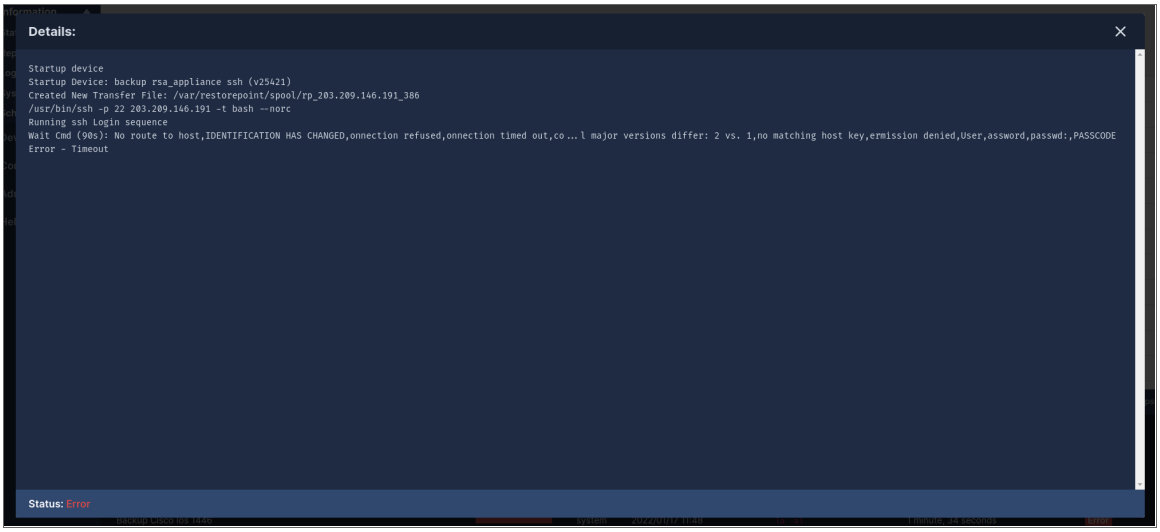
For more information on the **My Account** options, see *Adding a new user*.

Tasks Pane

The **Tasks** pane displays a list of activities that are currently running. This list is displayed on every page while tasks are in progress:



You can click on the magnifying glass icon to show the **Progress Log**, which displays real-time information about the running task:



Working with Skylar Compliance

You can use the Skylar Compliance user interface to add, configure, monitor, and control your devices. This section covers how you can get started with Skylar Compliance.

NOTE: If you are an administrator, you can find more information about installing Skylar Compliance and connecting to Skylar Compliance for the first time in *Installing Skylar Compliance*.

- To manually add the devices you want to configure and monitor with Skylar Compliance, see *Adding Devices to Skylar Compliance*.
- The Skylar Compliance device discovery engine uses a variety of methods to discover hosts on your network that can be imported to the main device list. You can also be notified by email of new devices that are installed on your network. For more information, see *Device Discovery*.
- You can run manual backups or schedule automatic device backups. For more information, see *Running Backups*.
- To create configuration compliance policies and assign the policies to devices, see *Device Policies*.
- For additional features and processes, see the chapter in this manual that has the tab name and chapter name as the page in Skylar Compliance, such as *System Settings* for the **System Settings** page on the **[Administration]** tab in the left-hand navigation.

Chapter 2

Installing Skylar Compliance

Overview

Skylar Compliance is available as a hardware appliance or a VMware virtual appliance. This section describes how to perform the initial configuration of your Skylar Compliance appliance and configure it to communicate with other devices on your network.

This chapter covers the following topics:

Before You Begin 7

Firewall Requirements 7

Encryption 8

Browser requirements 9

Skylar Compliance Virtual Appliances 9

IP Address Setup 17

Connecting to Skylar Compliance for the First Time 19

Before You Begin

Before you install your Skylar Compliance appliance, ensure you meet the following requirements:

- For hardware installations, 1U of rack space available to install the appliance, with a standard 240V power socket
- For hardware installations, allocate a port on your Ethernet switch for the appliance
- The appliance has an allocated static IP address
- You have configured your firewall to allow traffic between the appliance, and the network devices and servers that Skylar Compliance will control
- For virtual deployments, verify that you are running VMware ESX vSphere 6.7U2 or later
- For virtual deployments, verify your ESX host has 4 GB RAM available and the datastore where the virtual machine will be deployed has 256 GB available
- Configure your firewall to allow outbound traffic from Skylar Compliance to the Internet. If you have a firewall between any of your devices and Skylar Compliance, you may need to open additional ports. For more information, see device-specific details in the **Plugin Guide** (Help > Plugin Guide) on the Skylar Compliance website.
- Configure your mail server to allow Skylar Compliance to relay email

Firewall Requirements

This section lists the ports used to by clients connecting to Skylar Compliance and the ports used by Skylar Compliance to connect to network devices and other servers.

NOTE: Your firewall policy might need to be modified for Skylar Compliance to function correctly.

Traffic from Clients to Skylar ComplianceSkylar Compliance

The following table lists traffic from Skylar Compliance to network devices:

Port	Purpose
443/tcp	Skylar Compliance user interface
22/tcp	Skylar Compliance shell access
161/udp	(optional) SNMP monitoring

Traffic from Skylar Compliance to Network Devices

Skylar Compliance connects to network devices in a variety of ways, depending on the vendor. Sometimes, devices use back-connections to transfer their configuration to Skylar Compliance. See the device-specific details in the **Plugin Guide** (Help > Plugin Guide).

Other Traffic Originating from Skylar Compliance

The following table lists outbound firewall requirements:

Port	Purpose
443/tcp	Download updates from Skylar Compliance update servers and HA database sync
53/udp	Lookup to DNS servers
25/tcp	Send notification emails using SMTP
123/udp	Time synchronization with NTP servers (optional)
22/tcp	Initiate remote support requests (*jmp1.restorepoint.com* and *jmp2.restorepoint.com*), or communicate with an agent's manager. (optional)

Encryption

All sensitive data stored in Skylar Compliance, including device configurations, is protected by encryption. Skylar Compliance encrypts data when it is written to a disk and decrypts it as it is read. Cleartext data is only held in volatile memory. Therefore, the data disappears when the appliance is shut down or rebooted, which renders data theft impossible without a valid encryption key. It is important to note that Skylar Compliance is encrypted-at-rest for the secure storage of backups and databases. Any use of third-party tools to perform a scan of Skylar Compliance backups or databases may result in a error message.

Skylar Compliance has two operational states:

- **Locked State**. When the appliance is powered up and no encryption password is entered by an administrator. In this state, Skylar Compliance cannot read its own database and therefore cannot perform any operations. An administrator must log in and provide the encryption password to unlock the database.
- **Normal State**. Once an administrator provides the encryption password at login, all system functions are enabled. Subsequent administrator logins will not require an encryption password until the appliance is powered down or rebooted.

> **CAUTION:** The entire Skylar Compliance database is encrypted. Therefore, it is vital that administrators remember both their normal and encryption passwords. Administrators must also keep their emailed password-recovery tokens safe. For more information, see *Connecting to Skylar Compliance After a Reboot*and *Password Reset*.

Browser requirements

Skylar Compliance requires a modern browser with JavaScript enabled. Skylar Compliance has been tested with the following:

- Chrome (v35)
- Firefox (v25)
- Internet Explorer 10
- Safari (v6)
- Opera (v12.10)

Skylar Compliance Virtual Appliances

You can install Skylar Compliance with the following virtual appliances:

- *Amazon Web Services*
- *Hyper-V*
- *Azure*
- *OpenShift*
- *Apache CloudStack*

Amazon Web Services

If you want to deploy Skylar Compliance on your AWS instance, go to the Request Amazon AMI page and complete the Amazon AMI form. When making the request, you will supply your Amazon EC2 account ID and the Region to which you want to deploy your Skylar Compliance instance to your Support contact. Then Support will share the AMI to your Amazon EC2 account.

To launch a Skylar Compliance instance:

1. Log in to the EC2 Console and click **[Launch Instance]**.
2. Give your instance a name and tag your instance, if needed.
3. On the ***My AMIs*** tab, select the *Share with me* radio button, and then select the Skylar Compliance AMI by searching "Restorepoint" in the ***Search*** field.
4. Select an **Instance Type**. You can change the sizing at a later stage. Click **[Next]** after you make your selection. Note the following guidelines:
    - For evaluation purposes, t3.micro is usually sufficient
    - For production purposes, t3.medium or t3.large are recommended

5. **In the Key pair (login)** pane, create an SSH key pair or select an existing one from the ***Key pair name*** drop-down field. After you select the SSH key pair, you can configure the instance details on the next screen.

> **WARNING:** Skylar Compliance uses DHCP for private IP address assignment. Ensure that the VPC/Subnet are configured to auto-assign the instance private IP address or enter the instance IP address in the **Advanced Details** section. ***You will not be able to change the instance IP address after you create it.***

6. On the **Network settings** pane in the **Firewall (security groups)** section, select the *Select existing security group* radio button or select the *Create security group* radio button. Ensure that you can communicate to the instance via HTTPS (port 443) and SSH (port 22). For more information, see the *Firewall Requirements* section in the Skylar Compliance User Guide.
7. In the **Configure storage** pane, two volumes are listed: *Root volume* and *EBS volume*. Both are 40GB by default. If you want to change the size of your appliance, ScienceLogic recommends you change the second volume labeled ***EBS volume***.
8. Review your settings and if they are correct, click **[Launch instance]**. The instance will launch. The first boot will take longer to launch than usual due to the initial volume encryption.
9. When the launch is complete, connect to the Skylar Compliance instance via HTTPS. Log in with ***admin*** as the username and ***admin*** as the default password and encryption password to decrypt the appliance. After the first login, log in again with ***admin*** as the username and password, and the initial setup screen will appear. Be sure to change your password during the initial setup.

VMware vSphere 6.7

You can download the Skylar Compliance Virtual Appliance as a .ZIP file from the URL provided by the Skylar Compliance team. The following steps refer to VMware ESX vSphere 6.7U2 or later:

1. Expand the Skylar Compliance .ZIP file in a suitable location on your PC.
2. Launch the vSphere HTML Client.
3. Right-click on the desired destination in the left-hand column and choose **Deploy OVF Template**, select **Deploy from file** and browse to the OVA file inside the extracted folder.
4. Select the OVA file in the folder. Click **[Next]**.

> **NOTE:** If you cannot use an OVA to deploy, extract the OVA file and select all the extracted files. There should be a .mf file, an .ovf file, and 2 .vmdk files. Then, click **[Next]**.

5. Enter a name (or keep the default name) for the virtual machine and select the inventory location, then click **[Next]**.
6. Choose the host or cluster, then click **[Next]**.
7. Select which datastore should be used, then click **[Next]**.
8. Choose **Network Mapping**, then click **[Next]**.

9. Check the summary information, then click **[Finish]**.
10. The virtual machine will now deploy. After completion, click **[Close]** in the completion dialog box.

IMPORTANT: Skylar Compliance is encrypted-at-rest for the secure storage of backups and databases. Any use of third-party tools to perform a scan of Skylar Compliance backups or databases may result in an error message.

IMPORTANT: ScienceLogic provides this procedure as a courtesy and does not offer support for third-party systems. For more information, including troubleshooting procedures for a VMware vSphere system, see the VMware documentation at https://vmware.com.

Hyper-V

You can obtain the Skylar Compliance Virtual Appliance from Support by entering a service request in the customer portal. Choose the ***Customer Operations Request*** option and the download will be provided.

1. Expand the Skylar Compliance .Zip file to a file location on your system.
2. Launch the Hyper-V Manager and select your system.
3. From the **Actions** drop-down menu, select *New*, and then select *Virtual Machine*.
4. From the **New Virtual Machine Wizard**, select **[Next]** and complete the following:
   - Specify the Virtual Machine Name, then click **[Next]**.
   - Select *Generation 2* as the Virtual Machine generation type, and then click **[Next]**.
   - Assign memory for the Virtual Machine in the ***Startup memory*** field and then click **[Next]**. Configure networking on the next pane of the wizard. Then click **[Next]**.
   - Select ***Use an existing virtual hard disk*** and browse to the location where you expanded the .ZIP file. Select either *restorepoint-master-disk001.vhdx* or *restorepoint-agent-disk001.vhdx* depending on whether you are running a master or an agent as the Virtual Machine hard disk. Then click **[Next]**.
   - Review the specifications for the new Virtual Machine and click **[Finish]**.
5. Right-click on the new Virtual Machine and select ***Settings***.
6. Go to **Security** and change the template from *Microsoft Windows* to *Microsoft UEFI Certificate Authority*.
7. Go to **SCSI Controller** to select **[Add new hard drive]**. Select either *restorepoint-master-disk002.vhdx* or *restorepoint-agent-disk002.vhdx* depending on whether you are running a master or an agent hard drive.
8. Click **[Apply]** to complete the setup. Your Virtual Machine is now ready to be started.

IMPORTANT: ScienceLogic provides this procedure as a courtesy and does not offer support for third-party systems. For more information, including troubleshooting procedures and updates for a HyperV system, contact Microsoft Support at https://support.microsoft.com/

Azure

You can obtain the Skylar Compliance Azure Virtual Appliance from Support by requesting that the Virtual Hard Drives (VHDs) be shared.

Go to the ***Support*** menu and click on *License & AMI Request*. Next click the **[Request Azure VHD]** button. On the **Request Azure VHD** page, follow the prerequisite instructions below:

Prerequisites

To generate a destination SAS URL for transferring VHDs to your Azure Storage account, follow the steps below:

1. Go to the Azure Portal and log in. Navigate to the **Storage Center** page.
2. Locate your desired Storage Account or create a new one.
3. On the selected Storage Account blade, click on the ***Storage Browser*** drop-down menu and select *Container Blobs* to view the list of containers.
4. Locate your desired Container Blob or create a new one.
5. Click the ***Action*** menu, located on the right side of the container row, and select *Generate SAS*.
6. Next, select the *User Delegation Key* radio button, located in the **Signing method** section on the **Generate SAS** pane to ensure better security.

NOTE: The *User Delegation Key* option is the only supported option at this time. To generate the SAS URL , you must be assigned one of the following roles: Storage Blob Data Owner, Storage Blob Data Contributor, or Storage Blob Delegator role at the Storage Account level. If you are not assigned one of the listed roles, you will see a warning message that you do not have the correct permissions, and your generated URL will not work.

7. Then select *Read* and *Write* from the ***Permission*** drop-down menu.
8. Enter the start and end date and time of the token validity in the ***Start*** and ***Expiry*** fields. The token is only valid during this time frame.
9. Click **[Generate SAS Token URL]** and copy the Blob SAS URL. Keep the copied Blob SAS URL in a known location as you will need it in the next step.

Transfer VHDs

To transfer the VHDs you must complete the **Request Azure VHD** pane on the left side of the **Azure VHD Request** page in the Support Center.

1. Select *Skylar Compliance* from the ***Please Choose a Product*** drop-down menu.
2. Select a version number from the ***Product Type or Version*** drop-down menu.
3. Select the required checkboxes from the **Appliance Types** section. Select *appliance* from the ***Product Type or Version*** drop-down menu. Then select both the ***Appliance Data*** checkbox and the ***Appliance OS*** checkbox.
4. Locate the Blob SAS URL that you copied in the steps above and enter it into the ***Blob SAS URL*** field.
5. Click the **[Submit Azure VHD Request]** button.

ScienceLogic will transfer the necessary VHDs to your desired container. You should see the operating system VHD and the data VHD in your container.

NOTE: By clicking on the **[Submit Azure VHD Request]** button, you authorize ScienceLogic to utilize the provided destination SAS URL for transferring the necessary VHDs associated with the selected appliances (s) to your Azure Storage Account container.

Deploying a VHD

To deploy the Virtual Machine, you must create an image with both of the virtual hard drives. Ensure that you know which drive is the operating system and which drive is for data.

- The operating system disk must be a Linux disk type and generation.
- The data disk should be a disk type *None*.
- Both disks must have a minimum of 40GB and you should only change the data disk if you require additional data on Skylar Compliance.

To deploy the Virtual Machine:

1. Create your virtual machine from your operating system disk and configure it to allow the following inbound ports:
    - HTTPS 443
    - SSH 22
2. Add the data disk to the virtual machine. Ensure it is readable and writeable.
3. Customize the remaining settings as they pertain to your individual environment and requirements.
4. If you require agents, make sure to enable *Pingable* under the ***Network Settings*** after your deployment has finished.

IMPORTANT: ScienceLogic provides this procedure as a courtesy and does not offer support for third-party systems. For more information, including troubleshooting procedures and updates for an Azure system, contact Microsoft Support at https://support.microsoft.com/

OpenShift

To deploy Skylar Compliance with OpenShift:

1. Download the OS KVM image from the email from ScienceLogic.
2. Go to **Virtualization** > **Catalog**.
3. Select the project you are using.
4. Click **Add volume**.
5. Set the volume options:
   - ***Name***. Your choice
   - ***Source type***. Volume
   - ***Upload PVC image***. Upload the OS KVM image you downloaded
   - ***Disk size***. 40 GB
   - ***Preference***. linux
6. Click Save.
7. Navigate to **Virtualization** > **VirtualMachines**.
8. Click **[Create]**, then select *YAML* from the dropdown and use the YAML code in the following code block.
9. Click **[Create]**.

Virtual Machine YAML

Replace every placeholder before creating the VM:

`<VM_NAME>`: Name for the new VM (lowercase letters, numbers, hyphens)

`<NAMESPACE>`: Project the VM will be created in

`<OS_DISK_NAME>`: Bootable volume to boot from

`<OS_DISK_NAMESPACE>`: Project the bootable volume is in

`<STORAGE_CLASS>`: Storage class for both disks

`<DATA_DISK_SIZE>`: Size of the blank data disk, e.g. 40Gi

```
apiVersion: kubevirt.io/v1
kind: VirtualMachine
metadata:
  name: <VM_NAME>
  namespace: <NAMESPACE>
  labels:
    app: <VM_NAME>
```

```
spec:
  runStrategy: Always
  dataVolumeTemplates:
    - metadata:
        name: <VM_NAME>-rootdisk
      spec:
        sourceRef:
          kind: DataSource
          name: <OS_DISK_NAME>
          namespace: <OS_DISK_NAMESPACE>
        storage:
          storageClassName: <STORAGE_CLASS>
    - metadata:
        name: <VM_NAME>-datadisk
      spec:
        source:
          blank: {}
        storage:
          storageClassName: <STORAGE_CLASS>
          resources:
            requests:
              storage: <DATA_DISK_SIZE>
  template:
    metadata:
      labels:
        kubevirt.io/domain: <VM_NAME>
    spec:
      domain:
        firmware:
          bootloader:
            efi:
              secureBoot: false
        cpu:
          cores: 2
          sockets: 1
          threads: 1
        memory:
          guest: 4Gi
        devices:
          disks:
```

```
        - name: rootdisk
          bootOrder: 1
          disk:
            bus: virtio
        - name: datadisk
          disk:
            bus: virtio
      interfaces:
        - name: default
          masquerade: {}
      rng: {}
  networks:
    - name: default
      pod: {}
  terminationGracePeriodSeconds: 180
  volumes:
    - name: rootdisk
      dataVolume:
        name: <VM_NAME>-rootdisk
    - name: datadisk
      dataVolume:
        name: <VM_NAME>-datadisk
```

Apache CloudStack

You can download the Skylar Compliance KVM image as a .ZIP file from the URL provided by the Skylar Compliance team. The following steps refer to Apache CloudStack with KVM hosts:

1. Before you begin, confirm with your CloudStack administrator that the KVM hosts support UEFI Secure boot.
2. Expand the Skylar Compliance .ZIP file in a suitable location on your local machinee.
3. Log in to the CloudStack user interface.
4. Go to **Images** > **Templates** and select the option to register a template from a local file.
5. Browse to the QCOW2 file inside the extracted folder and select it.
6. Enter a name or keep the default name for the template.
7. Select **KVM** for Hypervisor and **QCOW2** for Format.
8. Select **virtio** for Root Disk Controller.
9. Select **Oracle Linux 9** for OS Type. If this entry is not available, select **Other Linux (64-bit)**.
10. Select **Intel/AMD64** for Arch. This field is not available in all versions of CloudStack.

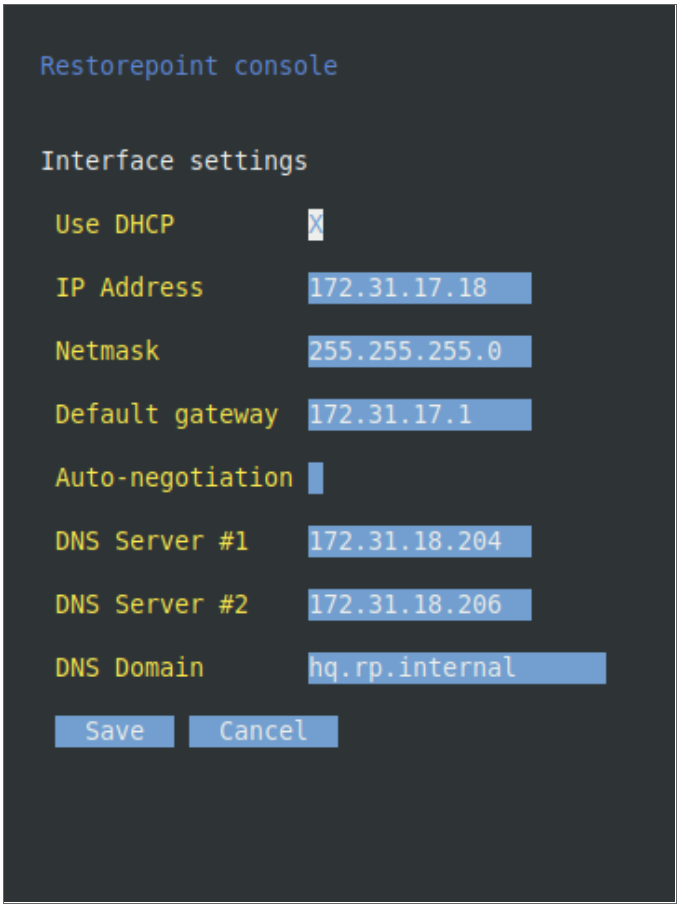
11. Enable HVM, then submit the form.
12. Wait until the template status is Ready.
13. Start the new instance wizard and select the template you registered.
14. Select a compute offering.
15. Add a data disk for backup data.
16. Enable Show advanced settings.
17. Select **UEFI** for Boot Type and **Secure** for Boot Mode.
18. Check the summary information, then launch the instance.

IP Address Setup

To set up Skylar Compliance, you must configure the network parameters, which include the static IP address you have allocated to the appliance, and the DNS and gateway settings for your network. Follow these steps:

1. Connect a monitor and keyboard to suitable ports on the rear panel of the appliance, or open the virtual machine console in the Virtual Infrastructure client.

2. At the login prompt, typed the default user name (*admin*) and password (*admin*) for the device and then choose option 1 on the console menu:



3. Type the IP address, Netmask, default gateway, and primary DNS server as prompted. The DNS server must be able to resolve public names (for example, support.restorepoint.com), otherwise the appliance cannot retrieve software updates.
4. Enter *y* to confirm the settings. If the settings are applied successfully, the console menu will be redisplayed. You can **exit** now.

You can disconnect your monitor and keyboard. To continue the initial setup, open a browser window on a network connected PC and enter the IP address you set for the appliance in the URL bar.

Alternative Method for Setting the IP Address

You can also connect to the Skylar Compliance appliance for initial setup over a network using the factory-configured default IP address/netmask (192.168.1.1/255.255.255.0), if these settings do not conflict with any devices already on your network. Use a browser to connect to `https://192.168.1.1` and set the IP address as shown above.

If these settings *are* in use on your network, you may connect the device directly to a PC using an Ethernet cross-over cable. Configure your PC to use an address in the 192.168.1.2 - 254 range, then use a browser to connect to `https://192.168.1.1`.

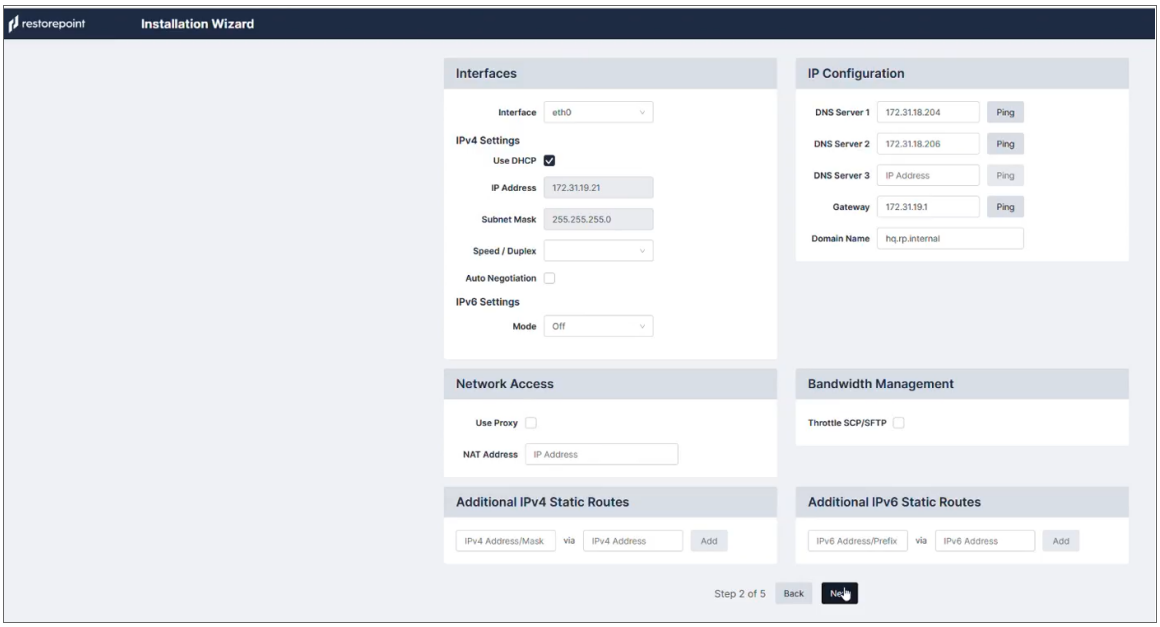
Connecting to Skylar Compliance for the First Time

After you set the IP address for Skylar Compliance, use a browser on a network-connected PC to connect to the IP address and complete the initial configuration.

IMPORTANT: Skylar Compliance initially uses a self-signed certificate. Because of this, your web browser will warn you of an invalid (untrusted) certificate. This is normal behavior because the appliance certificate is not signed by a Trusted Certificate Authority. The session will still be encrypted. Refer to your browser instructions on how to proceed and accept the unsigned certificate. A valid (signed) certificate can be uploaded to Skylar Compliance after the initial configuration is completed.

To connect to Skylar Compliance for the first time:

1. Log in with the default username (*admin*) and default password(*admin*). Be sure to change your password after the initial login.
2. Skylar Compliance displays the **End-User License Agreement**. Read the terms of the Agreement, then click **[Accept]** to signify that you accept the Agreement. You will not be able to use Skylar Compliance if you do not accept the Agreement.
3. The **Installation Wizard** page appears. You can use this page to configure your network settings.



4. Supply values in the following fields:

- ***Interface***. Select an interface from the drop down list.
- ***Use DHCP***. Select this checkbox if you want to use a DHCP server for your interface and other options will be disabled.
- ***Enable FIPS 140-3 Mode***. Select this checkbox only if your environment requires FIPS 140-3 compliance. When enabled, Skylar Compliance reconfigures the operating system and the application to use only FIPS-approved cryptography. This setting is permanent; you cannot disable it after installation, and you would need to reinstall the appliance to revert it. The appliance reboots automatically to complete activation. If you are installing offline, FIPS activates on your next manual reboot instead.

  Leave the checkbox cleared if you do not need FIPS.
- ***IP Address***. Type your Skylar Compliance IP address. Skylar Compliance and its agents can add IPv4 and IPv6 IP addresses. “Host” fields across Skylar Compliance can now accept an IPv4/IPv6 address or a hostname (excluding DNS servers (IP address-only).
- ***Subnet Mask***. Type your subnet mask associated with the IP address
- ***Speed/Duplex***. Select the link speed and duplex from the drop down list.
- ***DNS Server 1***. Type the DNS Server address for your network. Click **[Ping]** to check connectivity.
- ***DNS Server 2***. Type the second DNS Server address from your network. This field is optional. Click **[Ping]** to check connectivity.
- ***Gateway***. Type the default gateway for your network. Click **[Ping]** to check connectivity.
- ***Domain Name***. Type the default domain name.
- ***Use Proxy***. Select this checkbox if proxy is required for internet access.
- ***NAT Address***. Type the NAT address if connection is required by your firewall.
- ***Additonal Static Routes***. If the devices that you want to add to Skylar Compliance are located on different networks, you may need to define additional static routes. If required, type the network IP address and the destination gateway IP address and click **[Add]**.
- ***Throttle SCP/SFTP***. Select this checkbox to limit the amount of network bandwidth Skylar Compliance uses.

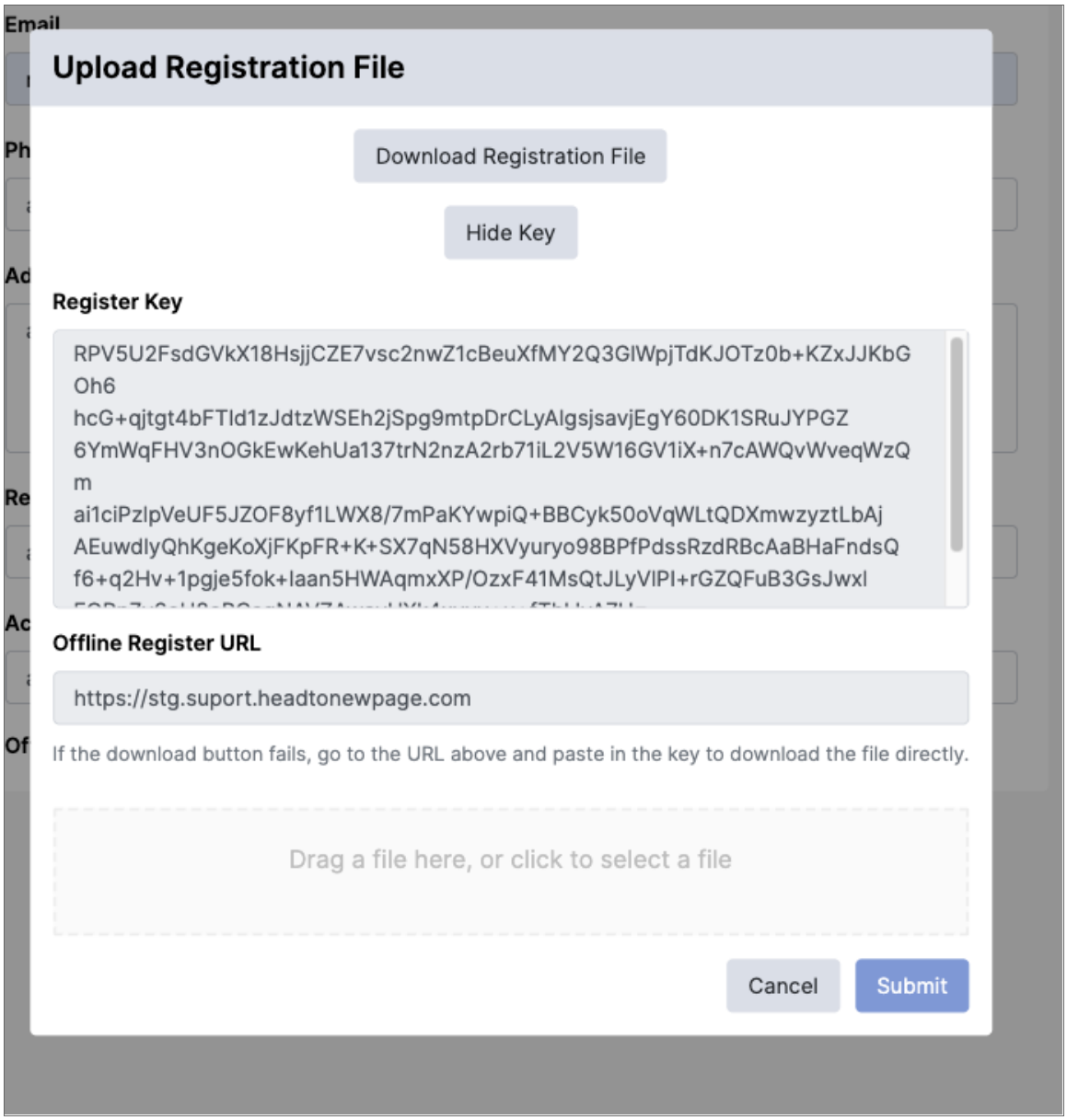
5. Click **[Next]** and the **Alerts** and **SMTP** page appears. You can use this page to configure credentials for system notifications. Supply values in the following fields:
   - ***Email errors to***. Type the email address you would like the error alerts to be delivered to.
   - ***Email from***. Type the email address you want the email to originate from.
   - ***Host***. Type the IP address of your mail server. Click **[Ping]** to check connectivity.
   - ***Port***. Click the arrows in the right of the field to navigate to the correct port number for your mail server. Click **[Test]** to test the connection.
   - ***Verify Certificate***. Check this box to check the SMTP server certificate against the certificates trusted by the appliance, including any chain marked *SMTP server* under **Trusted CA Certificates**. This option is always on when FIPS mode is enabled.
   - ***Username***. Type the username for your mail server.

- ***Domain Name***. Type the password for your mail server.
- ***From***. Type an email address to use in the "From" field for notifications.
- ***To***. Type a default email address to send email alerts to.

6. Click **[Next]** and the **Admin User** page appears. You can use this page to configure the account for an admin level user. Supply values in the following fields:
    - ***Username***. Type a Skylar Compliance username.
    - ***Email***. Type an email for the administrator user.
    - ***Password***. Type a password for the administrator user. Your password must be a minimum of 8 characters with mixed case, numbers, symbols, and cannot be a dictionary word. Your password must be different from your encryption password. Click **[Show]** to display the password.
    - ***Encryption Password***. Type an encryption password for the admin user. Encryption passwords are required for decryption after a restart. Click**[Show]** to display the password.
    - ***Recovery Question***. Type a recovery question to be used if the user forgets their password. A recovery token will be sent to you from ScienceLogic via email.
    - ***Recovery Answer***. Type the answer to the recovery question.
7. Click **[Next]** and the **Activation** page appears. You can use this page to configure contacts and other settings to activate Skylar Compliance. Supply values in the following fields:
    - ***Company Name***. Type the name of the company that is using the Skylar Compliance system.
    - ***Contact Name***. Type a name for a point of contact regarding the Skylar Compliance system.
    - ***Email***. Type an email for a point of contact regarding the Skylar Compliance system.
    - ***Phone***. Type a phone number for a point of contact regarding the Skylar Compliance system.
    - ***Address***. Type an address for a point of contact regarding the Skylar Compliance system.
    - ***Reseller***. Type the company name of the reseller, if applicable.
    - ***Activation Code***. Type the activation code you received from ScienceLogic if you are connected to the internet.
    - ***Offline?***. Select this checkbox if you are using Skylar Compliance offline.

> **NOTE:** If the **The appliance is not connected to the Internet** option is checked, the appliance will operate in offline mode and will not attempt to contact the update server. The **[Force Check]** button changes to **[Manual Upgrade]**, which you can click to download an update package to your workstation and manually upload it to Skylar Compliance. For more information, see Offline Installation/Upgrade.

8. Click **[Finish]**.
9. If you entered an activation code, you will be redirected to the Skylar Compliance login page once installation is complete.
10. If you selected the ***Offline?*** checkbox, the **Upload Registration File** pane appears.



11. If the browser has internet connectivity:
    - Click the **[Download Registration File]** button. Skylar Compliance provides a file to download with a filename similar to rpupdate_20250106154424.bin.
    - Navigate back to your Skylar Compliance system and drag the file to the **Upload Registration File** pane to upload it or click inside the pane to select the file.

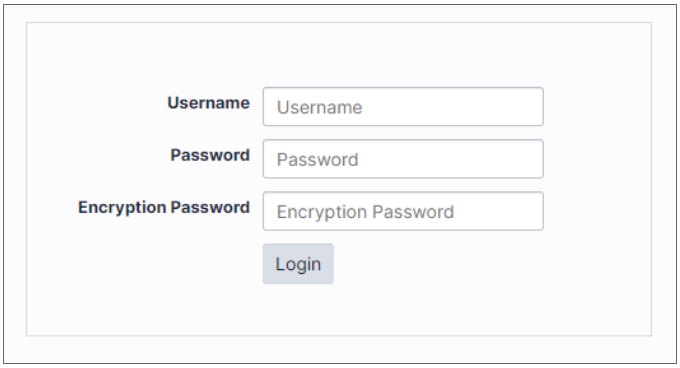
12. If the browser does not have internet connectivity:
    - Copy the ***Appliance Key*** provided in the pane and click the Skylar Compliance register link (https://support.restorepoint.com/register) provided in the middle of the pane.
    - On the **Skylar Compliance Register** page, paste the ***Appliance Key*** that you copied above and click ***Register***.
    - Skylar Compliance provides a file to download with a filename similar to rpupdate_20250106154424.bin. Click **[Download]**.
    - Navigate back to your Skylar Compliance system and drag the file to the **Upload Registration File** pane to upload it or click inside the pane to select the file.
13. Click **[Submit]** and you will be redirected to the Skylar Compliance login page once installation is complete.

IMPORTANT: The Skylar Compliance installation process time can vary and may take up to 30 minutes. ScienceLogic recommends that you do not click **[Submit]** more than once, but wait for Skylar Compliance to redirect you to the login page.

Connecting to Skylar Compliance After a Reboot

When Skylar Compliance is rebooted, it will start in a locked state. It is not able to perform any operations until the encryption password is entered, and only admin-level operators can log in to the appliance.

To enter the encryption password, use a browser to connect to the appliance and provide your administrator credentials and the encryption password:



The appliance will then transition to the normal operation mode, and subsequent administrator logins will not require an encryption password.

While some versions of Skylar Compliance currently run on CentOS Linux, updates and releases of CentOS Linux were discontinued, as follows:

- CentOS Linux 8 reached End of Life (EOL) on December 31, 2021
- CentOS Linux 7 reached EOL on June 30, 2024
- CentOS Linux 6 reached EOL on November 30, 2020

Skylar Compliance now uses OL8 and OL9 as the primary supported operating systems. This topic covers how to migrate from the CentOS Linux platform to the OL8 or OL9 operating system.

NOTE: Skylar Compliance releases are completely independent of Skylar One platform releases.

Prerequisites for Converting Skylar Compliance to Oracle Linux 8 or 9

- ***All appliance types***. Open a case with Support to request an upgrade, if you have not already done so.
- Ensure you are running the latest Skylar Compliance version 5.6 release. You cannot upgrade from a re lease earlier than 5.6. See *Migration Paths for CentOS Virtual Machines to Oracle Linux 8 or 9.*
- Take a snapshot or backup of your Skylar Compliance appliance in case a rollback is needed. For more information, see *System Archive*.
- ***Virtual machines only***. Acquire virtual machine(s) with an OL8 or OL9 operating system having similar or better specifications (CPU, memory, disk size) than the existing virtual machine for the primary Skylar Compliance appliance and all existing agents, if you are using agents.
- Ensure you have the encryption password, administrator password, and serial number (if this is a hardware appliance) of your existing appliance.

Migration Paths for CentOS Virtual Machines to Oracle Linux 8 or 9

Before you can convert your Skylar Compliance virtual appliance to OL8 or OL9, you must ensure it is updated to a version supported by the conversion process and you must open a case with a Skylar Compliance Support engineer so they can assist in the process. They will be able to help determine your operating system and your Skylar Compliance version.

CentOS 8 Virtual Machines

After you confirm your Skylar Compliance operating system is CentOS 6 or CentOS 8, and your Skylar Compliance version is 5.6, use the following procedure to update your operating system to Oracle Linux 8 or 9.

NOTE: If you are running Skylar Compliance version 5.4 or 5.5 on CentOS 6 or CentOS 8, contact Support for assistance with upgrading your version to 5.6 on Oracle Linux 8 or 9.

To update your Skylar Compliance system to version 5.6:

- Update from Restorepoint version 5.3.1 to Skylar Compliance version 5.4:
    - Ask the Restorepoint Support engineer to set the appliance to version 5.4 in the Skylar Compliance backend.
    - Update to your virtual appliance Skylar Compliance version 5.4.
- Update from Skylar Complianceversion 5.4 to Skylar Compliance version 5.6:
    - Ask the Skylar ComplianceSupport engineer to set the appliance to version 5.6.
    - Update your virtual appliance to Skylar Compliance version 5.6.

After your Skylar Compliance appliance is updated to Skylar Compliance version 5.6, you can proceed to update your appliance to OL8 or OL9. This process requires you to create a new appliance and then follow the migration steps.

Converting a Skylar Compliance Hardware Appliance to a Hardware Appliance Running OL8 or OL9

If you have a Skylar Compliance hardware appliance, you must contact Customer Operations to submit a service request with *ScienceLogic Support*. You must provide your hardware serial number so they can validate the hardware and provide a new appliance with OL8 or OL9 installed. When you have the new hardware appliance, you can update your Skylar Compliance appliance. See *Updating a Skylar Compliance Appliance* for more information.

Converting a Skylar Compliance Virtual Appliance to a Virtual Appliance Running OL8 or OL9

If you are using Skylar Compliance on a virtual machine running CentOS, you must contact Customer Operations to submit a service request with *ScienceLogic Support* to request an upgrade. They will provide you with a download link for the latest image for the platform you are using, for example, AMI for an AWS installation. See *Updating a Skylar Compliance Appliance* for more information.

Converting a Skylar Compliance Virtual Appliance to a Hardware Appliance on OL8 or OL9

If you want to move from using a Skylar Compliance virtual appliance to using a Skylar Compliance hardware appliance, you must contact Customer Operations to submit a service request with *ScienceLogic Support* to request the hardware appliance. Customer Operations will work with you and your Account Executive to procure a new appliance with OL8 or OL9 installed. After you receive the Skylar Compliance hardware appliance, you must perform a full migration of your virtual appliance data to the new hardware appliance. See *Full Migration* for more information.

Skylar Compliance Appliance Migration

This section covers how to migrate your data to a new hardware or virtual appliance.

Before you Begin the Migration

1. Provide the existing serial number to Customer Operations so they can generate a new activation code and share the new image or hardware appliance.
2. Configure the appliance IP address on your network and complete the online registration.
3. Using your new activation code, install and configure the new appliance. For more information, see *Installing Skylar Compliance*.
4. Make sure that both Skylar Compliance appliances are running the same software version. You can verify the software versions on the **System Status** page (System Status > Appliance Software).
5. The appliances normally update themselves by connecting to the Skylar Compliance update servers, but you can force an update using the **[Force Check]** button on the **[Appliance]** tab (Administration > System Settings > Appliance). The same page shows the current software version and build number.

Migration Paths

There are two migration paths:

1. *Partial Migration*. Migrates the device information, such as IP addresses, credentials, and so on. Most users choose partial migration, because it is simpler, and you can complete it within a few minutes.
2. *Full Migration*. Includes all of the device backups and restores the appliance SSH keys.

IMPORTANT: Only a full migration will restore the appliance SSH keys. This is an important consideration if you are using SSH Public Key Authentication (PKA), because devices will not allow the new appliance to log in until the new appliance SSH key is authorized. Devices that perform strict SSH checks may also prevent logins, even if using SSH password authentication.

Partial Migration

This migration moves over only your device settings. Device configuration files and Skylar Compliance settings are not migrated.

1. Log in to the existing Skylar Compliance appliance and click **Devices** in the left-side menu.
2. Select the checkbox next to the column title ***Name*** to select all devices (or select which devices to export individually).
3. Click **[Export]** to generate a CSV file with the device data.
4. Log in to the new appliance, and then click **Devices** in the left-side menu.
5. Click **[Import]**. In the dialog that appears, choose the CSV file you exported in step 3. This file is typically in your the **Downloads** folder. All of the devices should appear in the list.

Full Migration

The full migration uses the Skylar Compliance Archive feature, which exports all of the system configuration to an external server.

1. Configure archiving on the existing appliance. This should already be in place, as it is an essential disaster recovery function.
2. Go to the **Archive** page (Administration > System Setting > Archive).
3. Configure the file server to which Skylar Compliance uploads its archive and set up an automated disaster recovery Archive. Skylar Compliance supports FTP, SCP, SFTP, or Windows file servers for archiving.
4. Create a new archive on the server by clicking **[Archive Now]**. This operation may take a long time, depending on the amount of data stored on the appliance.
5. On the new appliance, import the archive from the server.
6. On the **Archive** page (Administration > System Settings > Archive), configure archiving in the same way as it was on the existing appliance (that is, IP address, protocol, path and credentials), and then click **[Restore Archive]**.
7. Skylar Compliance displays a list of archives available on the remote server in a drop-down list. Choose the most recent archive and click **[Restore]**.



During the process, you might be prompted for the password and encryption password of your existing appliance. Provide the details for the administrator account. Again, this may take a long time to complete; at the end of the process, all of the Skylar Compliance settings (except the IP address for the appliance) and all data stored on the old appliance will be restored on to the new one. For more information about archiving, see *System Archive*.

Migration with Agents

To perform migration when your environment has Agents:

1. Deploy new agents on a new virtual machine with the Oracle Linux 8 or 9 operating system and perform the Initial Master Setup in the agent.
2. Set the IP address of the new appliance for each agent.
3. Skylar Compliance supports agent deployment within an RPM. Additionally, Skylar Compliance also supports communication from agent to Skylar Compliance appliance over a port of your choosing. The default port 22 can be changed when setting up the agent.

NOTE: If you need HTTPS enabled on the new appliance, you must create a new certificate. For more information, see *HTTPS Certificates*.

Updating a Skylar Compliance Appliance

The following steps are for virtual deployments only.

The Skylar Compliance appliance checks the update server for software updates every 24 hours and installs them automatically. Installation updates only occur when there are no other tasks running, so there is no service downtime.

Force Check for Upgrade

If you have either of the following options selected (Administration > System Settings > Appliance), you must do a **Force Check** to update your appliance. Automatic updates will not occur for:

- Disable Automatic Version Upgrades
- Disable Automatic Minor Updates

For more information about Force Check, see *Software Updates*.

NOTE: If the ***The appliance is not connected to the Internet*** option is checked, the appliance will operate in offline mode and will not attempt to contact the update server. The **[Force Check]** button changes to **[Manual Upgrade]**, which you can click to download an update package to your workstation and manually upload it to Skylar Compliance. For more information, see *Manual Updates*. You can also see the Knowledge Base article Offline Installation/Upgrade.

Frequently Asked Questions

What downtime can I expect?

- Usually, each update only takes a few minutes and will only proceed when no other tasks are running. If you have a busy system, you might need to pause the scheduler to process the upgrade.
- Depending on the number of devices you have, creating or restoring an archive can take a long time. Skylar Compliance recommends that you allocate at least 12 hours for the migration after the pre-requisites have been gathered.

Will my license be migrated?

- No. Support will generate a new activation code license based on the serial number of the new appliance. You can copy and paste the new code during the deployment of the new appliances.

Will my device certificates be migrated?

- Yes. Device certificates will be migrated if restoring an archive on to the new appliance. (Full Migration)

I have agents on CentOS. How do I migrate them?

- See *Migration with Agents* above.

Will SSH keys for agents be migrated?

- Yes. SSH keys for agent will be migrated during an archive and restore.

Will SSH host keys of the appliance be migrated?

- Yes. SSH host keys will be migrated during an archive and restore.

I have High Availability enabled in CentOS. How do I migrate the secondary appliance?

- To migrate a High Availability appliance set up, you must first set up the new HA cluster and then follow the full migration or partial migration steps above on the primary appliance.
- Ensure the secondary appliance is running the identical Skylar Compliance and operating system version as the primary.
- Complete the set up on the secondary appliance. For more information, see the *High Availability* section in the Skylar Compliance guide.

Will my existing users be migrated?

- Yes. All existing local and LDAP users (and LDAP settings) will be migrated if restoring an archive onto the new appliance. (Full Migration)

Known Issues

- *Issues with Agents*. This topic encompasses a wide range of problems, but usually the cause is the agents have not been migrated to Oracle like the primary and there are conflicting ciphers, macs, and Kexs.
- *Domain not Found*. This error message can appear when viewing a device. Follow the steps in the article to resolve the issues.
- *Converting Last Alert Policy*. This is a common database issue that occurs if the customer uses the Generic Push device plugin.

If you run into any of these problems, contact a support engineer.

Chapter 3

Status

Overview

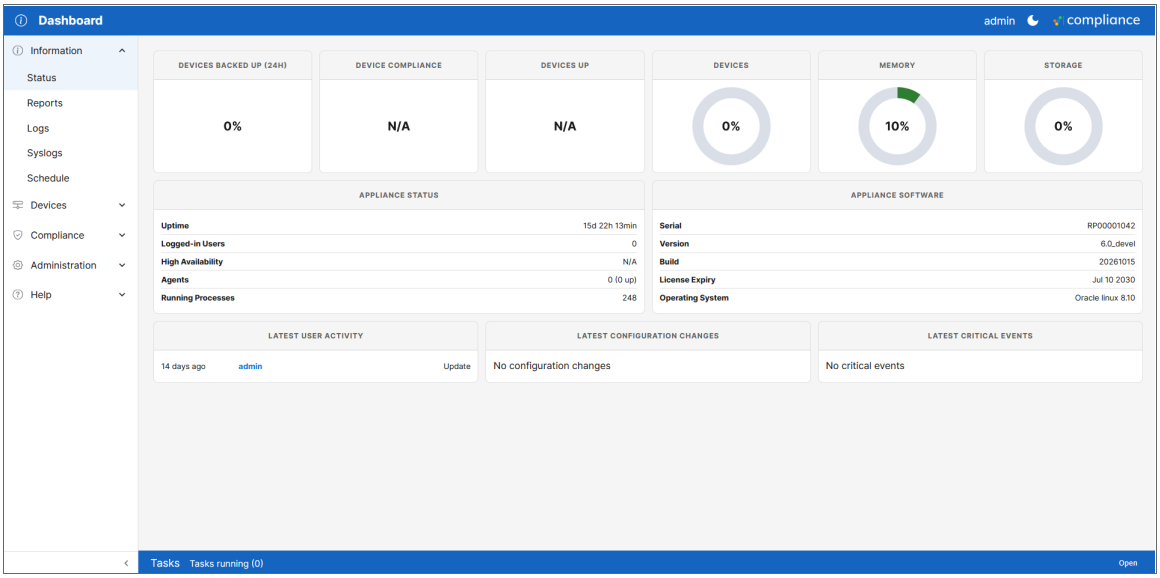
The **Status** page (Information > Status), also called the **Dashboard** page, displays an overview of the health of your Skylar Compliance system and displays the number of devices that are being backed up.

This chapter covers the following topics:

Viewing System Status *31*

Viewing System Status

The **Status** or **Dashboard** page is the default page when you first login to Skylar Compliance:



The following type of graphs can be displayed on the **Dashboard** page:

- ***Devices Backed Up (24h)***. Successful and failed scheduled backups in the last 24 hours. Additionally, mouseover mention devices not scheduled for backup.
- ***Device Compliance***. The number of compliant and non-compliant devices, and the number of devices with no policy assigned.
- ***Devices Up***. The number of devices that are currently being monitored and responding to Skylar Compliance. If you click on the graph, a moving average chart covering the past 24 hours is displayed.
- ***Devices***. The total number of devices configured on the appliance, and the maximum devices allowed on your current license.
- ***Memory***. The amount of RAM currently being used by the Skylar Compliance appliance and the total amount of RAM available.
- ***Storage***. The amount of disk space used and the total amount of disk space for the Skylar Compliance appliance

The following information is displayed in text panes on the **Dashboard** page:

- ***Appliance Status***. The uptime, number of logged in users, *High Availability* status (if enabled), *Agents* status (if enabled), and number of running tasks.
- ***Appliance Software***. The serial number, version, build number (including a link to the change log for that version), and license expiration date of the Skylar Compliance installation. This information is also available in the footer.
- ***Latest User Activity***. Administrator logins/logouts, and other user-initiated operations.

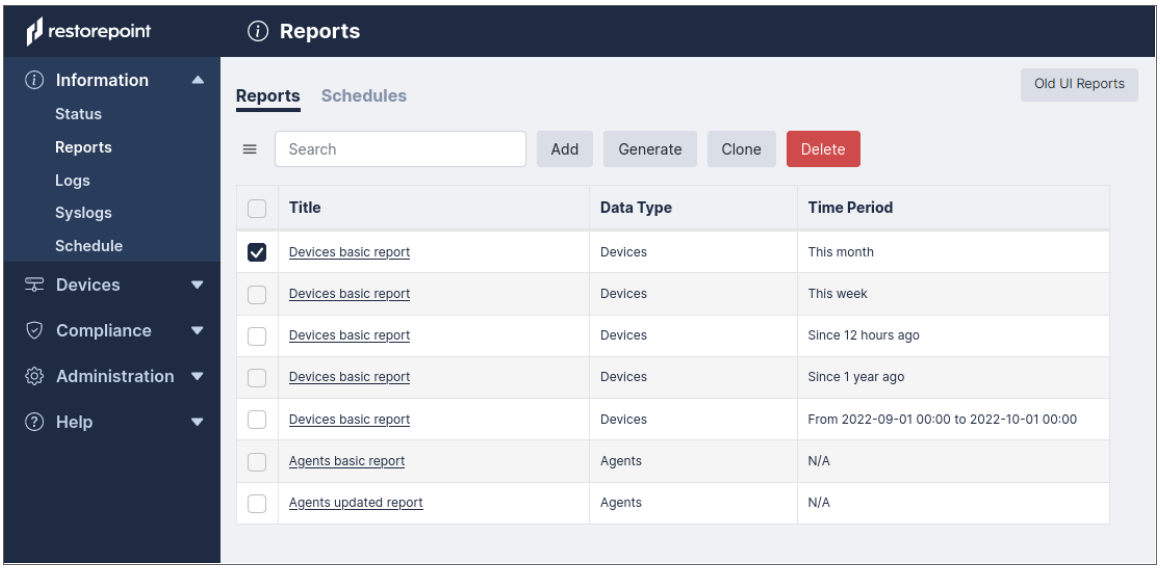
- ***Latest Configuration Changes***. Any devices that have reported modified configurations.
- ***Latest Critical Events***. Any backup failures, bad logins, or other important information.

Chapter 4

Reports

Overview

This chapter describes how you can perform a multitude of report-related functions in Skylar Compliance. The **Reports** page (Information > Reports) primarily allows you to add, generate, and schedule reports to your set specifications. However, you can also clone and delete reports/report schedules for better data refinement. You can select multiple individual reports, also called multireports, on this page. The check-boxes located to the left of the listed reports and schedules allow you to multiselect.



This chapter covers the following topics:

Adding a Report *35*

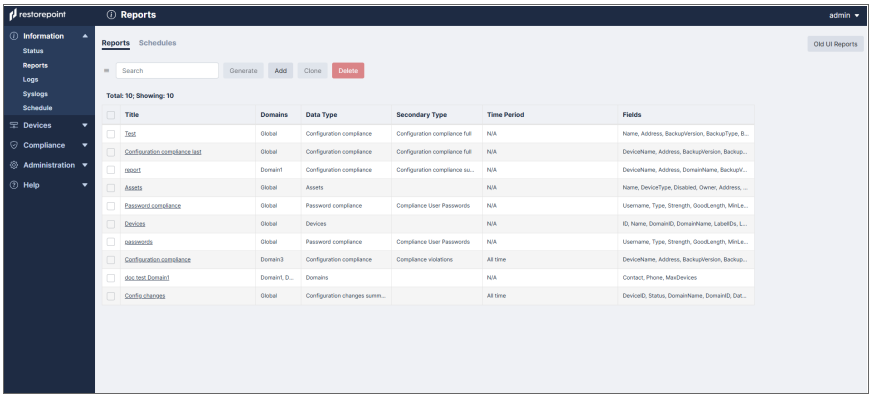
Editing a Report *36*
Generating a Report *37*
Cloning a Report *38*
Adding a Report Schedule *39*
Editing a Report Schedule *40*
Deleting a Report or Report Schedule *40*
Viewing Old User Interface Reports *41*

Adding a Report

You can add reports that provide device data suited to your selected fields.

To add a new report:

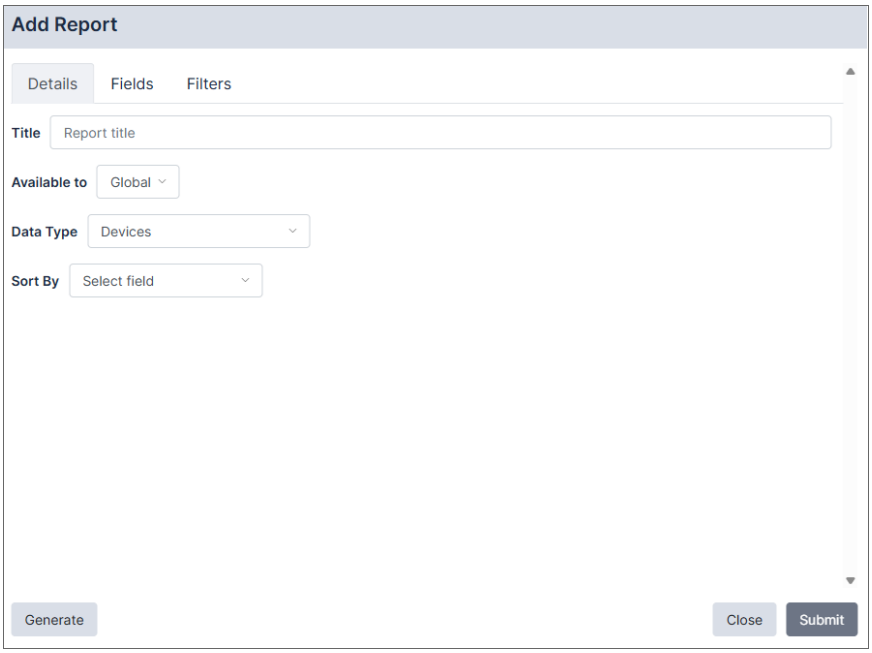
1. Go to the **Reports** tab (Information > Reports) and click **[Add]**.



2. The ***Add Report*** modal appear. Complete the following field on the **[Details]** tab:
   - ***Title***. Enter your report's title.
   - ***Available to Domains***. Select the domains to which you want the report shared.
   - ***Data Type***. Select your report data type.
   - ***Sort by***. Determine which column field that the generated table on your report will be sorted by.
3. On the **[Fields]** tab, select the check boxes for the data fields you want to appear in the report.

> **NOTE:** Any "Additional Info Command" values will be added to the same column when generating reports, based on the command name. For example, if you add multiple "ls" commands, they will appear under the same column on the generated report.

4. On the **[Filters]** tab, click **[Add]** to add the filters you want on your report. Select your ***Plugin (=)***, ***Label (=)***, and their associated plugins/labels. Filters limit, or exclude, a specific ***Domain***, ***Location***, ***Device Type***, or ***Device***. A device must match *all* filters to be included in the report; there are a wide range of combinations that can be met for your report.



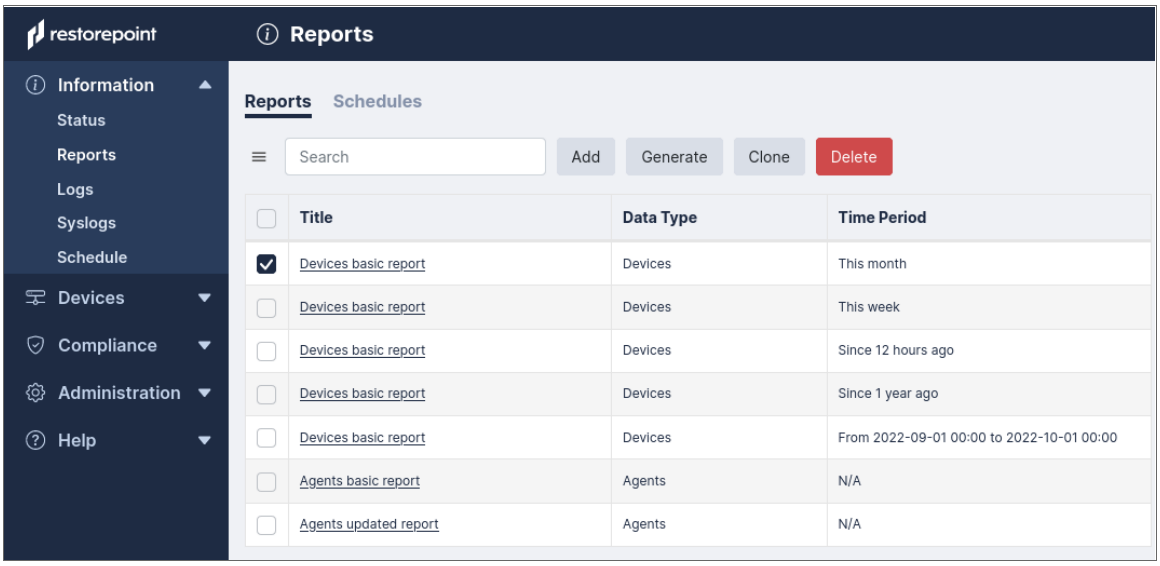
5. Click **[Submit]** to add the report. Your report will appear in the **Report** page list.

Editing a Report

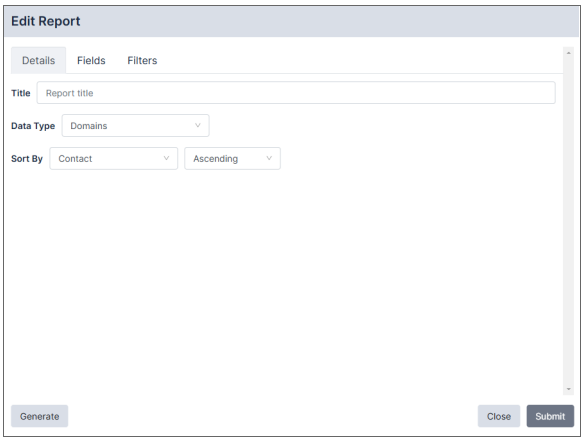
You can edit existing reports to reflect any report updates that come after creation or perform additional report functions.

To edit a report:

1. Click the **Reports** (Information > Reports) tab and select your *Report Title* from the Reports list to edit that specific report.



2. The ***Edit Report*** modal appears. Update the fields you want to edit:



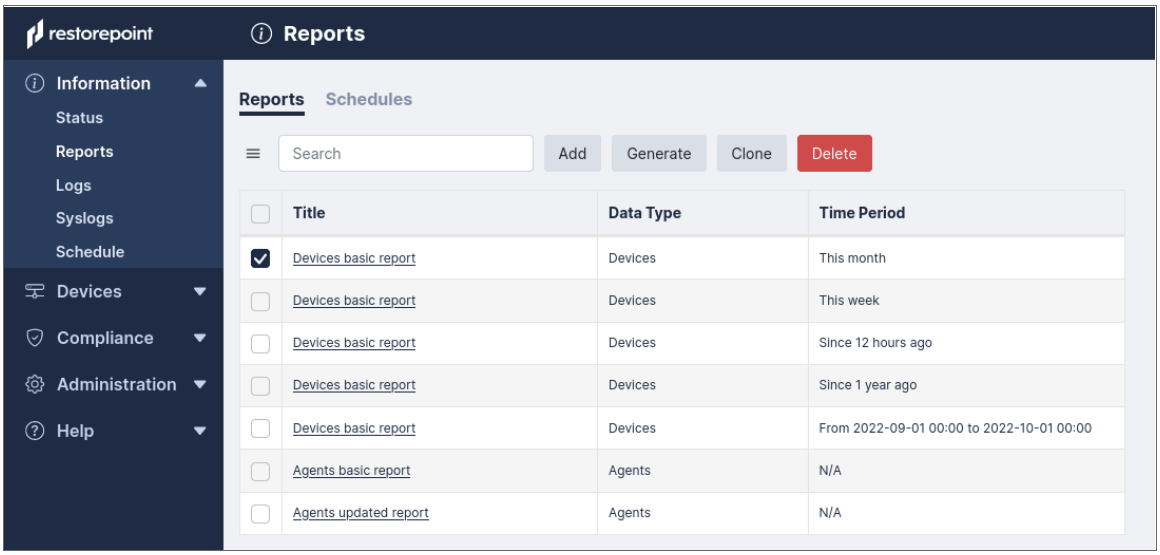
3. Click **[Submit]** to submit your report edits.

Generating a Report

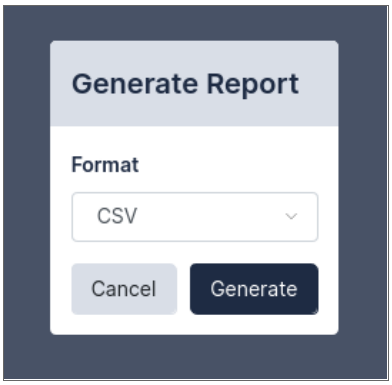
You can generate reports to view device data suited to your report's selected fields.

To generate a report:

1. Click the **Reports** (Information > Reports) tab and select the checkbox next to your report to generate and click **[Generate]**.



2. The **Generate Report** modal appears. Select your report's *Format*. Reports can be produced in these formats: CSV and PDF.



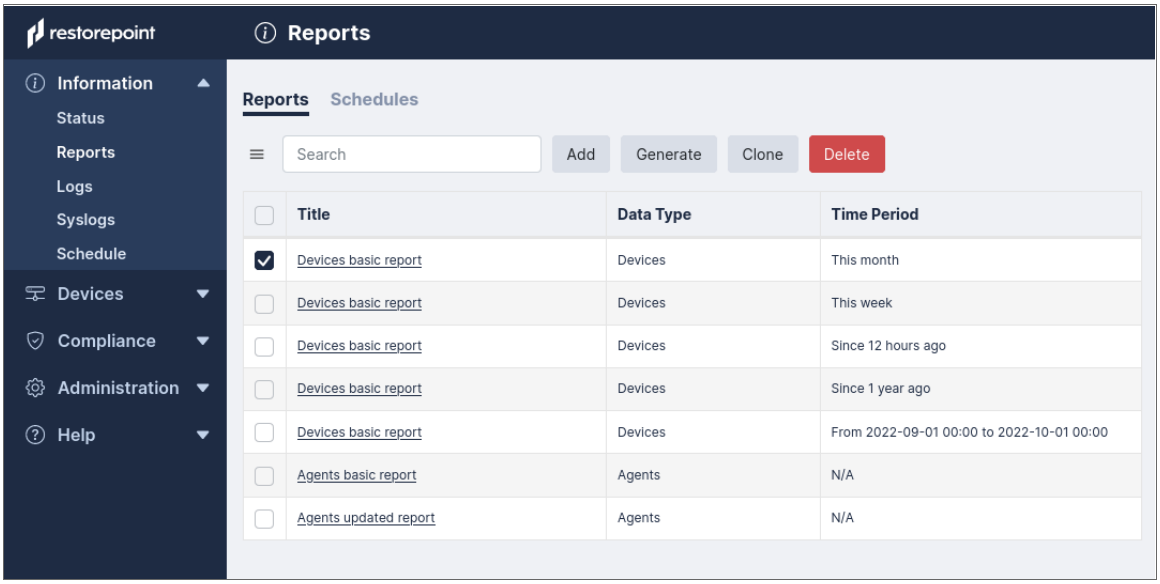
3. Click **[Generate]** to view the report in your selected format.

Cloning a Report

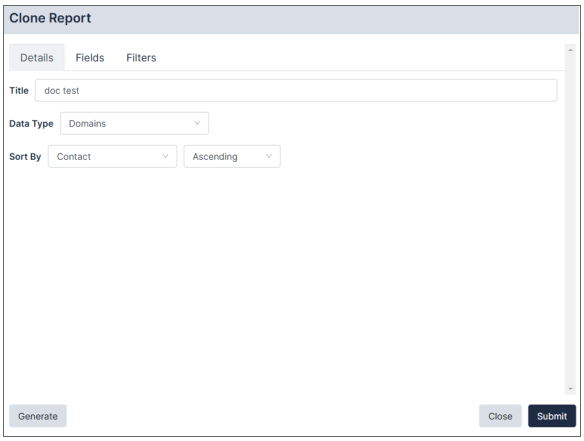
You can clone existing reports to add a new report that is similar to another.

To clone a report:

1. Click the **Reports** (Information > Reports) tab and select the checkbox next to the report you want to clone and click **[Clone]**.



2. The ***Clone Report*** modal appears. Complete the following fields:



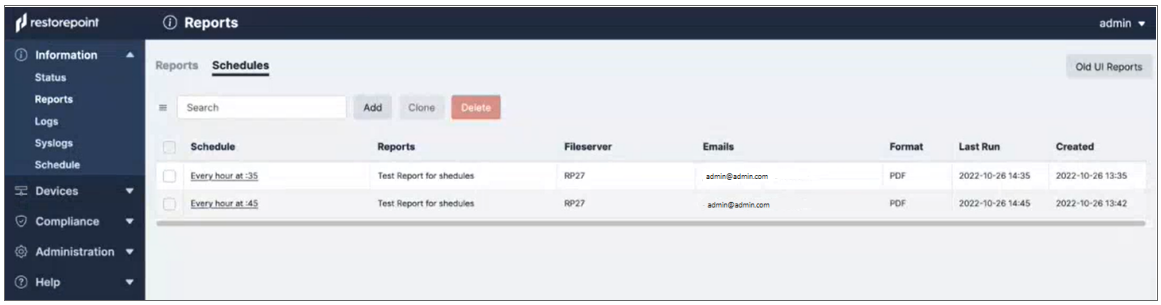
3. Click **[Submit]** to finish adding the clone report.

Adding a Report Schedule

You can schedule reports to run automatically at a selected time. Every schedule requires a minimum of one email or fileserver to be set.

To add a scheduled report to run automatically:

1. Click the **[Schedules]** (Information > Reports > Schedules) tab.



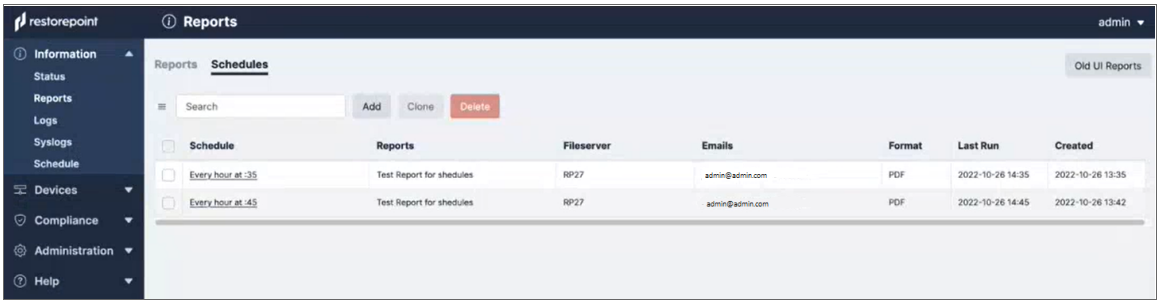
2. Click **Add**.
3. The ***Add Schedule*** modal appears. Complete the following fields.
    - ***Every [Number] [Time increment] at [Number]***. Enter your report schedule's run frequency.
    - ***Fileserver***. Select your fileserver.
    - ***Emails***. Enter the email address(es) that will receive the report.
    - ***Format***. Reports can be produced in these formats: HTML, CSV, PDF, and XML.
    - ***Reports***. Select a report to test.
4. Click **[Submit]** to complete your new report schedule.

Editing a Report Schedule

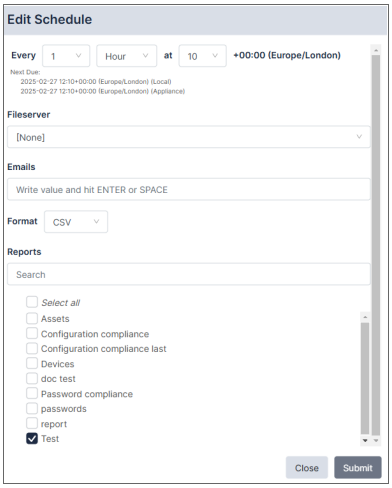
You can edit existing report schedule to reflect any schedule updates that come after creation or perform additional schedule functions.

To edit a report schedule:

1. Click the **[Schedules]** (Information > Reports > Schedules) tab and select your *Schedule Title* from the Schedules list to edit that specific schedule.



2. The ***Edit Schedule*** modal appears. Update the fields you want to edit.



3. Click **[Submit]** to submit your schedule edits.

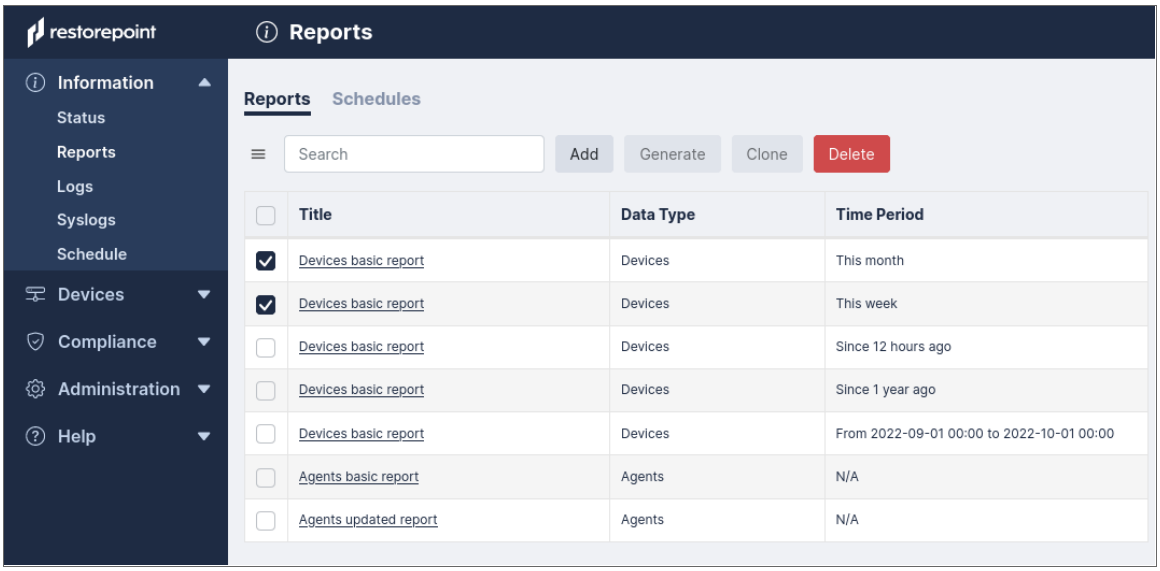
Deleting a Report or Report Schedule

You can delete existing reports, or report schedules, from their respective lists.

To delete a report or report schedule:

1. From either the **[Reports]** or **[Schedules]** tab, select the check-box next to your report(s), or report schedule(s), to remove.

2. Click **[Delete]**. The selected report(s) or report schedule(s) will no longer appear in the list.



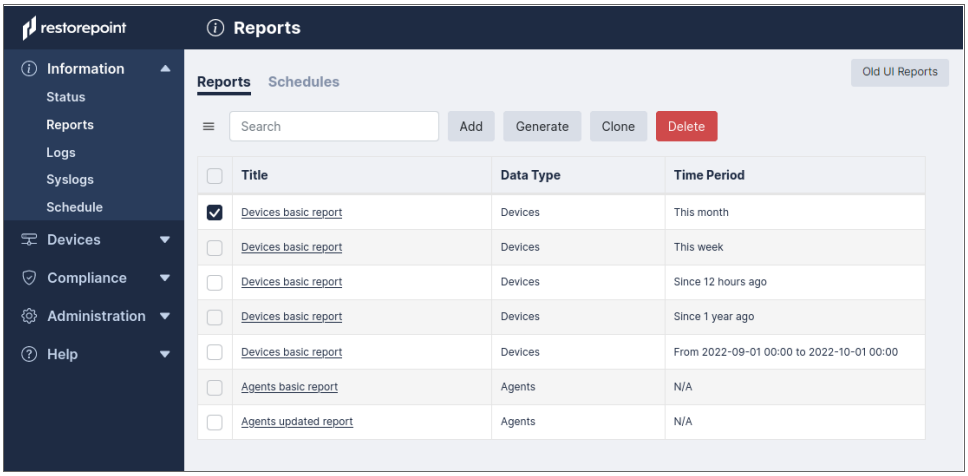
Viewing Old User Interface Reports

You can view old Skylar Compliance user interface reports that have been migrated over from the old user-interface.

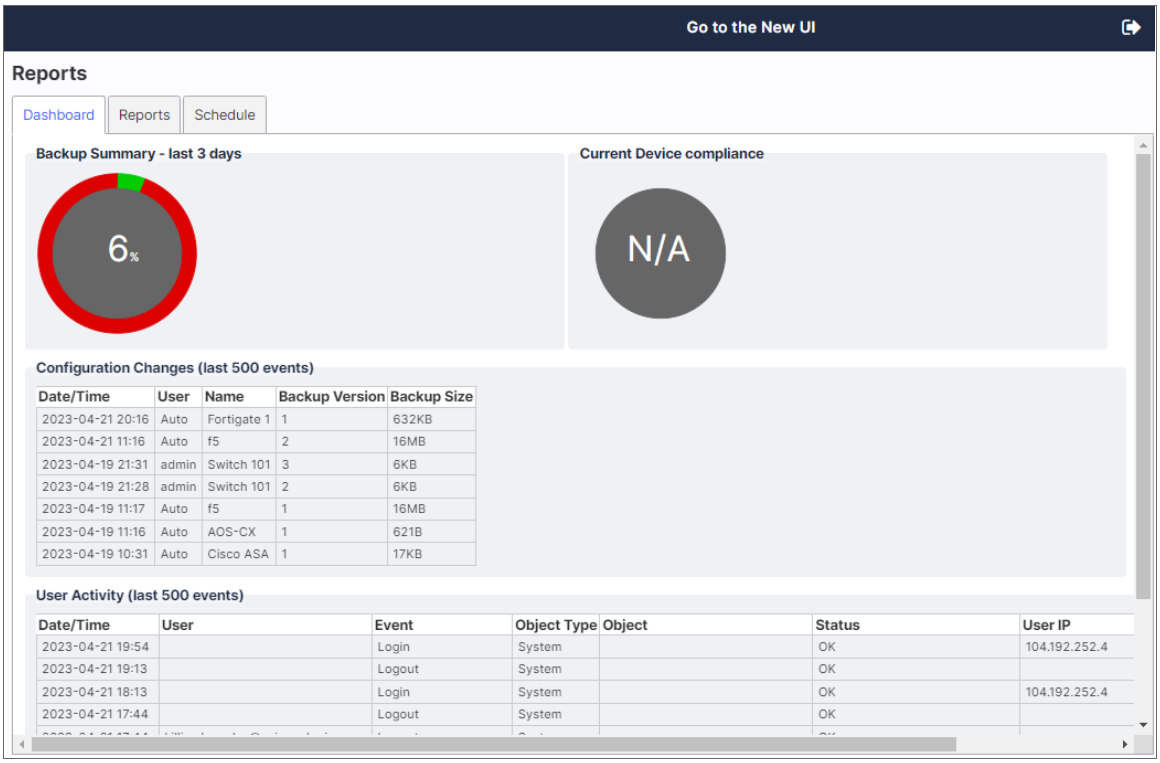
IMPORTANT: Old user interface reports (Information > Reports >Old UI Reports) will be deprecated in upcoming releases. To prevent any data loss, you should migrate any old reports tot he new reports (Information > Reports). For more information, contact ScienceLogic Support.

To view old reports:

1. From the ***Reports*** tab, click **[Old UI Reports]**.



2. The old version of the Skylar Compliance **Reports** page appears and is available for reviewing. Click **[Go the New UI]** to return to the new user-interface's **Reports** module.



Chapter 5

Logs

Overview

The **Logs** page displays detailed information about system activity.

This chapter covers the following topics:

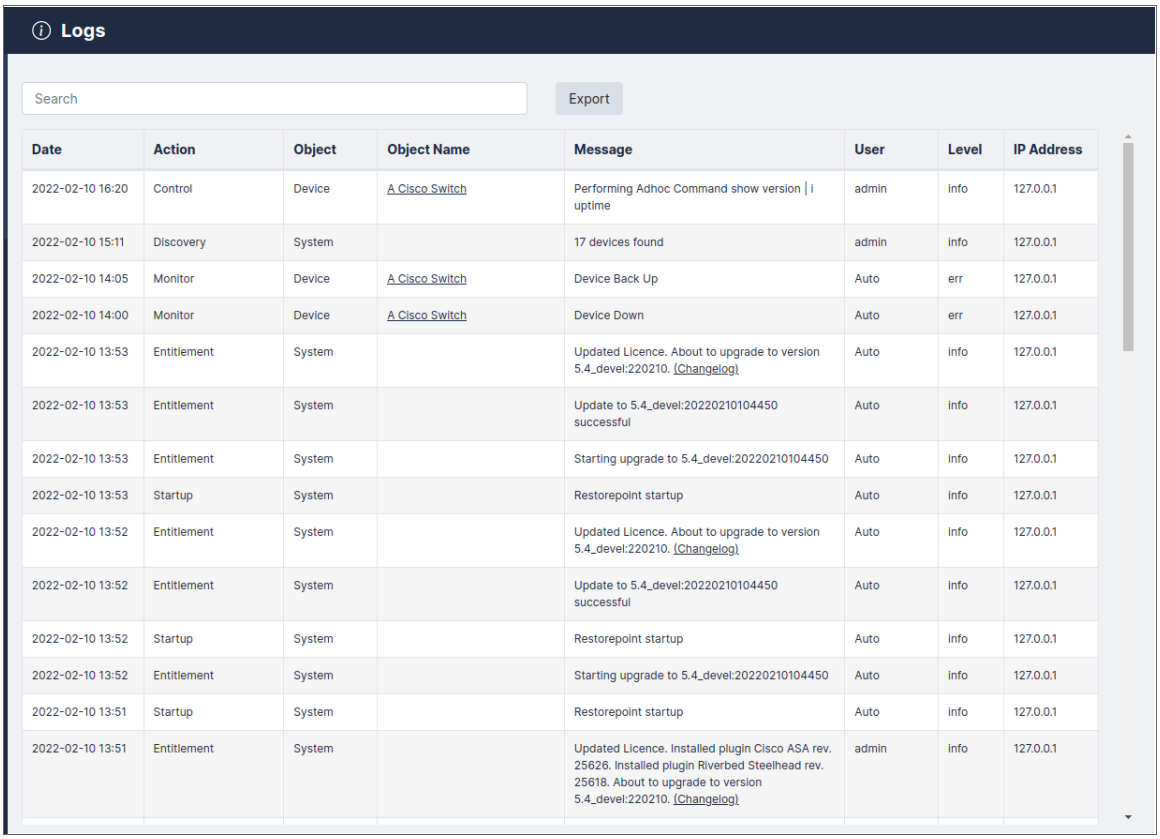
Event Log 44

Syslogs 45

Event Log

These are the log messages for user activity, device operations, and system messages. A typical entry displays:

- ***Date***. The specific time of an event.
- ***Action***. The event type.
- ***Object***. The device, user, or system configuration object to which the event refers.
- ***Object Name***. The device, user, or server that an action was performed on.
- ***Message***. The status, return, or error message associated with the event.
- ***User***. The user associated with the event (or Auto for scheduled events).
- ***Status***. `OK` or `Error`
- ***IP Address***. The IP Address that is associated with the event, or *localhost*.



Date	Action	Object	Object Name	Message	User	Level	IP Address
2022-02-10 16:20	Control	Device	A Cisco Switch	Performing Adhoc Command show version | i uptime	admin	info	127.0.0.1
2022-02-10 15:11	Discovery	System		17 devices found	admin	info	127.0.0.1
2022-02-10 14:05	Monitor	Device	A Cisco Switch	Device Back Up	Auto	err	127.0.0.1
2022-02-10 14:00	Monitor	Device	A Cisco Switch	Device Down	Auto	err	127.0.0.1
2022-02-10 13:53	Entitlement	System		Updated Licence. About to upgrade to version 5.4_devel:220210. (Changelog)	Auto	info	127.0.0.1
2022-02-10 13:53	Entitlement	System		Update to 5.4_devel:20220210104450 successful	Auto	info	127.0.0.1
2022-02-10 13:53	Entitlement	System		Starting upgrade to 5.4_devel:20220210104450	Auto	info	127.0.0.1
2022-02-10 13:53	Startup	System		Restorepoint startup	Auto	info	127.0.0.1
2022-02-10 13:52	Entitlement	System		Updated Licence. About to upgrade to version 5.4_devel:220210. (Changelog)	Auto	info	127.0.0.1
2022-02-10 13:52	Entitlement	System		Update to 5.4_devel:20220210104450 successful	Auto	info	127.0.0.1
2022-02-10 13:52	Startup	System		Restorepoint startup	Auto	info	127.0.0.1
2022-02-10 13:52	Entitlement	System		Starting upgrade to 5.4_devel:20220210104450	Auto	info	127.0.0.1
2022-02-10 13:51	Startup	System		Restorepoint startup	Auto	info	127.0.0.1
2022-02-10 13:51	Entitlement	System		Updated Licence. Installed plugin Cisco ASA rev. 25626. Installed plugin Riverbed Steelhead rev. 25618. About to upgrade to version 5.4_devel:220210. (Changelog)	admin	info	127.0.0.1

Use the **[Export]** button to export the event log as a CSV file.

Entries in the system log will be deleted according to the retention policy set on the *Log Settings and Alerts* page.

Syslogs

The following messages are logged to the Skylar Compliance syslog service by both the appliance itself and any devices configured to log to it.

Date/Time	Date/time of an event
Process	Syslog Process
Level	Syslog level (`Alert`, `Critical`, `Error`, `Warning`, `Notice`, or `OK`, corresponding to severity levels 1- 6).
Message	Status/Error message associated with the event.
Facility	Syslog Facility
Source	The IP Address that is associated with the event or *localhost*.

Chapter 6

Schedule

Overview

The **Schedule** page (Information > Schedule) displays upcoming scheduled tasks, including the next backup for each device.

This chapter covers the following topics:

Scheduled Tasks *47*

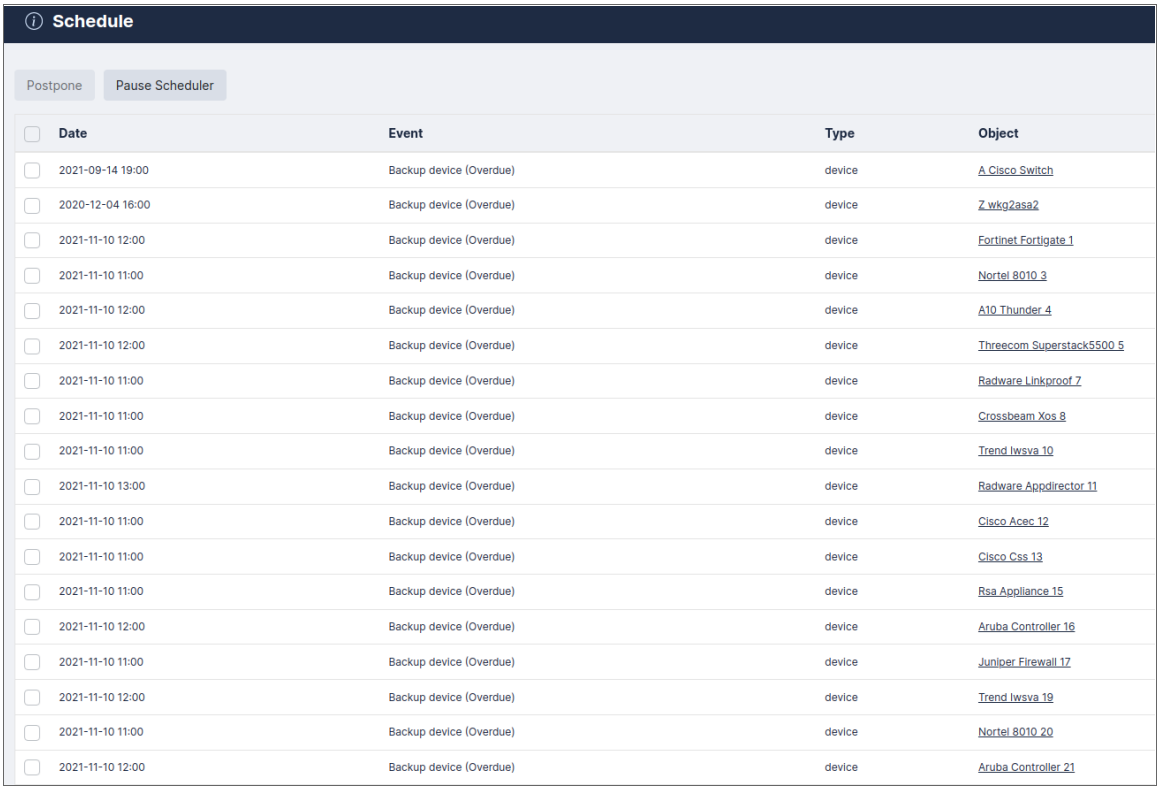
Postponing Tasks *47*

Pausing Tasks *48*

Scheduled Tasks

For each task, the **Schedule** page displays the following information:

- ***Date***. Date and time when the next task is due.
- ***Event***. Name of the scheduled event.
- ***Type***. Type of task. Possible types are backup, discovery, archive, etc.
- ***Object***. Device, user, or system configuration object to which the task refers.



Postponing Tasks

You can postpone any scheduled event to remove the next occurrence of a scheduled task. To postpone a scheduled task:

1. Find the task that you want to postpone and select it's checkbox.
2. Click the **[Postpone]** button.

Pausing Tasks

You can pause a scheduled task so it doesn't run until you unpause the task. To pause a scheduled task:

1. Find the task that you want to pause and select it's checkbox.
2. Click the **[Pause Scheduler]** button.

Chapter 7

Device List and Discovery

Overview

The **Device List** page (Devices > Device List) contains a list of all of your discovered devices. On this page, you can add, edit, import, and export devices, along with other activities.

This chapter covers the following topics:

Adding Devices to Skylar Compliance 50

Adding a New Device Manually 50

Importing Multiple Devices Using a CSV File 54

Device Discovery 55

Running a Manual Backup 59

Editing an Existing Device 59

Device Monitoring 61

Viewing the List of Configurations for a Device 62

Backup File Operations 68

Cloning 69

Adding Devices to Skylar Compliance

You can add devices to Skylar Compliance using the following methods:

- *Adding a New Device Manually*
- *Importing Multiple Devices Using a CSV File*
- *Automatic Discovery*

The **Device** page allows you to:

- Display all the existing backups for a device
- Compare the configurations of two devices

The **Discovery** page allows you to:

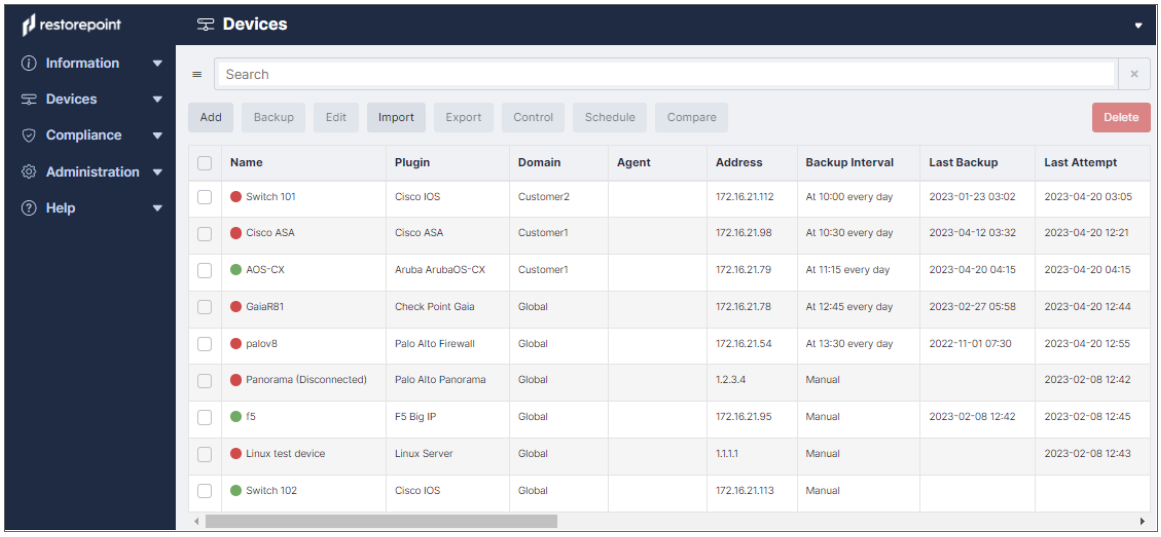
- Define the networks you wish to scan
- Schedule a periodic network scan
- Import discovered devices into the main device list

Adding a New Device Manually

How you configure a new device may vary slightly from one device to another. Please see device-specific information in the Plugin Guide (**Help > Plugin Guide**).

To create a new device:

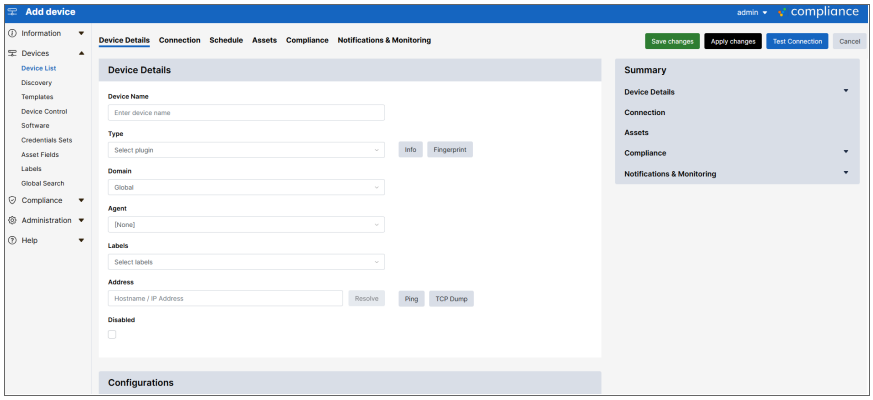
1. Go to the **Device List** page (Devices > Device List).



2. Click the **[Add]** button on the top left hand corner of the page. The **Add device** page appears. Complete the following fields:

- ***Device Name***. Type a name for the device that is up to 64 characters long.
- ***Type***. Select the device type. You can start typing in the *Select Plugin* field to filter the list. This list only displays the device types that are currently available on your license.
    - Click the **[Info]** button to view additional device data.
    - Click the **[Fingerprint]** button to view data about header banners, like SSH or FTP, if you enter an IP address in the device ***Address*** field.
- ***Domain***. Select the domain that the device is assigned to. This field is only present if Domain Administration is enabled on your appliance. For more information, see *Administration Domains*.
- ***Agent***. If the device is managed via an agent, select the appropriate agent from the dropdown list.
- ***Labels***. Select and set Labels to be applied to your devices; these help filter and group devices.
- ***Address***. Type the device IP address. You can click the **[Resolve]** button to automatically fill the ***IP Address*** field. Skylar Compliance will keep the IP address up to date with your DNS and manual changes to the IP address will be ignored.
- ***Open Terminal***. You can click this button to open a web-based virtual terminal to the device that you can use for troubleshooting. If you select **Skylar Compliance Credential**, the field uses the credentials you have defined on the **Connection** tab. Otherwise, you will need to provide your own credentials for logging into the device. For more complex terminal use, ask your account manager about **Skylar Compliance Universal Console**.
- ***Owner Email***. Type the email address(es) of the device administrator(s). By default, this field is filled with the notification email address defined on the **System Configuration** page.
- ***Email on Config Change***. Select this checkbox to automatically trigger an email notification to the device owner when a device configuration change is detected. This option is not available for all device types.
- ***Email on Start Backup***. Select this checkbox to automatically trigger an email notification before a backup starts for this device. This notification creates a 1 minute delay before the backup starts.
- ***Email on End Backup***. Select this checkbox to automatically trigger an email notification when a backup completes. If this checkbox is not selected, Skylar Compliance will only send an email notification if the backup fails, or if a configuration change is detected and **Email Config Change** is selected.
- ***Syslog Change Detection***. If this field is available on your Skylar Compliance system, select the checkbox for Skylar Compliance to automatically detect when a device is modified and automatically retrieve its configuration. Note that this feature is only available for specific devices. For more information, see the Plugin Guide (**Help > Plugin Guide**).
- ***Log Transcript***. Select this checkbox to create a full transcript log for this device for debugging purposes. A transcript log is automatically saved if the backup fails, so this is rarely needed.
- ***Types***. Select the types of configurations to backup for this device.

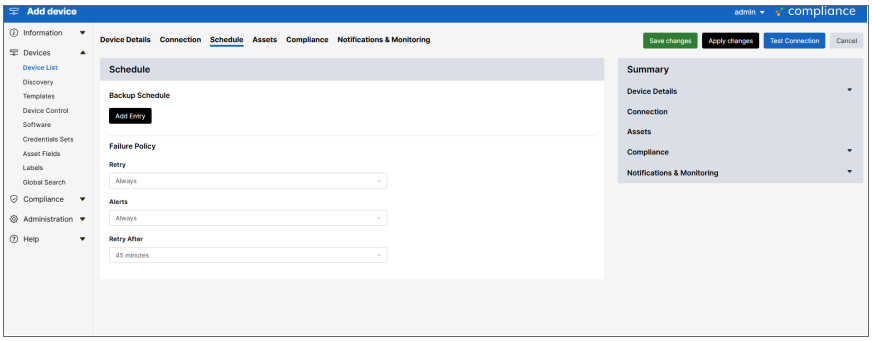
- ***Filename Prefix***. Optionally type a custom filename prefix for the device configuration files, and check the relevant fields to include. A preview of the filename will appear in the ***Preview*** field.
- ***Monitor***. Select this checkbox to monitor the device. For more information, see *Device Monitoring*.



3. Click the **[Connection]** tab and complete the following fields:
   - ***Protocol***. Select the appropriate connection protocol for your device, such as telnet or SSH. The options may vary depending on the device type.
   - ***Username***. Type the administrator account username for the target system.
   - ***Password***. Type the password associated with the administrator account. For some devices you may need to enter more than one password. The field color ranges from red to green to indicate the password strength, according to the policy set in the *Password Policies* page.
   - ***Use Skylar Compliance Credentials?***. You can select this checkbox and select a **Credential Set** instead of entering a username and password. Credential sets are reusable username/password combinations that can be shared among different devices (See *Credential sets*).
   - ***Back Connection NAT***. Select this checkbox if Skylar Compliance accesses this device through a NAT router or firewall. This option will only be displayed if the device requires back-connections and if *Use NAT* is selected in the **System** page. If a **NAT IP Address** is configured here, it will override the corresponding Domain (Section *Administration Domains*) and System (Section *Network Address Translation (NAT)*) settings.
   - ***Use SSHv2 PKA***. Select this checkbox if you want to use SSH Public Key Authentication instead of password-based authentication when connecting to the device. Click the **[Show Keys]** button to display Skylar Compliance's public SSH keys.
   - ***Disable SSH Strict Host Key Checking***. Disables the SSH host key validation and logs when the key changed.
   - ***Verify certificate***. Shown for HTTPS-based protocols. Checks that the device certificate is valid for the address used to reach it and is issued by a CA the appliance trusts. Most devices use self-signed certificates, which fail this check, so leave it off for them. New devices default to on when FIPS mode is enabled.

- ***Clear Cache***. If you have replaced a device, Skylar Compliance may refuse to connect to it because it will detect that the device key has changed and display a connection error. This is a security feature of SSH. In order to override this feature, click the **[Clear Cache]** button.
- ***Backup Port***. If required for your device, enter the backup port you want to use.

4. Click the **[Schedule]** tab to configure the backup schedule for the device and click **[Add Entry]** to add one or more backup intervals. You can bulk add or remove schedules if multiple are selected on the **Device List** page.



> **NOTE:** For each schedule interval, you can override the config types to backup by selecting any of the **Config Type** checkboxes, or override the default retention policies by unselecting **Use Default Policy**. You can also override the Failure Policy on this page. For more information, see *Backup failures*.

5. Click the **Assets** tab and enter optional asset management details for the device:
   - ***Serial***. Type the serial number for the device.
   - ***Firmware***. Type the firmware the device has.
   - ***Asset ID***. Type the device ID for the device.
   - ***Notes***. Type any additional notes that you would like to include for the device.
   - ***Purchase Date***. Select the date you or your organization purchased the device.
   - ***Purchased From***. Type the business that you purchased the device from.
   - ***Manufacturer***. Type the manufacturer of the device.
   - ***Model***. Type the device model.
   - ***History***. Type any relevant history related to the device.
   - ***Owner***. Type the device owner.
   - ***Customer No***. Type the customer number.
   - ***Build Document***. Select **[Upload]** to upload a build document or **[Remove]** to remove a build document.

> **NOTE:** Custom fields can be added in the **Custom Asset Fields** page. For more information, see *Asset Fields*.

6. The **[Additional Info]** tab, if available, displays additional information retrieved from the device, such as license details, routing table, and network interfaces. You can also display the output of a saved action on this page using the ***New Info Command*** drop-down field. For more information on creating actions, see *Controlling a device*.
7. Click the **[Compliance]** tab and assign compliance policies to this device. For more information on compliance policies, see *Device Policies*.
8. Click the **Notifications & Monitoring** tab and enter optional notification details for the device:
   - ***Owner Emails***. Type the email address(es) that you want to receive device notifications.
   - ***Email on***. Select a task that you want to trigger a notification.
   - ***Log transcript***. Select this checkbox if you want the notification to include a transcript of the task.
   - ***Monitor Device***. Select this checkbox if you want to monitor the device.
   - ***Type***. Select how you want to monitor the device, using TCP connection or ping.
   - ***Email when down***. Select this checkbox if you want a notification to trigger when the device is down.
   - ***Fail after***. Type a number or use the scroll to define after how many attempts connecting to a device that a notification should be triggered.
   - ***Email when up***. Select this checkbox if you want a notification to trigger when the device connects after failing.
9. Click **[Save Changes]** to finish creating the new device. The **Device** page appears and the new device is added.



10. Once you add the device, you can select the checkbox next to the device and click the **[Backup]** button to perform a manual backup, if required. The backup progress and completion will be shown in the **Activity Display**. If the backup is completed successfully, the indicator next to the device name is green, and the date of the last backup is added to the **Device List** page.

Importing Multiple Devices Using a CSV File

If you need to add a large number of devices, you can click the **Import** button and select a comma-separated values (.CSV) file, that contains the device details.

When you create a comma-separated value (CSV) text file to import, include a line at the top of the file to indicate the columns for the attributes you want to import. Fields can be in any order. For example:

```
name,plugin,protocol,ip_address,username,password,password2,backup_
port,keep_backup,owner,serial_no,asset_id,location,notes
```

The following table lists the column name and its description:

Field	Description
domain_name	If there is not a domain_name present and you have permissions to create devices on the global domain, then the device will be saved on a global domain. If not, Skylar Compliance will find a domain with the same name and if you have permissions to create devices on that domain, it will be created there. *This field is optional*.
name	The device name. *This field is required*.
plugin	The device type (e.g. 'Cisco ASA' or 'cisco_asa').
protocol	The connection protocol, such as telnet or ssh. *This field is required.*
ip_address	The device IP address.
username, password, password	The login credentials for the device.
backup_port	The port to use to connect to the device, if required.
keep_backup	The backup retention policy (days).
owner, serial, no, asset_id, location, notes	Device details and descriptors. *These fields are optional.*

Device Discovery

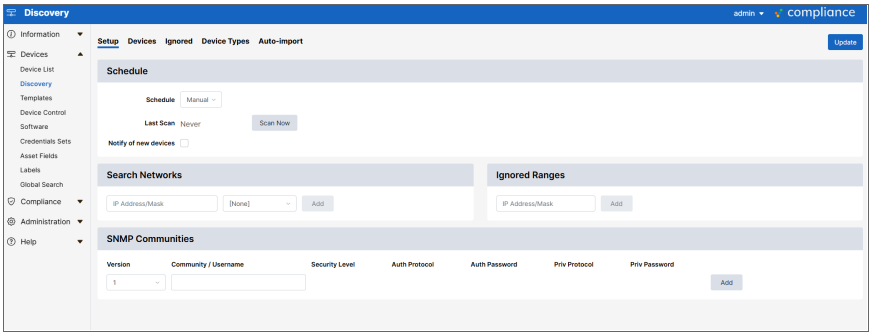
The Skylar Compliance device discovery engine uses a variety of methods to discover hosts on your network that can be imported to the main device list. You can also be notified by email of new devices that are installed on your network.

NOTE: Device discovery is not guaranteed to discover all the relevant devices on your network. Firewalls or the device configuration itself may negatively affect the discovery process. Similarly, the device type may not always be detected correctly. When you import a device, you are able to override the detected type.

Discovery Setup

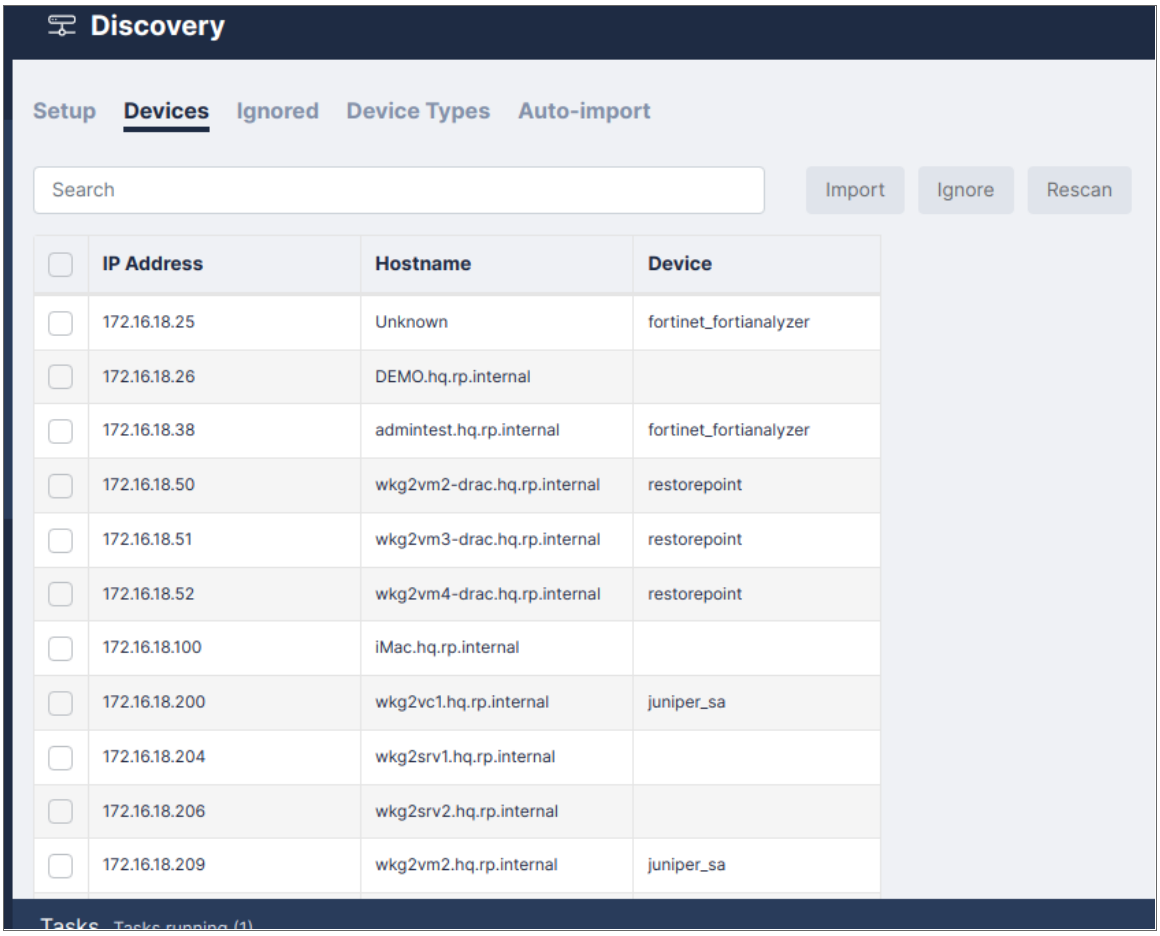
To configure discovery:

1. Go to the **[Setup]** tab (Devices > Discovery > Setup).
2. Type one or more network ranges (in CIDR notation) to scan in the ***Search Networks*** field, for example: `10.20.0.0/16` and click **[Add]**.
3. If you do not wish to scan a particular range, for example `10.20.10.0/24`, add this to the **Ignored Ranges** list.
4. You can optionally add one or more SNMP communities in use on your network: choose the SNMP version, enter a community string, and then click the **[Add]** button.
5. If you want to be notified of a new device, select the **Notify of new devices** checkbox.
6. If you want to use the Cisco Discovery protocol (https://en.wikipedia.org/wiki/Cisco_Discovery_Protocol), select the **Use CDP** checkbox.
7. If you want to use the Link Layer Discovery protocol (https://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol), select the **Use LLDP** checkbox.
8. Choose a scan schedule.
9. Click **[Update]**.
10. Click **[Scan Now]** to start the scan.



Discovered Devices

At the end of a discovery scan, a list of discovered devices is displayed is displayed in the **[Devices]** tab:



You must import the newly added devices into the main device list. To manually import your devices:

NOTE: To automatically import your devices, see *Automatic Import*.

1. Go to the **[Devices]** tab (Devices > Discovery > Devices).
2. Once the list of discovered devices is displayed, select the checkbox to the left of one or more devices.
3. Click **[Import]**.
4. You must then finish the configuration:
    - If you only select one device to import, the **New Device** page appears which includes automatically populated discovery information. After you review the information and make any required changes, click **[Save]**.
    - If you selected multiple devices, the devices will be imported without review. The devices are marked as incomplete and are displayed in red in the devices list. You can then complete the configuration and add authentication details or edit any default parameters and click **[Save]**.

Ignored Devices

The **Ignored devices** page displays a list of devices that will be ignored in future scans. To remove devices from the ignore list, select the devices then click **Un-ignore**.

You can review the list of ignored devices and make changes. To remove devices from the Ignored Devices list:

1. Go to the **Ignored** tab (Devices > Discovery > Ignored).
2. Once the list of ignored devices is displayed, select the checkbox to the left of one or more devices.
3. Click **[Unignore]**.
4. Click **[Update]**.

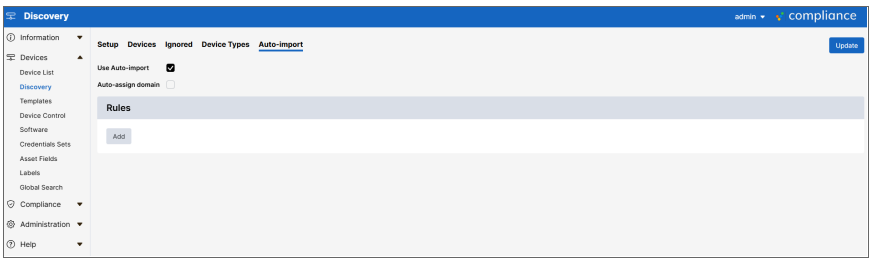
Device Types

The **Device Type Override** page allows you to force discovery scans to import a device as a certain type based on a hostname pattern. To override a device type:

1. Go to the **Device Types** tab (Devices > Discovery > Device Types).
2. Click **[Add]** and enter values in the following fields:
    - ***For hostname pattern***. Enter a hostname value to be assigned the device type.
    - ***use plugin***. Select a device type.
3. Click **[Update]**.

Automatic Import

You can automatically import your devices to the **Device** page after setting up discovery. To automatically import your devices:



1. Go to the **Auto-import** tab (Devices > Discovery > Auto-import).
2. Select the ***Use Auto-import*** checkbox.
3. Click **[Update]**.

Running a Manual Backup

To run a manual backup:

1. Go to the **Device** page (Devices > Device List).
2. Select the checkbox to the left the devices that you want to back up and click **Backup**.

> **NOTE:** You can also run a manual backup by clicking the **Backup Now** button on the **Edit Device** page (Devices > Device List > Select Device > Edit).

Scheduling an Automatic Backup

You can automatically schedule backups for a large group of devices by spreading the backups over a day, a week, or a month. To automatically schedule backups:

1. Select the checkbox to the left of the relevant devices on the **Devices** page (Devices > Device List), and click the **[Schedule]** button.
2. Select the desired time interval, and the daily Start/End time and/or the Start/End day. For example, you can configure the schedule to run backups only at night or during the weekend.

Exporting the Device List

Click the **[Export]** button to save the device database in a CSV file.

Editing an Existing Device

To edit an existing device:

1. Go to the **Devices** page (Devices > Device List).
2. Click on the name of the device that you want to edit. The **Edit Device** page appears
3. Make any required changes and click the **[Save changes]** button.

Editing Multiple Devices

To edit multiple devices:

1. Go to the **Devices** page (Devices > Device List).
2. Select the checkbox to the left of the devices that you want to edit.

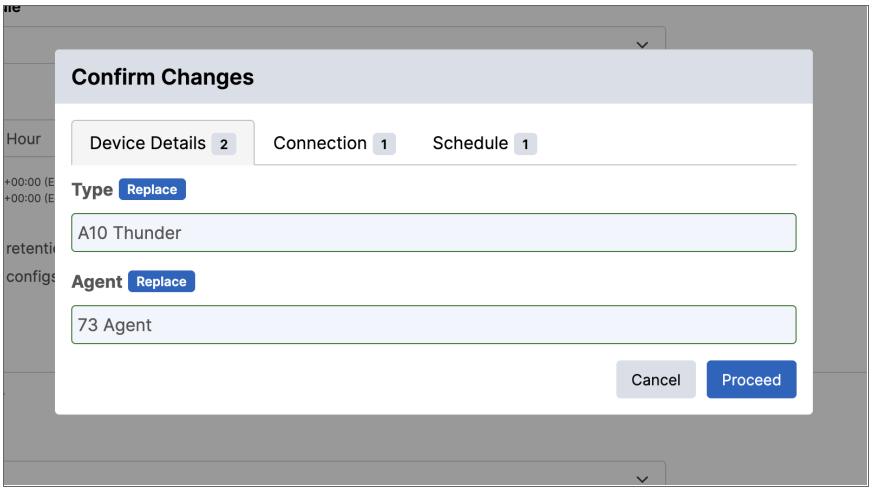
NOTE: If you select devices with different Plugins or domains, a warning message will display at the top of the device list.

3. Click **[Edit]**. The **Edit Devices** page appears.
4. Edit the fields that need to be updated. In each field, you can select from the following options:
   - ***Keep as is***. This keeps the values for all devices.
   - ***Replace***. This replaces the values for all devices. If you want to clear this value for all selected devices, leave the value blank.
   - ***Add new***. This adds the selected values to existing values for all selected devices.

TIP: If you are editing devices with the same Plugin or type, or if you selected a value for the ***Type*** field when editing the devices in step 4, you can change certain Plugin-specific options at the bottom of the **[Device Details]** tab and on the **[Connection]** tab.

NOTE: You can change the certificate for multiple devices if all of the selected devices use an HTTPS-based protocol.

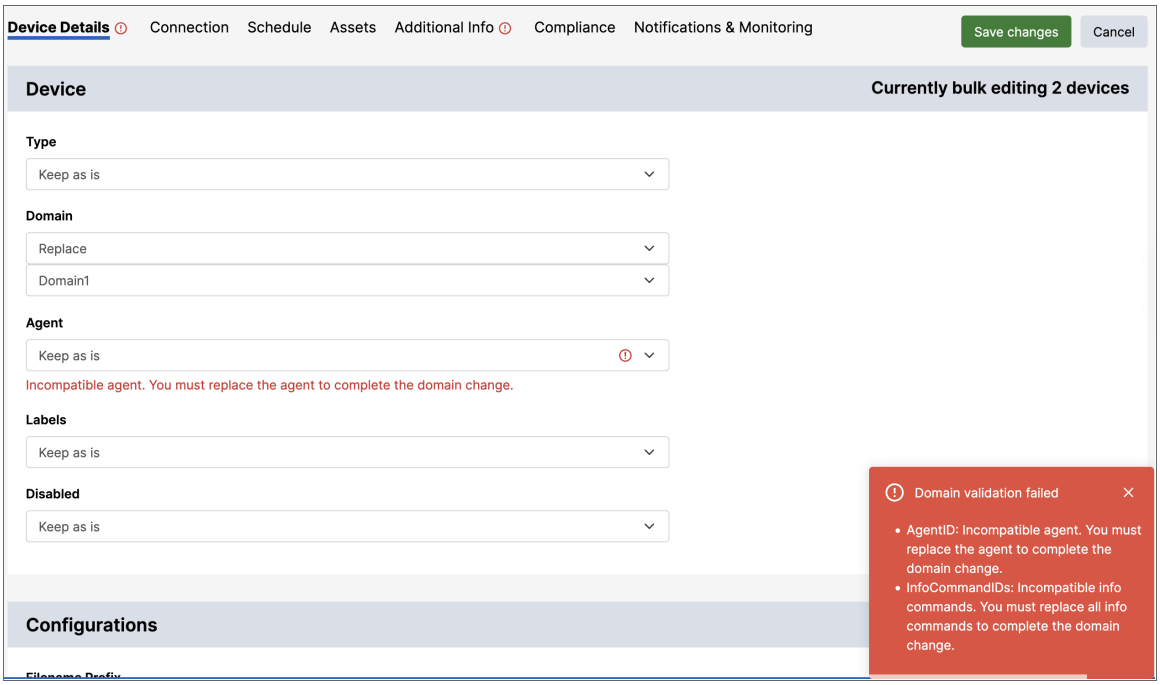
5. Once you have edited all fields that need to be updated, click **[Save Changes]**. The **Confirm Changes** modal will appear, describing all pending changes. Be sure to review all pending changes for each tab.



6. Once you have verified the changes to be made, click **[Proceed]**. If validations succeed, your changes are saved. If validations fail, errors will display in the user interface, allowing you to correct the issues. Fix the issues and then repeat step 5.

Troubleshooting Domain-related Errors

Domains are used to link multiple entities together, so when you change the domain for any devices, consider that those devices might have Agents, Labels, Credentials, Info Commands, and/or Policies linked to the existing domain. Any changes you make are validated after you submit the changes, and warnings will display if there are any errors:



To resolve errors in a situation like the example above, select *Replace* for the affected fields, and choose either nothing (to clear the fields for all selected devices), or select one of the available values.

Deleting an Existing Device

To delete an existing device:

1. Select the device(s) you want to remove.
2. Click **[Edit]**, and ensure that the ***Disabled*** field is set to *Yes* to prevent accidentally deleting a device you have not disabled.
3. Click **Save**.
4. The devices you want to remove are selected. Click **[Delete]**.

Device Monitoring

Skylar Compliance can monitor devices by periodically checking that the TCP port used for backup (for example, telnet or SSH) is accepting connections, or by sending ICMP Echo Requests (pings) to the

device. Monitoring is disabled by default and can be enabled or disabled for each individual device.

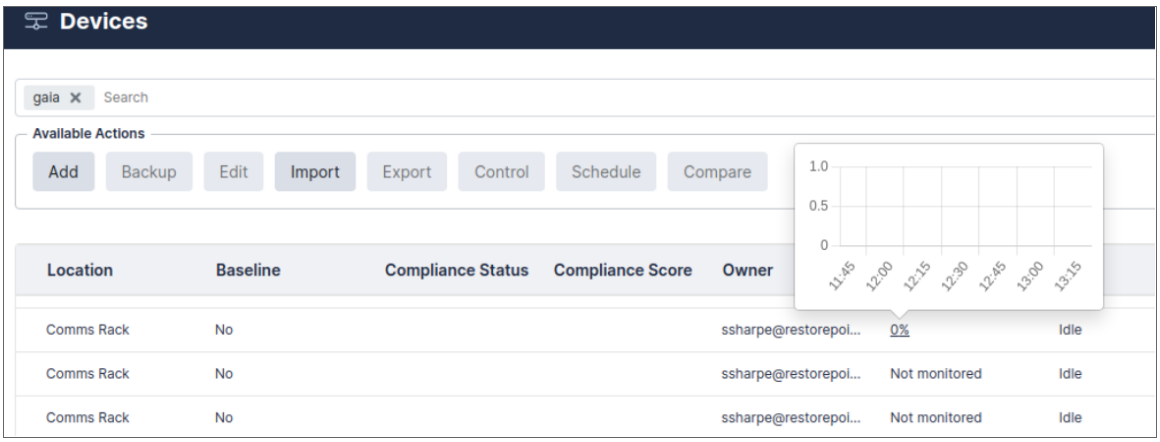
Enabling Monitoring

To enable monitoring, open the relevant device **Edit** screen:

1. From the Device List, select a device, click the **[Notifications & Monitoring]** tab, and select the **Monitor Device** checkbox. Additio
2. Select the **Type** of monitoring required. Normally, the device's TCP port used for backup is polled; if the *Ping* option is selected, the ICMP Echo Request (ping) will be used.
3. You can select **Email when down** to send an email notification if the device appears to be down. You can also choose to receive **Email when up**.
4. If the device fails to respond after the number of attempts specified in the **Fail after** box, it is considered "down".

Displaying Monitoring Information

You can hover over status information to display a Round Trip Time graph between Skylar Compliance and the device, in 5 minute intervals.



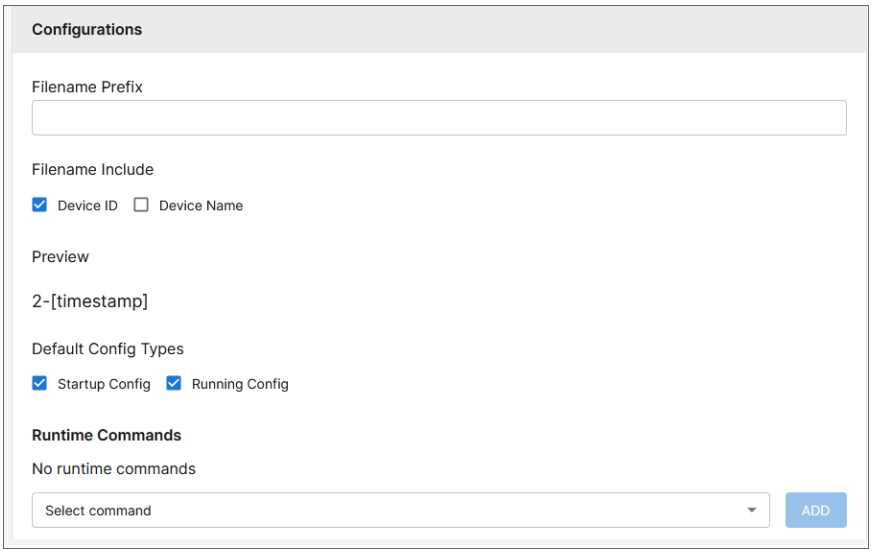
Clicking **[Uptime]** will display the monitoring graph for the device.

You can select any other monitored device from the field at the top of the page to display its graphs.

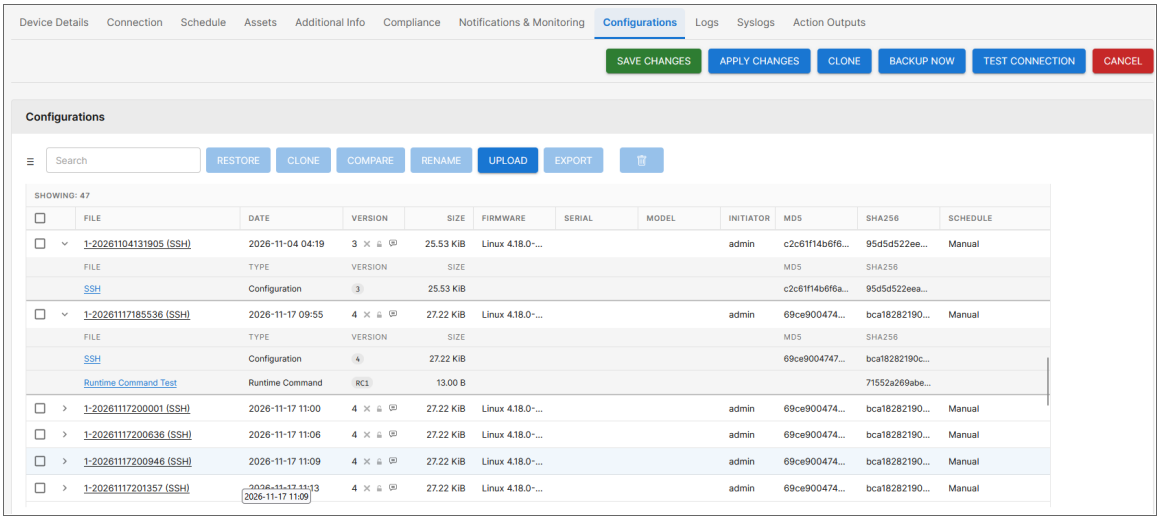
Viewing the List of Configurations for a Device

You can access the list of configurations for a device from the **Devices** page (Devices > Device List) by clicking the ***last backup*** column of the corresponding device, or by clicking the **[Configurations]** tab when you edit the device.

A configuration may contain more than one file. For example, a Cisco IOS device has a startup and a running configuration; you can choose which configurations should be backed up in the **Device Details** page.



If a device supports firmware identification, Skylar Compliance will display the firmware version detected at the time of backup, next to each configuration. A sample list is shown below:



Skylar Compliance keeps track of configuration changes by assigning a version ID to each unique configuration retrieved from a device. Identical configurations are not stored multiple times.

View	There are three available views: 1. **Default View:** A list of all the configurations retrieved from the device. 2. **Group by:** This view groups the configurations by File, Size, Firmware version, Initiator, or configuration version. 3. **Version Changes:** This view does not display consecutive entries with the same version ID, and therefore highlights configuration changes.
Baseline version	The checkmark shows the baseline version of a configuration. To set a baseline version, select the checkmark. The checkmark will become solid. Restoring a non-baseline

	configuration version to a device with a baseline configuration version will cause a compliance alert. For more information, see *Configuration Baselines*.
Retaining a version	You may want to retain a configuration indefinitely (a *milestone* configuration), that overrides your configured retention policy. For example, a backup taken just before a device upgrade. To retain a configuration, click the padlock icon next to the file name; the padlock will become solid. To undo this action, click the padlock icon again.
Adding comments	You can add a comment to a configuration by clicking the gray note icon next to the relevant configuration. Enter your comment in the pop-up dialog box and click OK; the icon will change color . To remove a comment, click the icon , delete the text, and click OK.

NOTE: The above options apply to a configuration version, rather than an individual backup.

Compare configurations	The **Compare** option is only available for the devices with text file or a tar/tgz archive of text files configurations. To compare two configurations, select two items using the checkbox to the left of the item, and click **Compare**. If the configurations are archives, Skylar Compliance will expand the archives and compare the individual files. Skylar Compliance will display the chosen configuration files side by side and highlight the differences; inserted lines will be displayed in blue and changed lines will be displayed in red. When **Only differences** is selected, Skylar Compliance will not display lines which are identical in both files, except those preceding or following a change. **Note:** Some devices embed a timestamp or fingerprint in the configuration every time a backup is performed. Wherever possible, Skylar Compliance ignores lines that only differ by such fingerprints when comparing configurations, so that only relevant changes are displayed.
Delete a configuration	Select a configuration using the checkbox and click **Delete**. This operation is usually only required to delete a milestone configuration (one you have chosen to retain indefinitely), because old configurations are automatically removed according to the retention policy.
Restore a configuration	To restore a configuration, select a configuration using the checkbox and click **Restore**. Additional options may be displayed, for instance which configuration type should be restored, or whether the device should be reset to complete the operation.
Upload Backup	This option allows you to upload a new device configuration file to Skylar Compliance from your PC.
Export Backup	You can export a device configuration from Skylar Compliance through your browser, email, make it available for FTP/TFTP/SFTP collection by a device, or export it to one of your pre-configured file servers.

Comparing Device Configurations

Skylar Compliance allows you to compare Device Configurations and sift through whole files to analyze any changes between them. You can use the compare function located on either the **Device List** page (Devices > Device List) or **Configurations** tab on the **Edit device** page. You can also select ***Show ignored***

changesin the **Compare Devices** window to view any changes that Skylar Compliance deems "not actual changes".

Examples of "not actual changes" that can be ignored include:

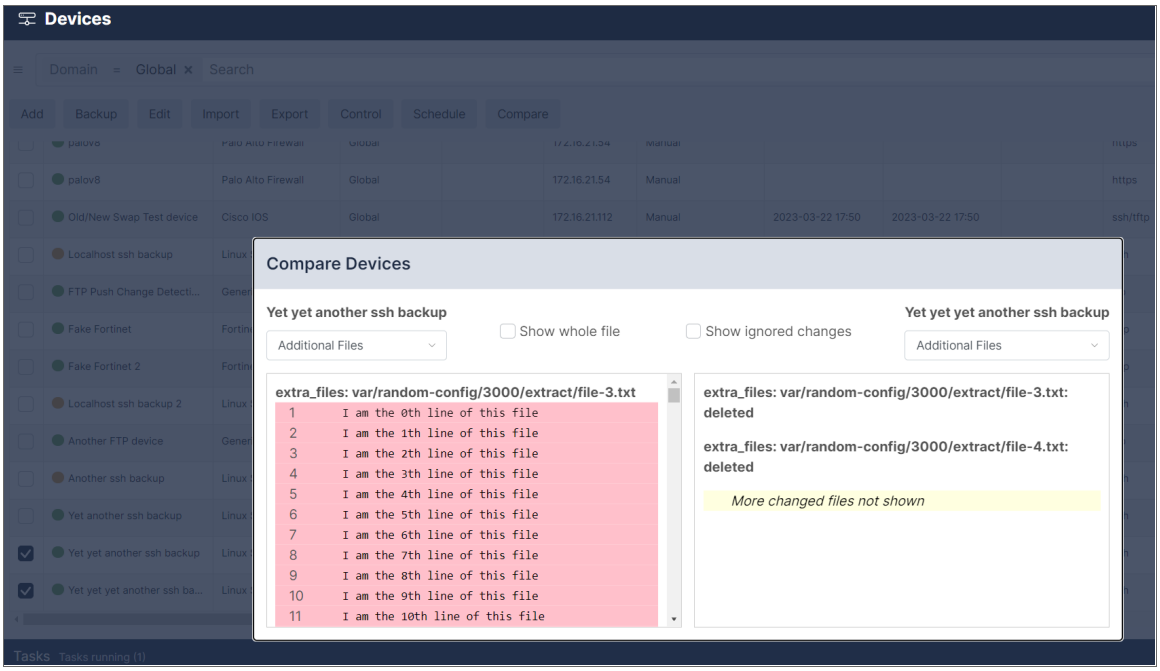
- Run-time variables, such as Cisco IOS ntp clock-period value
- Salted hashes, such as hashed passwords, certificates, keys
- Log files

You can now set Skylar Compliance to specifically ignore phrasing/words (like matching a regex), entire text-blocks (given the start/stop delimiters), and entire files (within tar/tgz/zip/xz config files).

To compare device configurations from the **Devices** page (Devices > Device List) or **[Configurations]** tab on the **Edit device** page:

1. Select the checkboxes next to the two devices/configurations you want to compare.
2. Click **[Compare]**. The **Compare Devices** window or **Compare Configurations** window appears.

3. You can view configuration changes between the selected files in this window. To help refine your viewing, you can select the ***Show ignored changes*** checkbox to view any "non-actual changes" and/or view the entire files by selecting ***Show whole file*** checkbox to review entire files.



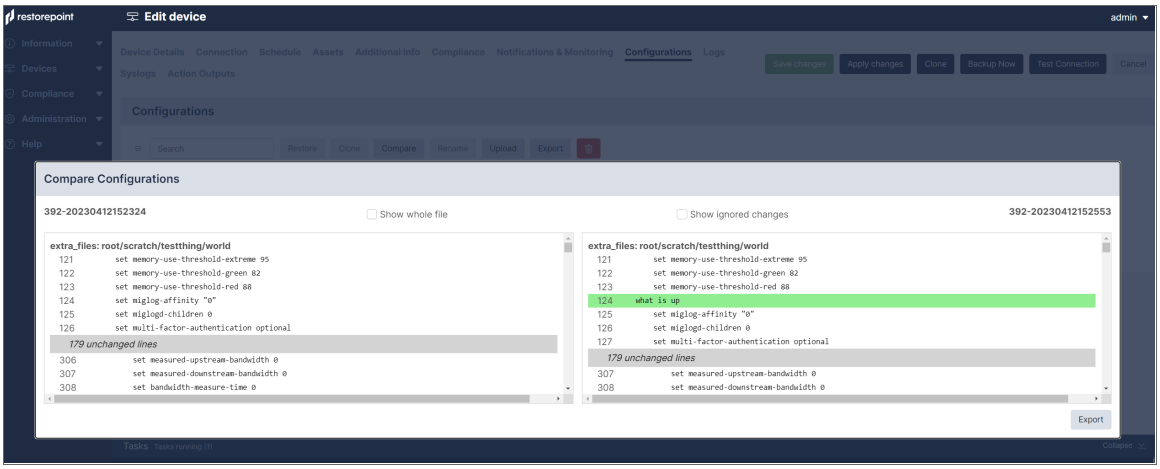
There are multiple parameters regarding specific config diff limits when you are comparing configs:

- 1000 lines is a cutoff for HTML diff before only changes are forced to be shown.
- 2000 lines is a cutoff for HTML diff when the diff gets truncated (for `rpcmd diff`, it is 5000).
- 2 million lines is a max number of lines for any of the two files before the diff is considered too large to be displayed.

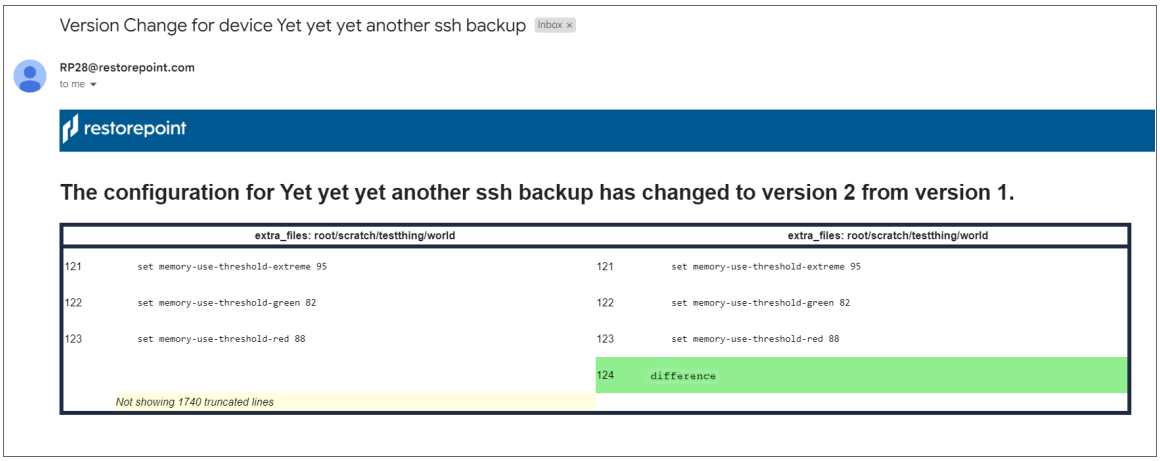
It is important to note that both 1000 lines and 2000 lines refer to the number of lines in the diff, not the configurations themselves."Diff" in this context refers to the whole set of lines to be displayed including unchanged lines, added lines, and deleted lines.

For example, if the produced diff has more than 1000 lines, it will be forced to show changes only.

Another example is if the diff has more than 2000 lines, it will be truncated and only the first 2000 lines of the diff will be used for generating the HTML output. The remainder or its changes will not be shown in the user interface. A message alerting you that the output was truncated will display at the bottom of the modal.



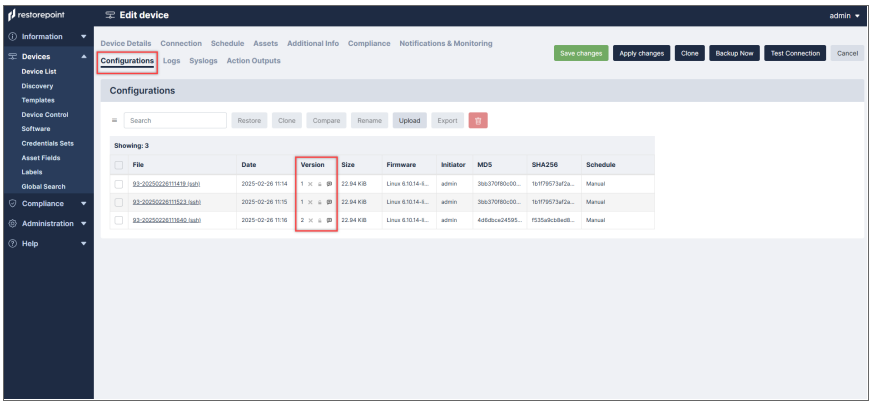
An Email Alert of your compare results is also sent when finished comparing configurations and/or devices.



Configuration Baselines

Configuration versions can be marked as *Baseline* by the *checkmark* symbol in the *Version* column of the **[Configurations]** tab. When you perform subsequent backups, an email notification is sent if the configuration differs from a baseline version. This allows you to quickly check if the current configuration is an approved version.

1. Go to the **Devices** page and select your device. The **Edit Device** page appears.
2. Click the **[Configurations]** tab and set the*Baseline* toggle (✔), *Retention* toggle (🔒), or *Comment* (💬) for your device in the ***Version*** column.
   - ***Baseline toggle on***. If you use the (✔), your configuration version will be marked as Baseline.
   - ***Baseline toggle off***. If you toggle to (✖), your configuration is not Baseline.



Backup File Operations

If a device configuration is a plain text file or a tar/tgz archive of text files, you can view the configuration contents by clicking the relevant tab or file name in the configuration page. If the configuration is an archive of text files, Skylar Compliance will attempt to unpack the archive and display each individual file. If the configuration is a binary file, or if the file is too large, Skylar Compliance will not display the contents.

From this page, you can copy this file to your local machine by clicking the **[Export]** button. After you export the file, you can use a text editor to edit the backup file, and then upload it back to Skylar Compliance using the **[Upload Backup]** button on the **[Configurations]** tab. You can push the edited configuration file to the device by clicking the **[Restore]** button.

Backup Failures

By default, after a device fails to back up, Skylar Compliance will retry the operation every hour until it succeeds, and it will send an error notification by email on every failed attempt. This behavior can be modified by changing the ***Failure Policy***, configured in the device **[Schedule]** tab:

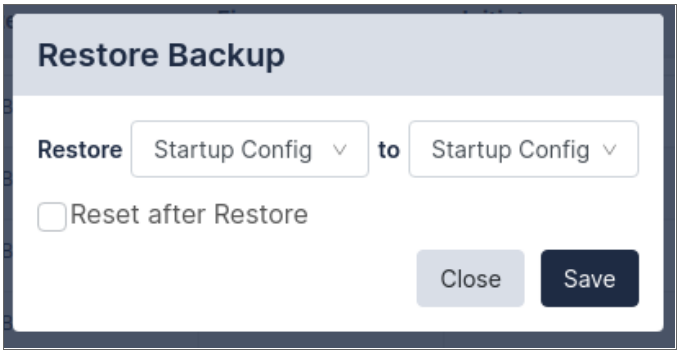
- From the ***Retry*** field, choose how many times to retry a failed backup. Backups are attempted every hour.
- Next, choose whether to revert to the set schedule or disable further backups when the last allowed failure occurs.
- Finally, choose when to be notified of a failure.

Restoring to an Existing Device

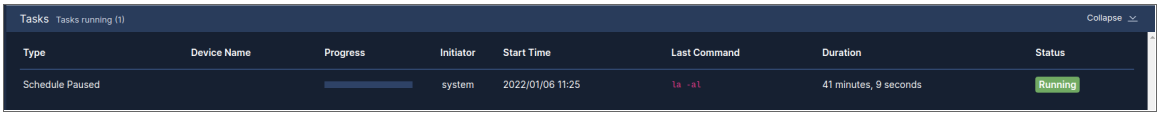
To restore a device:

1. Select ***Devices*** from the menu. Skylar Compliance displays the **Device List** page.
2. Click the entry in the ***Last Backup*** column next to the device you want to restore. Skylar Compliance displays all the available configurations.

3. Select a configuration by selecting its checkbox and click **[Restore]**. Skylar Compliance prompts you to confirm the restore operation. Depending on the device type, you may be prompted for additional options.



4. If the restore operation fails, you will see an activity in the activity display. You can click on the magnifying glass icon next to the progress bar to show a real-time progress log, which will aid in determining the cause of the failure. There is also a ***Transcript*** in the ***Logs*** tab for failed backups, which contains the details of the conversation with the device.



Restoring to a New Device

When a device is replaced, for instance due to failure, the following conditions must be met:

- The new device must run the same software version as the original.
- The new device must be configured with the same IP address and authentication details as the old device. Alternatively, you can temporarily change the IP addresses or credentials stored on Skylar Compliance to match those of the new device.
- If Skylar Compliance connects to the device using SSH, you may to need clear the SSH cache in Skylar Compliance in the **[Connection]** tab of **Device List**.

Cloning

The **Clone** button restores a configuration to a device that is different than the original, which produces a duplicate of the original device. This operation should be used with caution, as it may produce a duplicate IP address on your network.

Chapter 8

Templates

Overview

Templates are configurations that can be pushed to multiple devices. Each template can contain parameters, which are substituted for entered values for each device.

This chapter covers the following topics:

Templates *71*

Creating and Editing Templates *71*

Pushing Templates *72*

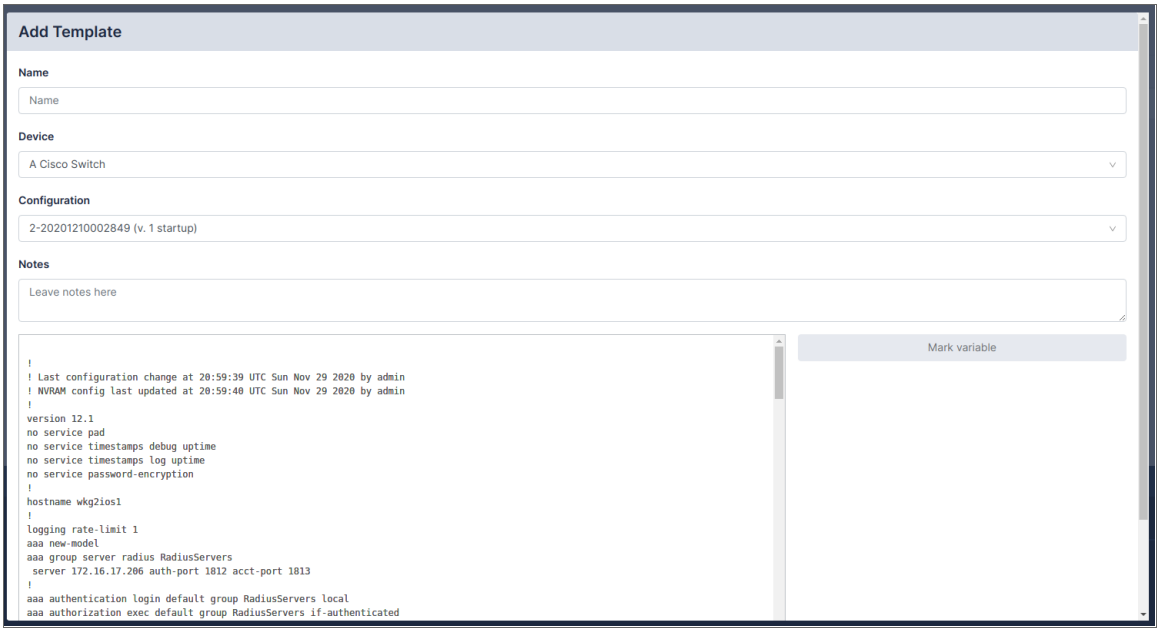
Templates

Templates are configurations that can be pushed to multiple devices. For example, during a large deployment of similarly configured devices.

Each template can contain parameters, which are substituted for entered values for each device. For example, a section might be marked “IP Address”, and the field will be applied when pushed to devices.

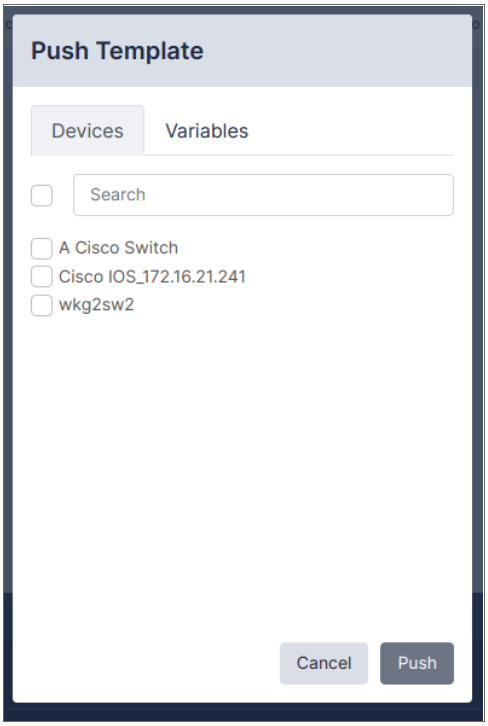
Creating and Editing Templates

1. Navigate to the **Template** page (Devices > Templates). Click **Add**, or click on an existing template name.
2. For new templates, select a device and configuration to base the template on.
3. After your template has loaded, select the configuration fields that you want to be substituted.
4. Click **Mark Variable** to name and store a highlighted value.
5. Once your template is created, the template values can be renamed or deleted with the relevant buttons.
6. Click **[OK]**. If you don’t provide a name and comment, a name and comment will be automatically generated.

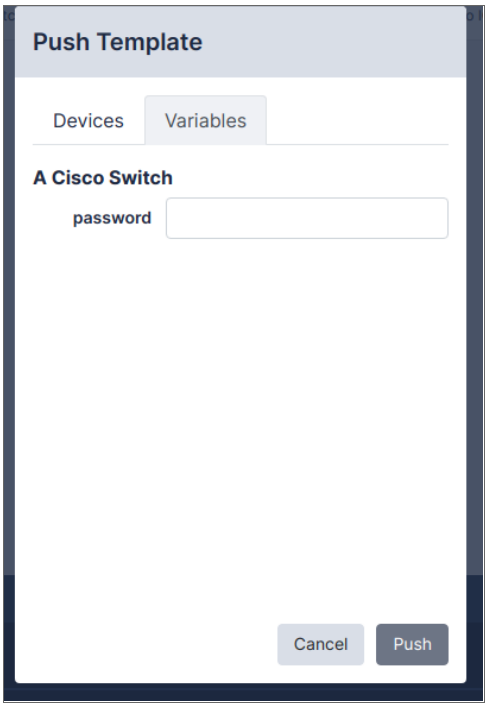


Pushing Templates

To push a template to a device, select the template from the **Template Management** page. Choose one or more devices using the device selector, and click **Push**.



If the template has any parameters, you must enter the values for each of the devices selected above:



Click **OK** to complete the operation.

Chapter 9

Device Control

Overview

This chapter describes how you can use Skylar Compliance to send a command-line interface (CLI) command to a device or group of devices and capture the output of the command. This tool can be used to perform a task concurrently on a group of devices.

This chapter covers the following topics:

Controlling a Device 75

Scheduled Actions 76

Lua Functions 78

Lua Applets 81

Controlling a Device

You can use Skylar Compliance to send a CLI command to a device or group of devices and capture the output of the command. This tool can be used to perform a task concurrently on a group of devices, such as changing the administrator password.

To use this function:

1. On the **Device List** page (Devices > Device List), click to check your device, and click the **[Control]** button. The **Control Devices** modal appears.
2. Select **New Action** from the drop-down menu, then complete the following fields:
    - ***Name***. Type a name for your action.
    - ***Description***. Give a unique descriptions for your action.
    - ***Type***. Select the type of command from the drop-down menu.
    - ***Variable Delimiter***. Select the variable delimiter from the drop-down menu.
    - ***Wait Duration (s)***. Type the number of seconds for Skylar Compliance to wait for a response from the device for each entered command.

      NOTE: Skylar Compliance will wait for the entire duration, even if the device outputs a response sooner than the configured duration. If multiple commands are entered, the wait duration should be configured to accommodate the command for which the device will take the most time to generate an output.

    - ***Log Transcript***. Select this checkbox to capture and store transcripts for successful device commands.

      NOTE: By default, transcripts are captured and stored only for failed device commands. Enabling the Log Transcript option will increase the number of stored records and overall storage usage in Skylar Compliance.

3. Type your commands in the text area.
4. Click **[Apply]** or **[Save]**.

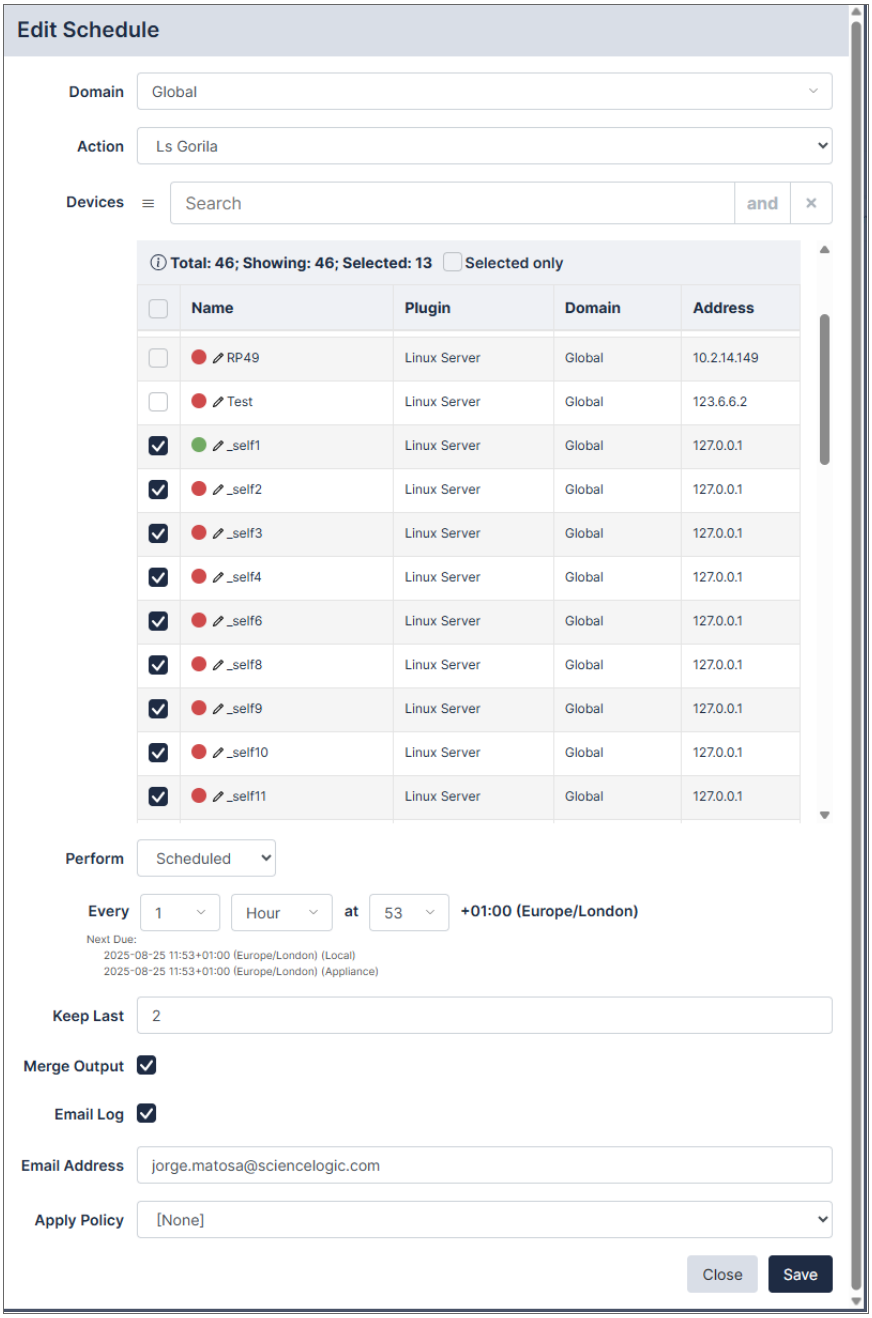
Device Control Actions can also be defined from the **Device Control** page (Devices > Device Control), by clicking **New Action**. If required, you can **Save** these commands as an **Action** for later execution, or for use in **Compliance Remediation**. Stored Actions can also be scheduled. For more information, see *Scheduled Actions*. Click **Perform** to execute the commands. Skylar Compliance will display the output of the commands for each of the selected devices. Device Control outputs are stored in the **Output** tab of the Device Control page.

Scheduled Actions

Actions can be scheduled and run automatically.

To add a new schedule to your device:

1. Go to the **Device Control** (Devices > Device Control) page and click the **[Schedule]** tab. Next, click the **[New Schedule]** button. The **New Schedule** modal appears.

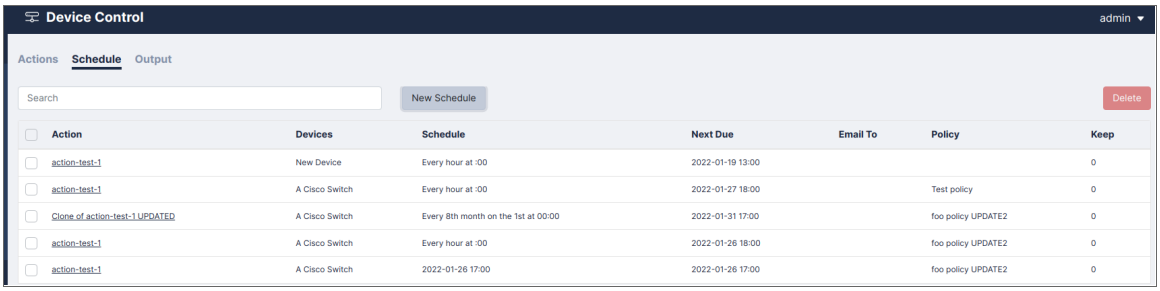


2. Complete the following fields:
   - ***Action***. Choose a option from the ***Actions*** drop-down field.
   - ***Devices***. Select the device or devices on which to perform the action
   - ***Perform***. Select a frequency, either *Scheduled* or *Once At* and a time interval or date.

- ***Keep Last***. Set the number of recent output runs you want to retain. Type "1" to keep all outputs from the most recent run. Type "2" to keep the outputs from the last two runs, and so on.
- ***Merge Output***. Select the ***Merge Output*** checkbox if you want to merge the output.
- ***Email Log***. Select the ***Email Log*** check box and enter an email address if you want to email the output of an action after execution.
- ***Apply Policy***. (Optional) Select a compliance policy to apply to the output of the action. For more information, see *Device Policies*.

NOTE: All logs are now stored in Skylar Compliance.

3. Click **[Save]** and the updated **Scheduled Action** page appears.



NOTE: Scheduled Actions cannot contain parameters.

Lua Functions

The **Device Control** page (Device > Device Control) features a more powerful way to interact with devices using the Lua programming language. Instead of sending a single command to a device, Lua offers control structures, loops, conditionals, match functions, and more. Using Lua, you can perform more complex tasks, including making decisions based on the device output.

The syntax does not require any specific programming experience or knowledge of markup languages like XML. For more information about Lua, see https://www.lua.org/docs.html.

Creating a Lua Function Action

To create a Lua Function action:

1. Go to the **Device Control** page (Devices > Device Control).
2. Click **[New Action]**. The **Add Command** modal appears.

3. Complete the following fields:
    - ***Name***. Type a name for your action.
    - ***Description***. Type a unique description for your action.
    - ***Type***. Select *Lua Functions* from the drop-down field.
    - ***Log Transcript***. Select this checkbox to capture and store transcripts for successful device commands.

> **NOTE:** By default, transcripts are captured and stored only for failed device commands. Enabling the ***Log Transcript*** option will increase the number of stored records and overall storage usage in Skylar Compliance.

4. Click **[+ Add Input]**. A new add input panel is added to the modal each time you click this button. Complete the following fields for each input:
    - ***Name***. Type a name for the input.
    - ***Source***. Select a source option from the drop-down field. The available options are:
        - *Text*. The normal, hardcoded variable added in the command.
        - *Prompt*. This variable is prompted and filled by the user when the action is performed.
        - *CSV*. This variable uses the format {name,value,deviceaddress/devicename}, where the value is the value of the variable, and the name is the unique name of the variable.
    - ***Value***. Enter the value of the variable you want to add to the command. This field is only editable if the ***Source*** type is *Text*.
    - ***Secret***. Select this box to stop the value from returning or displaying in the Skylar Compliance user interface. The value is also redacted from the output.



5. In the ***Function*** field, enter the code for the function(s) you want to use.

> **NOTE:** Your code will be wrapped in a function automatically. Do not wrap the code yourself.

6. From the **Devices** table, select the device(s) on which you want to execute the functions. You can use the ***Device Type*** and ***Domains*** drop-down fields to filter the devices available for selection.
7. Click **[Save]** to finalize your changes, or **[Perform]** to execute the commands immediately.

Error Handling for Lua Functions

You can use specific commands to help troubleshoot errors that might occur when executing Lua Function actions in Skylar Compliance.

The `error(message)` command sets an error on the current run of the action. This does not stop the action from executing. You can use the `return` command to stop the action from executing.

```
error("Something went wrong")
return
```

The `error()` command returns the current error string, or `""` if none has been defined.

```
if error() ~= "" then
    return
end
```

Below are two examples that use these commands for practical error handling.

Example: Device Rejected a Command

This example uses `error(message)` to set an error when the device output contains a known failure string. In the example, if `out` matches `"Invalid command"`, `error()` is called to record what went wrong, and then `return` is used to stop execution of the action. Without `return`, the action would continue running after setting the error.

```
sendget("show config", "$")
local out = before()
if out:match("Invalid command") then
    error("Device rejected 'show config'")
    return
end
print(out)
```

Example: Session Failure (Timeout, Connection Error)

This example uses `error()` with no arguments to read whether Skylar Compliance has already set an error. In the example, after `waitprompt()`, `error()` is checked before attempting to read the output of the action. If the session failed, there is nothing in `before()` worth outputting, so the action is exited early rather than outputting an empty or incomplete response.

```
send("show config")
waitprompt()
```

```
if error() ~= "" then
    return
end
print(before())
```

Lua Applets

Device Control (Device > Device Control) features a more powerful way to interact with devices using the Lua programming language. Instead of sending a single command to a device, Lua offers control structures loops, conditionals, match functions, etc. Using Lua, you can perform more complex tasks, including making decisions based on the device output.

To create a Lua action, go to the **Device Control** page (Devices > Device Control) and click **[New Action]**. Then select *Lua* from the **Type** drop-down menu.

The syntax is straightforward, and it does not require any specific programming experience or knowledge of markup languages like XML. For more information about Lua, see https://www.lua.org/docs.html.

IMPORTANT: Starting with the 5.6 20260715 maintenance release, you can no longer create device control actions using Lua Applets. Existing Lua Applet functions will continue to work, and you can use the *Lua Functions* action type to create new device control actions.

Using Parameters

You can use action parameters for different devices, using the format `$''parameter''$`, where `$` is the **Variable Delimiter** you've set for your Action.

For instance, to change the administrative password for a number of ScreenOS devices, select the devices and enter the command:

```
setadminpassword$password$
```

After you click **Perform,** you will be asked for a replacement string for each device. An unlimited number of parameters can be replaced this way.

NOTE: A parameter can only consist of letters, numbers, and the underscore character `_`. If the replacement string contains escape sequences (such as `\n`), they must be double-escaped (`\\n`).

Chapter 10

Software

Overview

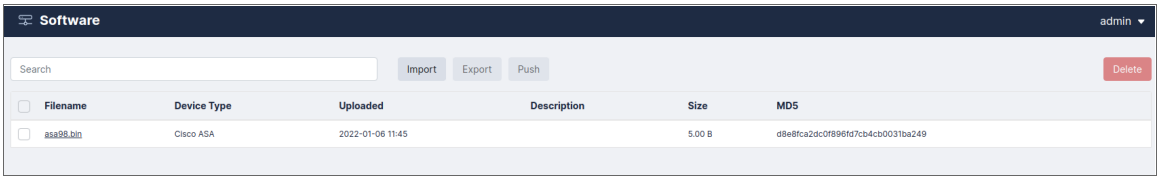
This chapter covers the following topics:

Software *83*

Skylar Compliance can be used as a repository for device firmware/software that allows you to upload files like firmware images and ISO images to the appliance. Software images can also be pushed to supported devices.

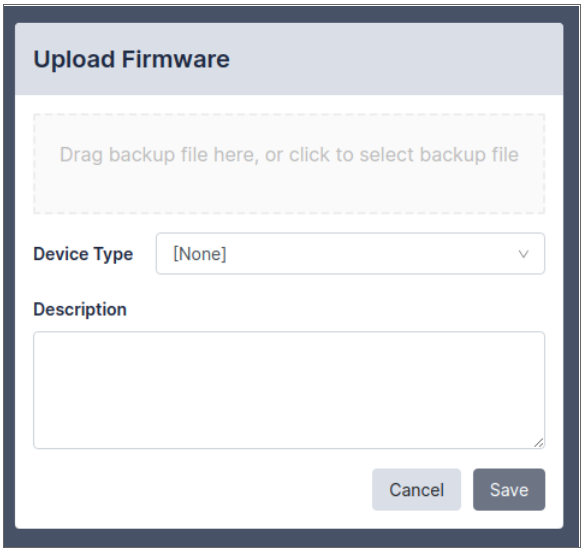
Software

Skylar Compliance can be used as a repository for device firmware/software that allows you to upload files like firmware images and ISO images to the appliance. Software images can also be pushed to supported devices.



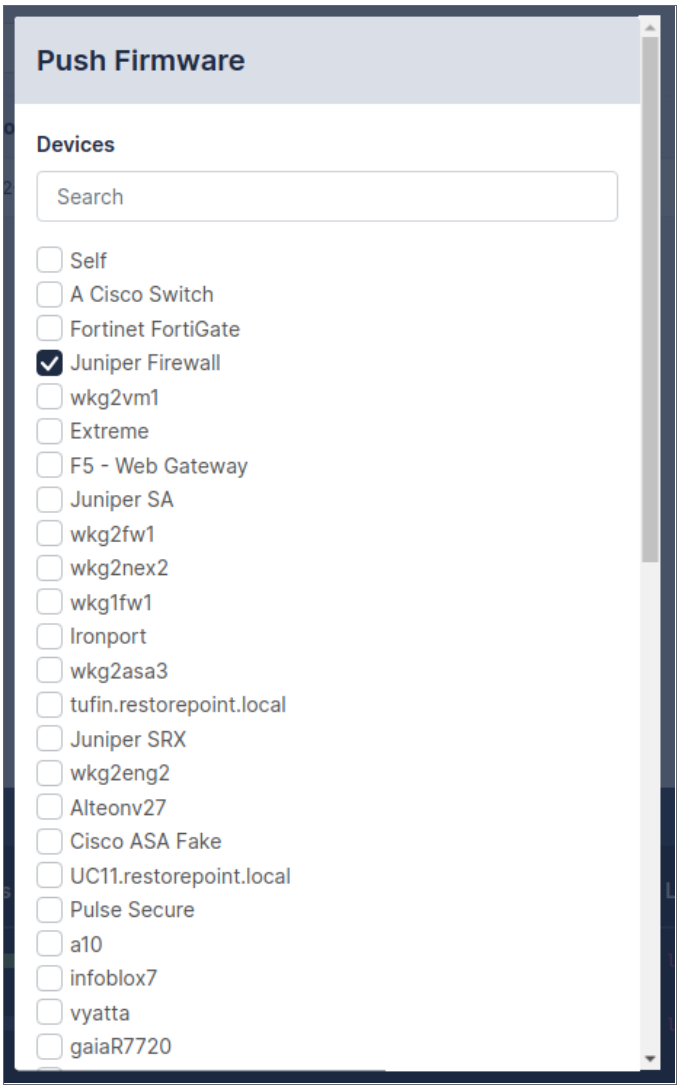
Uploading and Editing Firmware Images

1. Click **[Import]**, or an existing firmware name.
2. For new firmware, click the **[Browse]** button and navigate to the file from your hard drive.
3. Supply values in the **Device Type** and ***Description*** fields.
4. Click **[Save]**.



Pushing Firmware

Skylar Compliance can upgrade the firmware of a supported device using an image stored in the repository. Select a firmware image using the tickboxes, then click **[Push]**. Select the device from the menu, then click **[Push]** again; Skylar Compliance will perform the upgrade procedure recommended by the device vendor.



Please check the Plugin Guide (**Help > Plugin Guide**) for a list of devices that support this function.

Chapter 11

Credential Sets

Overview

Skylar Compliance can use predefined **Credential Sets** to authenticate to a device instead of individual usernames and passwords. Credential Sets are useful if several devices share the same authentication credentials.

This chapter covers the following topics:

Credential Sets *86*

Credential Sets

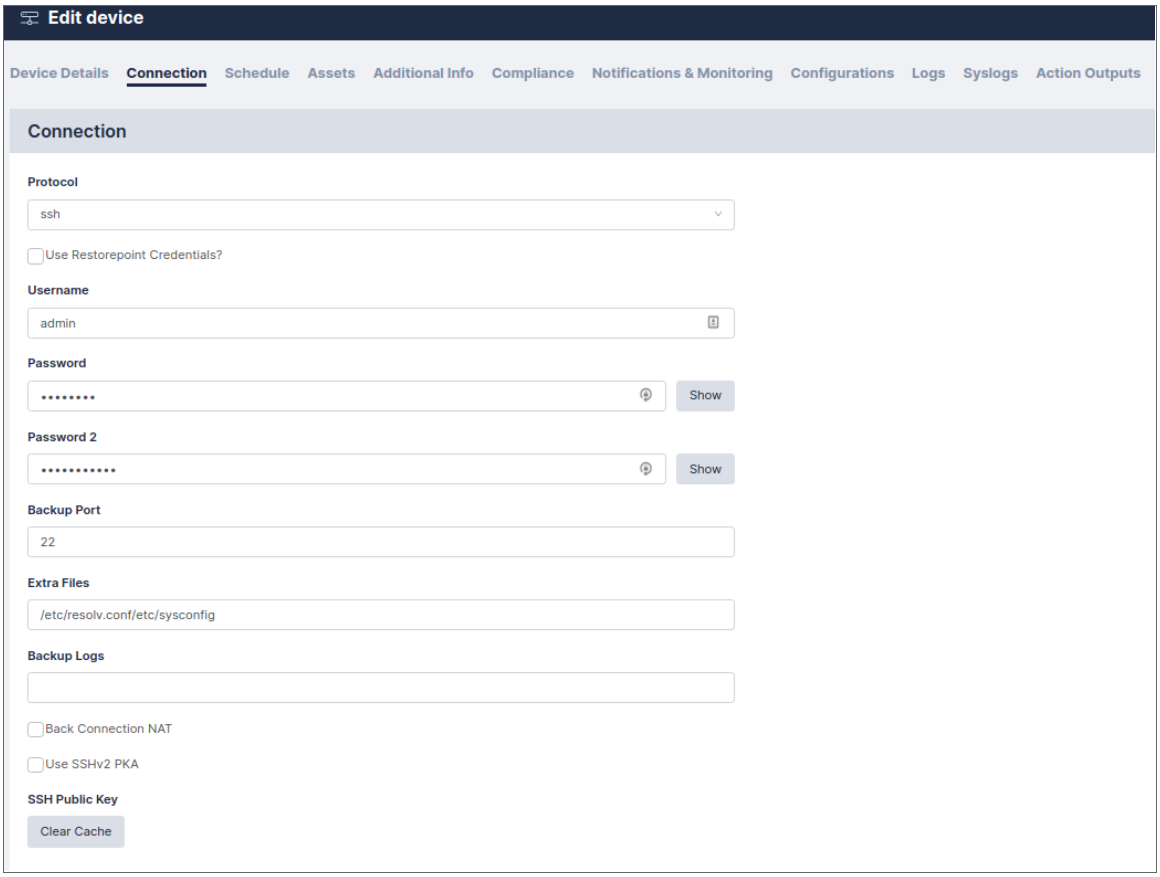
Skylar Compliance can use predefined **Credential Sets** to authenticate to a device instead of individual usernames and passwords. Credential Sets are useful if several devices share the same authentication credentials.

To create a Credential Set:

1. Go to the **Credential Sets** page (Devices > Credential Sets).
2. Click **[Add Set]**.
3. On the **[Details]** tab, complete the following fields:
   - ***Set Name***. Type a name for the credential.
   - ***Domain***. Select a domain to restrict the scope of this set to a particular domain. Otherwise choose *Global* to make this set available to all domains.
   - ***Username***. Type your device username.
   - ***Password***. Type your device password.
   - ***Password 2***. Type your second device password; typically this field is used for the enable password.
   - ***Add Custom Fields***. Click the **[Add Custom Fields]** button and type the name of the field you want to add in Skylar Compliance.
4. Click **[Save]**.

Using Credential Sets

To authenticate to a device using an existing credential set, leave the authentication details empty, check **Use Credentials**, and then select the correct credential set. Click **[Save]**.



To view which devices are currently using a selected Credential set, click the name on the **Devices > Credential Sets** page, and navigate to the **Devices** tab.

Integrating Skylar Compliance and CyberArk

You can integrate your CyberArk Vault with Skylar Compliance to populate credential information. To integrate CyberArk with a predefined Skylar Compliance device:

1. Identify the device and credential field that you want populated by the CyberArk Vault.
2. Go to the **Credential Sets** page (Devices > Credential Sets).
3. Click **[Add Set]** and supply values in the following fields:
    - ***Set Name***. Type a name for the credential.
    - ***Username***. Type your device username. If you want CyberArk to populate this value, leave this field blank.
    - ***Password***. Type your device password. If you want CyberArk to populate this value, leave this field blank.
    - ***Password 2***. Type your second device password; typically this field is used for the enable password. If you want CyberArk to populate this value, leave this field blank.

- ***Add Custom Fields***. Click the **[Add Custom Fields]** button and type the name of the field that you want to query from CyberArk so that CyberArk can populate the corresponding value in Skylar Compliance.

4. Click **[Save]**.
5. Go to the **System Settings** page (Administration > System Settings) and select the **[Security]** tab.
6. In the **Credential Providers** pane, click **[Add]**, and supply values in the following fields:
   - ***Name***. Type a name for the credential provider.
   - ***URL***. Enter the URL for your CyberArk Vault, specifically the GetPassword Web Service endpoint of the Central Credential Provider (CCP). You should not include any query parameters here, but add them to the ***Query Mappings*** section below.
   - ***Application ID***. Type the application ID that identifies Skylar Compliance application to your CyberArk vault.
   - ***Request Timeout (sec)***. Type a value, in seconds, after which Skylar Compliance will stop trying to communicate with CyberArk. Default value is 10 seconds.
   - ***RootCA Certificate***. Upload the PEM-encoded X.509 Root CA certificate required for secure TLS communication with CyberArk.
   - ***Client Certificate***. Upload the PEM-encoded X.509 client certificate required for secure TLS communication with CyberArk.
   - ***Client Key***. Upload the PEM-encoded client private key required for secure TLS communication with CyberArk.

     Query Mappings

     Click **[Add query mapping]** and supply values in the following fields:

   - ***Credential***. Select the credential that you created in steps 2-4 of this section.
   - ***Field***. Select the field that you want CyberArk to populate.
   - ***Query***. Type the query to retrieve field data from CyberArk. This is a required parameter to retrieve a secret value from the vault in conjunction with the ***Application ID***.

     Query. The query is a string with the following format:

     ```
     'Property=Value;Property=Value;...Propery=Value'
     ```

     where `Property` is one of the properties of the CyberArk account where the credentials are stored. Different types of accounts contain different properties, but most contain `UserName` and `Address`.

     For a successful query, you must include enough properties to return exactly one account, otherwise you will receive an error. For example:

     ```
     'safe=test;Database=hr;UserName=sa;Address=dbserver1.cyberark.local'
     ```

7. Click **[Save]**.
8. Go to the **Devices** page (Devices > Device List).
9. Select the checkbox to the left of your device and click **[Edit]**.
10. Go to the **[Connection]** tab.

11. Select the ***Use Restorepoint Credentials?*** checkbox and select the credential that you created in steps 2-4 of this section from the drop-down.
12. Click **[Save changes]**.

> **NOTE:** If the field does not populate in the user interface, you can click **[Backup Now]** when editing the device to view the device logs and the value that was populated from CyberArk.

Chapter 12

Asset Fields

Overview

In addition to the built-in Asset Management fields, you can also define custom fields. To do this, navigate to the **Assets Fields** page (**Devices > Asset Fields**). Custom fields can be of type ***Date***, ***Text*** (single-line), ***Textarea*** (multiple-line), and ***File***.

This chapter covers the following topics:

Asset Fields *91*

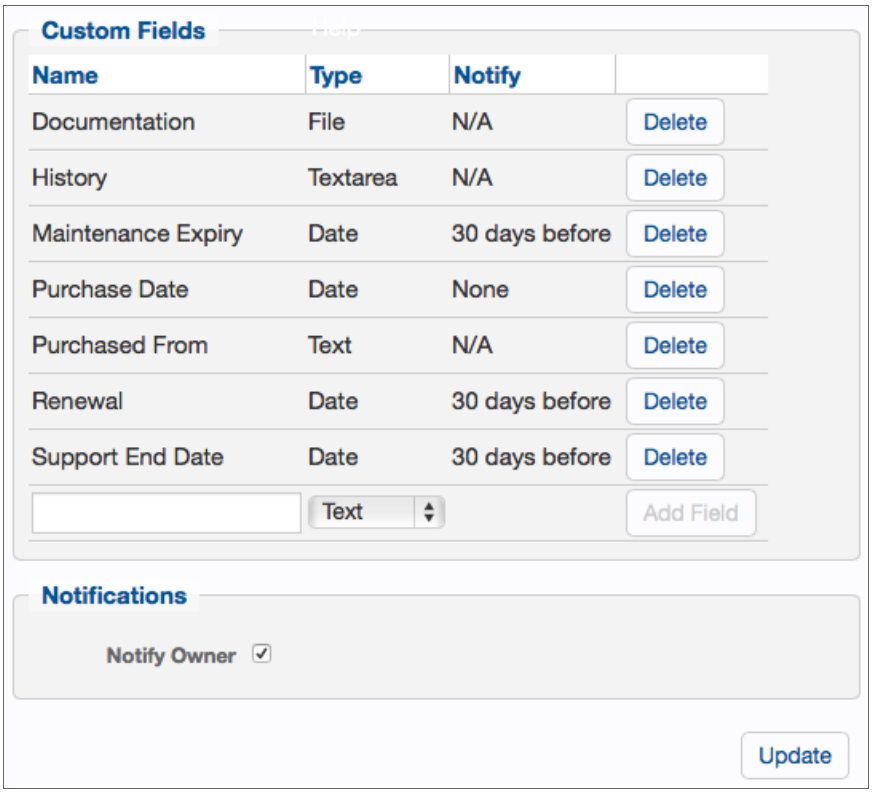
Asset Fields

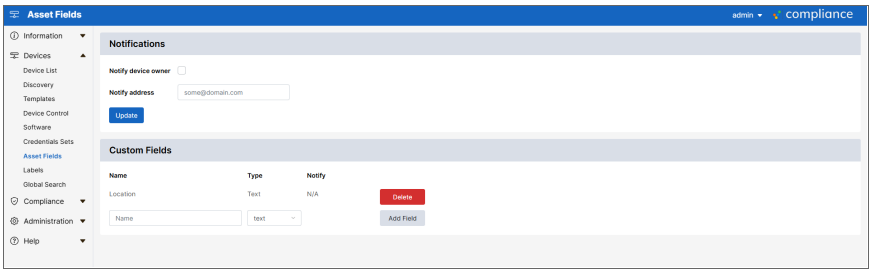
In addition to the built-in Asset Management fields, you can also define custom fields. To do this, navigate to the **Assets Fields** page (**Devices > Asset Fields**). Custom fields can be of type ***Date***, ***Text*** (single-line), ***Textarea*** (multiple-line), and ***File***.

Once defined, date fields can be set to give an **Expiry Notification**:

- 60 days before
- 30 days before
- When Reached

If set, an email is automatically sent to the device's owner on the specified expiration date. Expiry date is also used in reports.





Any custom fields defined in this page become immediately available in the **Assets** page of all devices managed by Skylar Compliance.

Chapter 13

Labels

Overview

You can use labels to filter and group devices. Users can create labels that are confined to a specific domain. When you create a new device or edit an existing device, you can set labels for that device.

This chapter covers the following topics:

Using Labels 94

Adding a Label from the Device Details Tab 94

Adding a Label from the Labels Page 95

Using Labels

When you create a new device or edit an existing device, you can set labels for that device.

For example, a user in an office consistently works with a set of devices because these devices are in that office. A label can be assigned to these devices. Use the label "Office Name"; this "Office Name" label, when set, can be used to filter and view any devices in the user's Device Table that are relevant devices to the "Office Name" label.

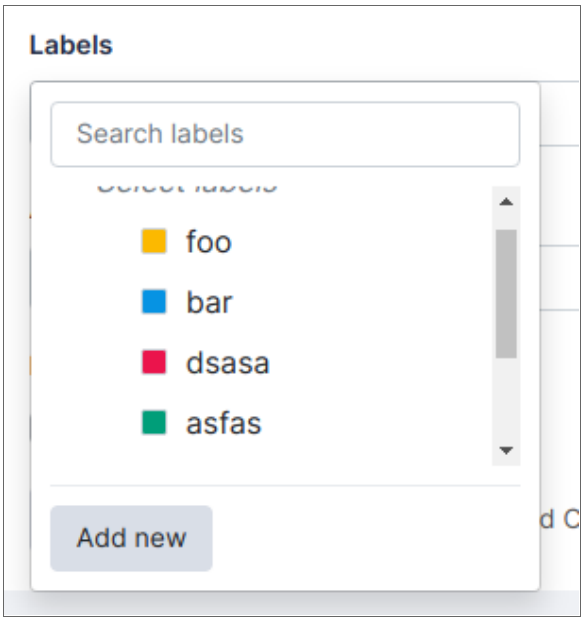
You can view and edit labels on the following pages:

- The ***Device Details*** tab when adding a device (Devices > Add) or editing a device (Devices > Select Device).
- The **Labels** page (Devices > Labels).

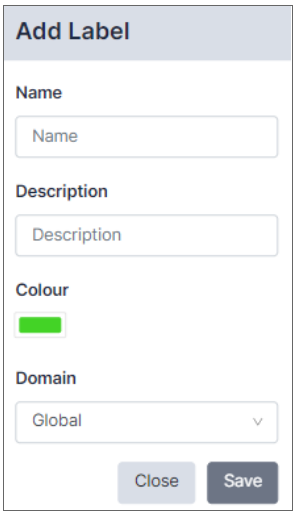
Adding a Label from the Device Details Tab

To add or edit a label from the **Device Details** tab:

1. Click your desired device from the Device Management page.
2. In the ***Device Details*** tab, click inside the **[Labels]** search field.
   You can search labels and/or add labels by clicking **[Add new]**.



3. Enter your new label's ***Name***, ***Description***, ***Colour***, and ***Domain***.

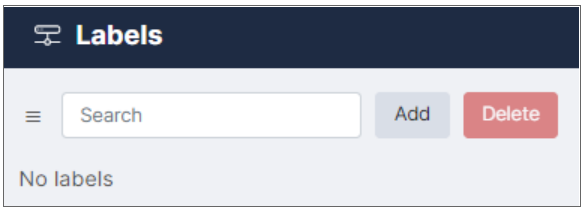


4. Click **[Save]**.

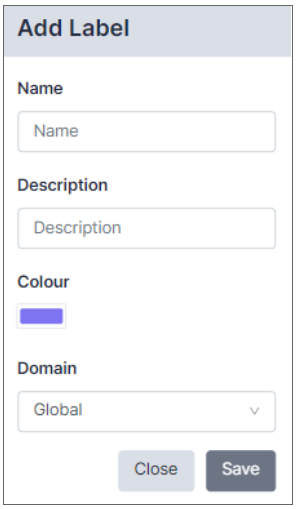
Adding a Label from the Labels Page

To add a label from the **Labels** page (Devices > Labels):

1. Click **[Add]**.



2. Enter your new label's ***Name***, ***Description***, ***Colour***, and ***Domain***.



3. Click **[Save]**.

These label options are also described in *Adding a new user*. For more information, see the Developer Documentation .

Chapter 14

Global Search

Overview

Skylar Compliance offers two types of searches to find the correct configuration backups on the **Global Search** page (Devices > Global Search). You can search via a string search or with a regular expression search.

This chapter covers the following topics:

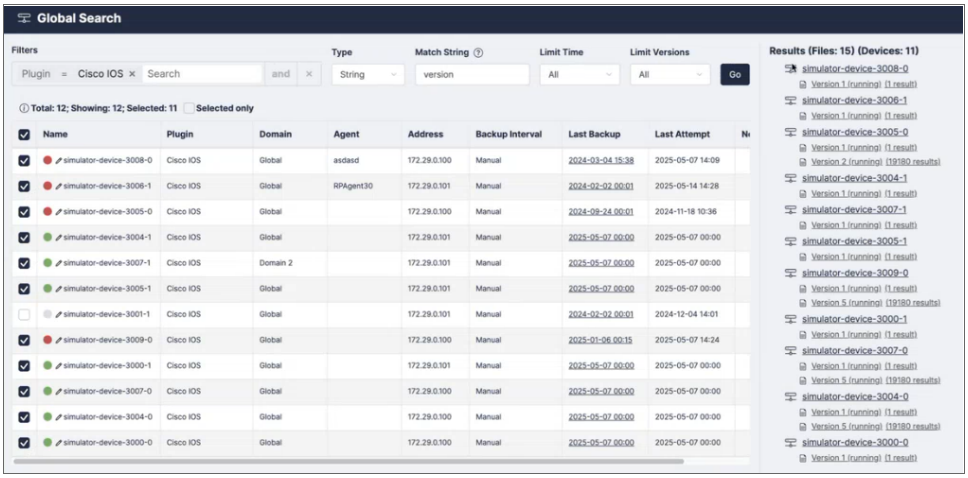
Global Search *98*

Global Search

Skylar Compliance offers two types of searches to find the correct configuration backups on the **Global Search** page (Devices > Global Search). You can search via a string search or with a regular expression search.

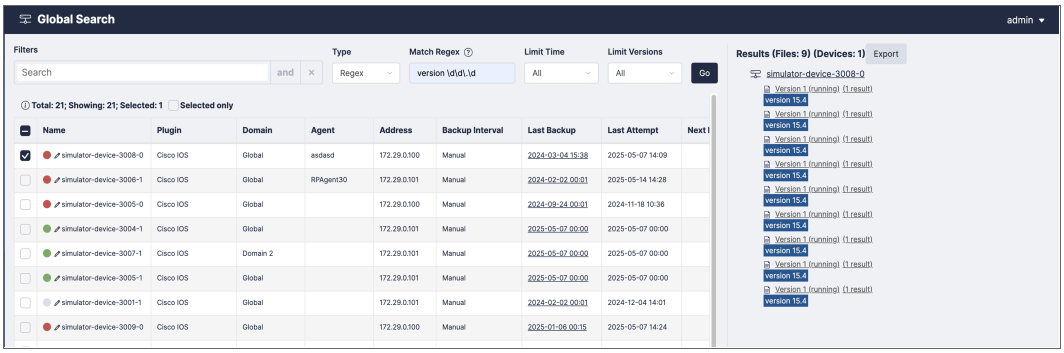
To perform a string search:

1. Select the search criteria in the ***Filter*** field that you want to search for. Click the *and/or* operator toggle to narrow your search. The ***Filter*** field will filter as you select or type your search criteria and will update the results in the table below the search modal.
2. Select *String* from the drop-down menu and type in any text you want to match specifically in the ***Match String*** field. For more information, click (?) for String Search Criteria help.
3. If desired, select a time limit and version limit from the ***Limit Time*** and ***Limit Versions*** drop-down menus.
4. Select the devices you want to search and click **[Go]**. The Global Search will display a preview of every search result in the **Results** pane on the right.



To perform Regex search:

1. Select *Regex* from the drop-down menu to search by regular expression for a more advanced search.
2. Type in any text you want to match specifically in the ***Match Regex*** field. For more information, click (?) for Regex Search Criteria help.
3. If desired, select a time limit and version limit from the ***Limit Time*** and ***Limit Versions*** drop-down menus.
4. Select the devices you want to search and click **[Go]**. The Global Search will display a preview of every search result in the **Results** pane on the right.



5. Select the results that you want to export and click the **[Export]** button to export to a .csv file.

Chapter

15

Device Policies (Policy Library and Rules Library)

Overview

You can use Skylar Compliance to create rules and policies to verify that your devices comply with corporate or regulatory guidelines.

A ***rule*** is a pattern that is applied to configurations or device firmware version to test whether the configurations or firmware contain a certain phrase or regular expressions, or if they match an existing device template. If the tests fail, a compliance violation is triggered and an email alert is sent to the device owner. A ***policy*** is a group of one or more rules.

This chapter covers the following topics:

Device Policies and Rules *101*

The Policies Tab *101*

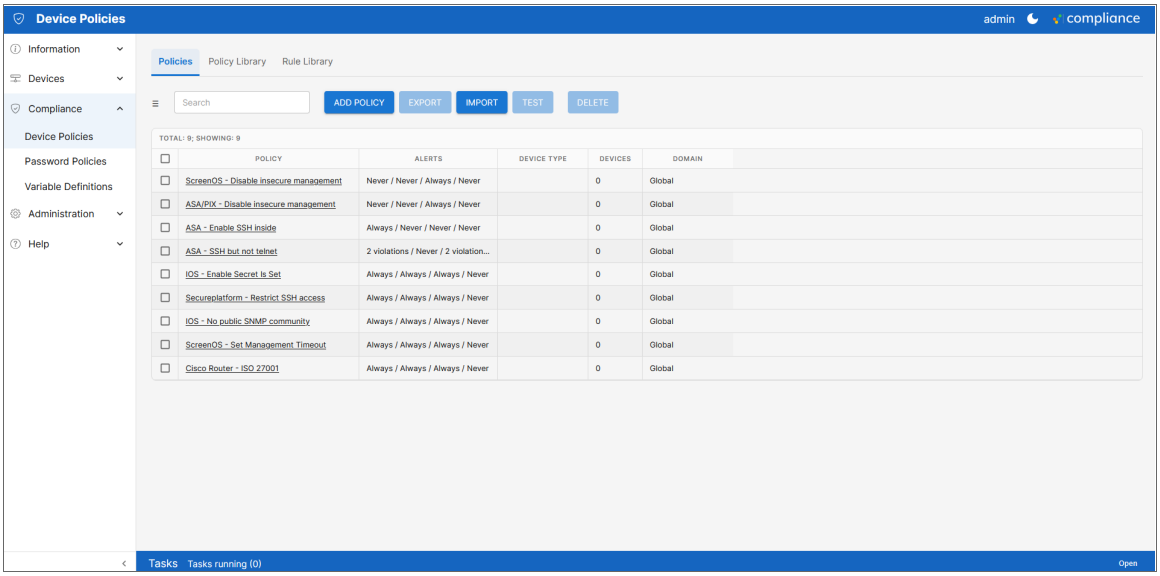
The Policy Library Tab *103*

The Rule Library Tab *118*

Lua Functions *123*

Device Policies and Rules

You can use the three tabs on the **Device Policies** page (Compliance > Device Policies) to create and use configuration compliance rules and policies that you can assign to devices.



A ***rule*** is a pattern that is applied to configurations or device firmware version to test whether the configurations or firmware contain a certain phrase or regular expressions, or if they match an existing device template. A rule can also be applied to or tested against a command output. If the tests fail, a compliance violation is triggered and an email alert is sent to the device owner.

A ***policy*** is a group of one or more rules. You can create Configuration Policies for devices that have a text configuration file or a TGZ archive of text configuration files.

The Policies Tab

The **[Policies]** tab on the **Device Policies** page (Compliance > Device Policies) contains a list of the currently installed compliance policies for your devices. This tab displays by default when you first go to the **Device Policies** page.

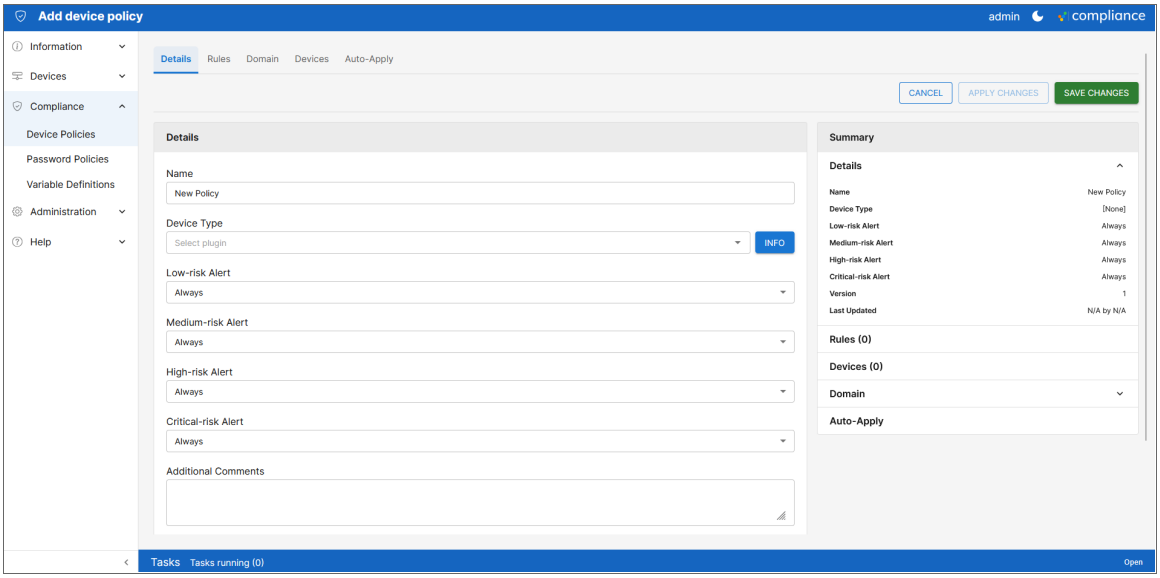
Select a policy from the list to make changes to the policy on the **Edit device policy** page. For more information, see *Editing a Device Policy*.

Creating a Device Policy

After you have created one or more rules, or if you want to use one or more of the existing rules, you can create a new device policy.

To create a new device policy:

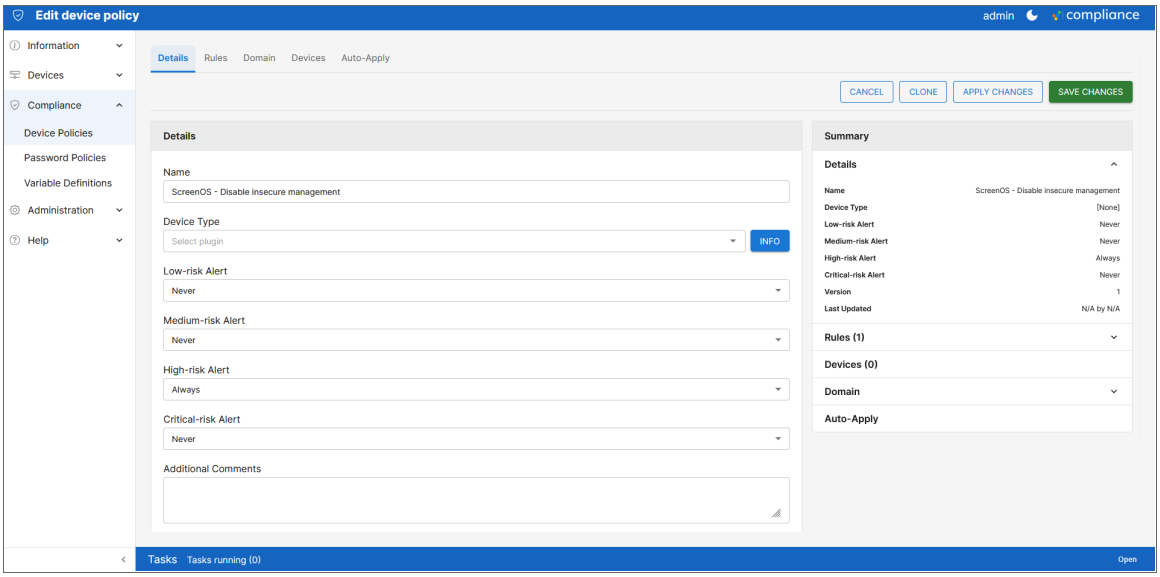
1. On the **Device Policies** page (Compliance > Device Policies), click **[Add Policy]**. An **Add device policy** page appears.



2. Enter the following details on the **[Details]** tab:
   - ***Name***. Type a name for the new device policy.
   - ***Device Type***. Select a device type from the drop-down field. Click the **[Info]** button to view a pop-up with more information about the device you selected.
   - ***Low-risk Alert***. Choose the criteria for low risk alerts to generate from the drop-down field.
   - ***Medium-risk Alert***. Choose the criteria for medium risk alerts to generate from the drop-down field.
   - ***High-risk Alert***. Choose the criteria for high risk alerts to generate from the drop-down field.
   - ***Critical-risk Alert***. Choose the criteria for critical risk alerts to generate from the drop-down field.
   - ***Additional Comments***. Add any other information you might need for this policy.
   - ***Log Transcript***. Enable this option to capture and store transcripts for all compliance rules. You can view the transcript on the **Logs** page (Information > Logs) or on the **[Logs]** tab of a device. Transcripts are not stored by default. Using this option will increase the number of stored records and overall storage usage.
3. Click **[Save Changes]**.

Editing a Device Policy

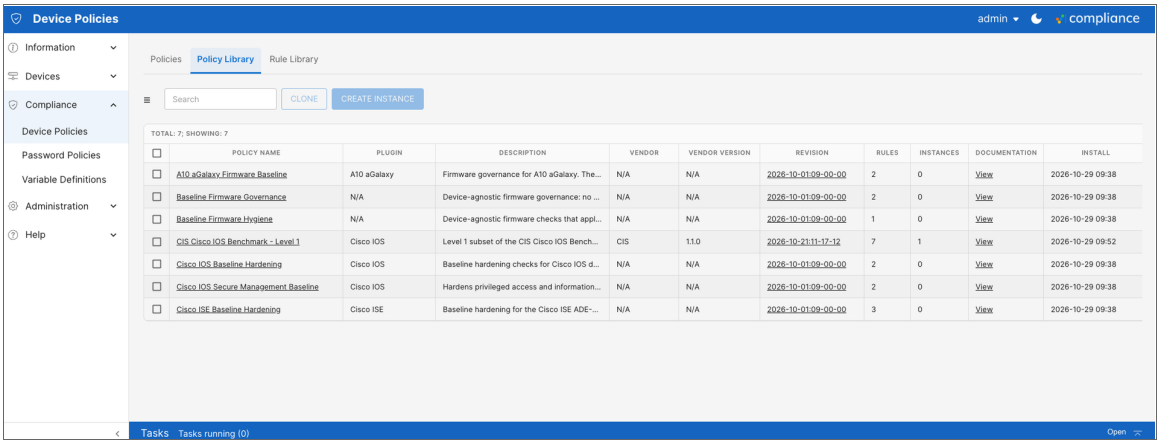
When you click the name of a policy, an **Edit device policy** page for that policy appears, where you can edit or clone (make a copy) of that policy.



The Policy Library Tab

The **[Policy Library]** tab on the **Device Policies** page (Compliance > Device Policies > Policy Library) provides access to the packaged policies from ScienceLogic installed on the system. These read-only policies, also called ***library policies***, are delivered with compliance updates (Administration > Software Updates).

Library policies contain a set of rules, such as hardening baselines, for one device type or for all device types, along with a changelog and documentation that explains what the rules do. ScienceLogic maintains these library policies through policy library updates.



The **[Policy Library]** tab lists all of the library policies installed on the appliance. Library policies do not belong to a domain. Every domain sees the same list.

For each library policy, the list shows:

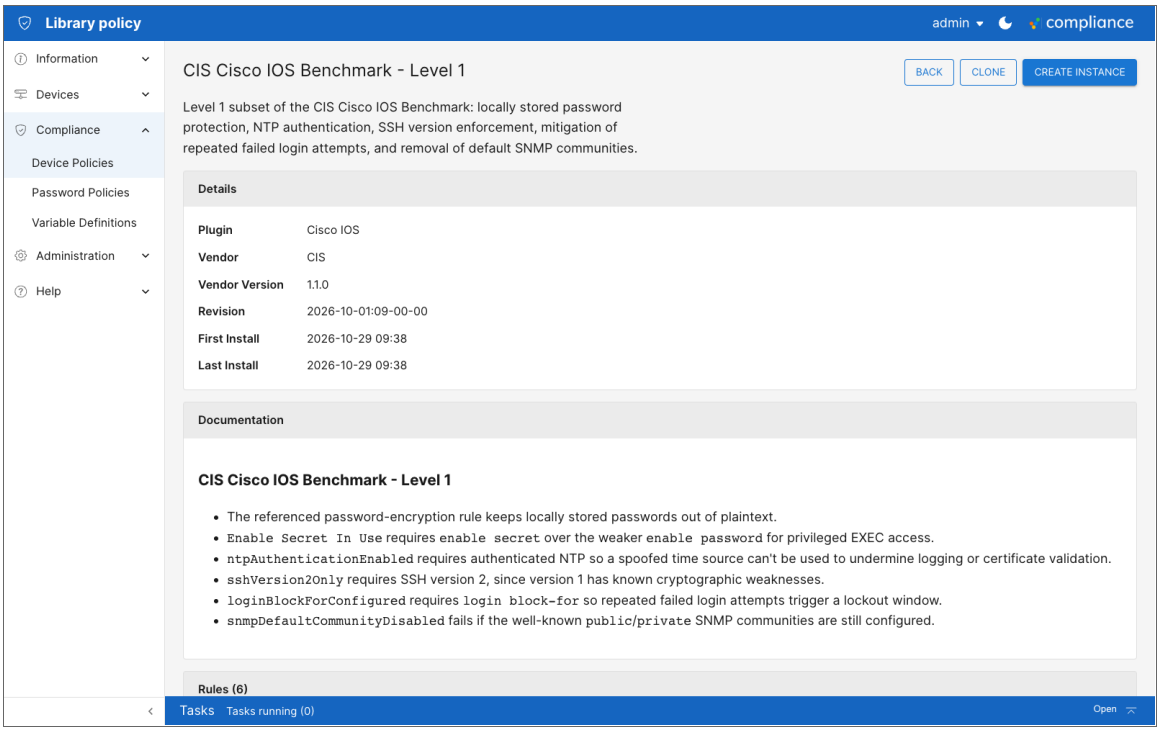
- ***Policy Name***. Select a name to open the library policy page.
- ***Plugin***. The device type the policy applies to. *N/A* means the policy applies to any device type.
- ***Description***. A summary of what the policy checks.
- ***Vendor***. The organization whose benchmark or guide the policy is based on, such as *CIS*. *N/A* displays for policies authored by ScienceLogic.
- ***Vendor Version***. The version of the vendor's benchmark or guide that the policy is based on.
- ***Revision***. When ScienceLogic published the installed version of the policy. The revision is the same on every appliance. Select it to see the policy's changelog.
- ***Rules***. The number of rules in the policy.
- ***Instances***. The number of instances of the policy in the domains you can access.
- ***Documentation***. Click **View** to read the policy's documentation.
- ***Install***. When the installed version of the policy was installed on this appliance.

If the **[Policy Library]** tab is empty, no policy library update has been installed on the appliance yet. For more information, see *Policy Library Updates*.

> **NOTE:** You need the *View Device Policy* permission to see the contents of the **[Policy Library]** tab, and the *Modify Device Policy* permission to create instances and clones.

Viewing a Library Policy

To view the details of a library policy, click the name of the policy from the **[Policy Library]** tab. A **Library policy** page appears:



Library policy pages include the following sections:

- **Details**. The plugin, vendor, vendor version, and revision of the policy, when the appliance first received the policy (***First Install***), and when its current revision was installed (***Last Install***).
- **Documentation**. Notes from ScienceLogic about what the policy checks and why.
- **Rules**. The rules in the policy, with the name and severity that the policy gives each rule, and the type and group for each rule. Select a rule name to view the rule. You cannot edit it.
- **Changelog**. The changes ScienceLogic made in each revision of the policy.
- **Instances**. The instances of the policy in the domains you can access. Select an instance to edit it. This section appears once the policy has at least one instance.

The [Clone] and [Create Instance] buttons at the top of the page let you *clone* (copy) or *create* a policy based on that library policy.

Creating an Instance of a Library Policy

A library policy is a read-only template. To use a library policy, you need to select the library policy and then create a device policy from it, either as an instance or as a clone:

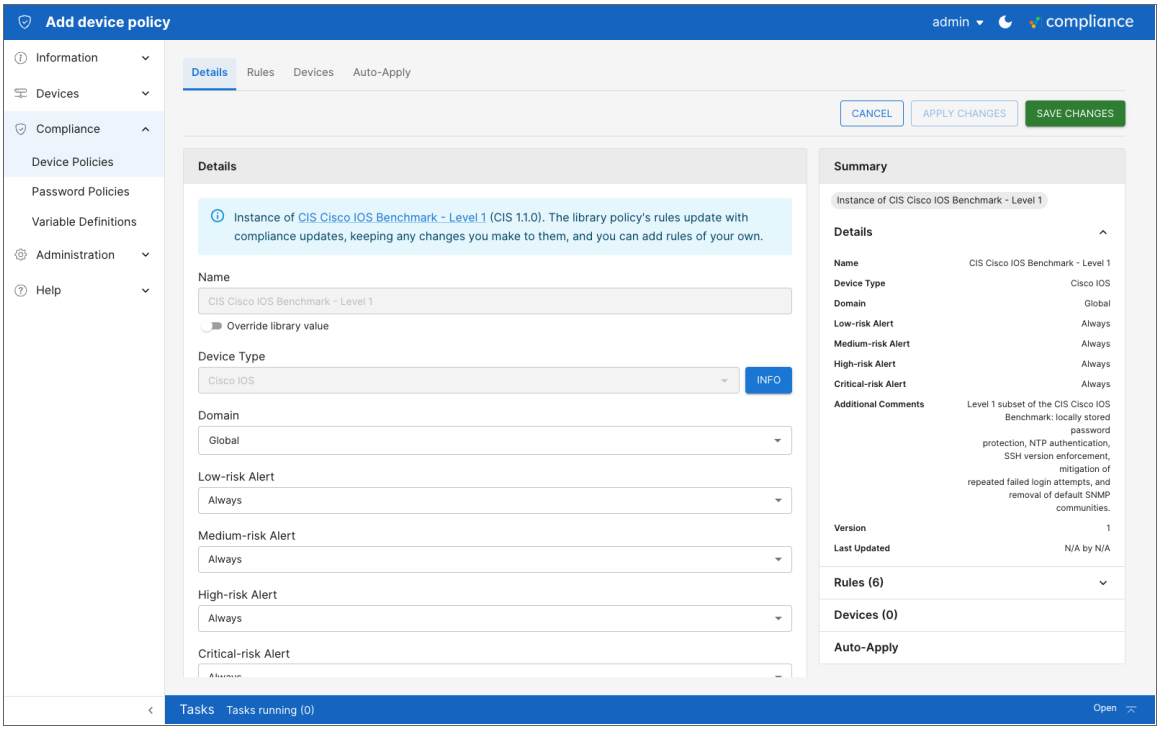
- An ***instance*** of a policy stays linked to its library policy. When ScienceLogic updates the library policy, the instance is updated too, and the changes you made to the instance are kept. For more information, see the following procedure.
- A ***clone*** of a policy is an independent copy of the library policy. Its rules become your own rules, and policy library updates never change it. For more information, see *cloning an instance.*

TIP: Create an *instance* to keep up with changes that ScienceLogic makes to a benchmark. Create a *clone* when you need to change the policy beyond what an instance allows, for example to remove rules permanently or to use the rules with another device type.

To create an instance of a library policy:

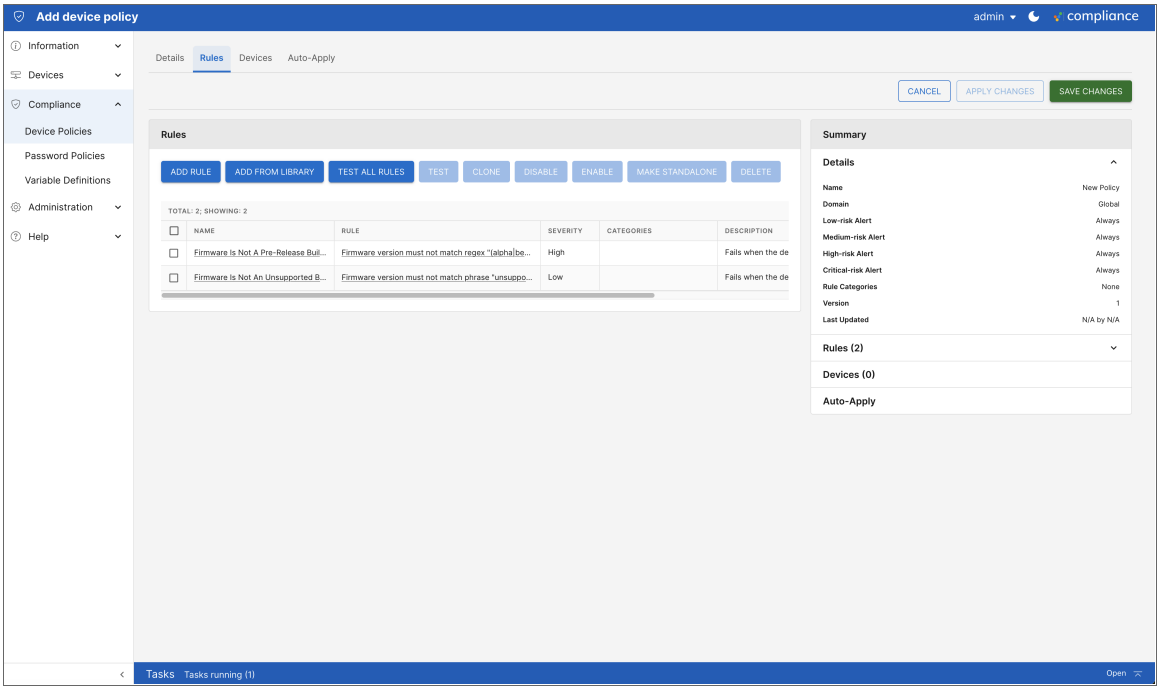
1. Go to the **[Policy Library]** tab on the **Device Policies** page (Compliance > Device Policies > Policy Library).
2. Click the checkbox next to the library policy you want to use and click **[Create Instance]**. You can also click **[Create Instance]** on the library policy page.

   The **Add device policy** page appears, with fields already filled in from the library policy. A banner names the library policy aligned with the instance; click **Open in the Rule Library** to see the rule on the **[Rule Library]** tab.



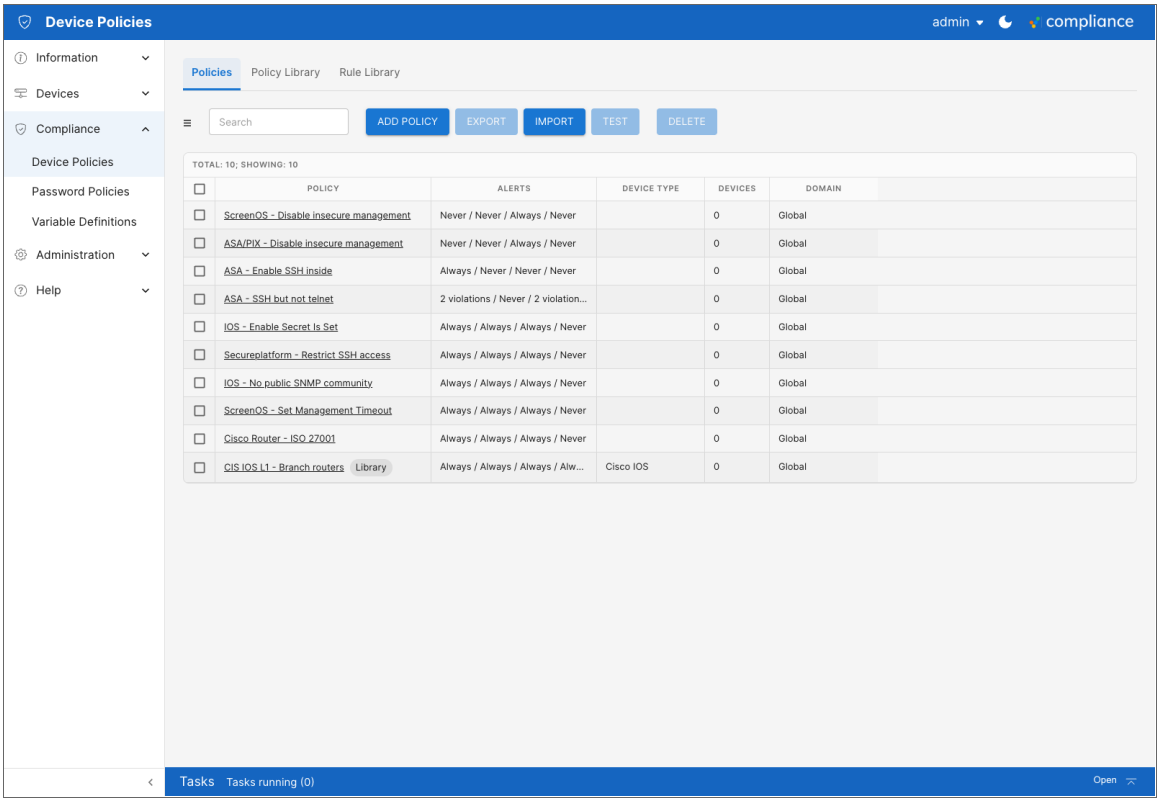
3. Complete the fields on the page:
   - ***Name*** and ***Additional Comments*** show the library policy name and description. To use your own, turn on ***Override library value*** under the field, and then edit the field. For more information, see *Instance Name and Comments*.
   - ***Device Type*** is set to the library policy's device type and cannot be changed. To use a library policy's rules with another device type, clone the library policy instead.
   - Complete the remaining fields, such as ***Domain*** and the alert thresholds, as you would for any device policy.

4. If needed, click the **[Rules]** tab to review the rules that the instance gets from the library policy. All of these rules are enabled in a new instance. You can add rules of your own by clicking **[Add Rule]**. **[Add from Library]** becomes available after you save the policy.



5. If needed, select devices on the **[Devices]** tab, or set up the **[Auto-Apply]** tab.

6. Click **[Save Changes]**. The new policy appears on the **[Policies]** tab with a *Library* tag. Select the tag to open the library policy.



TIP: You can create several instances of the same library policy. For example, you can create one for each domain, or one for each group of devices that needs different alert thresholds.

Editing an Instance

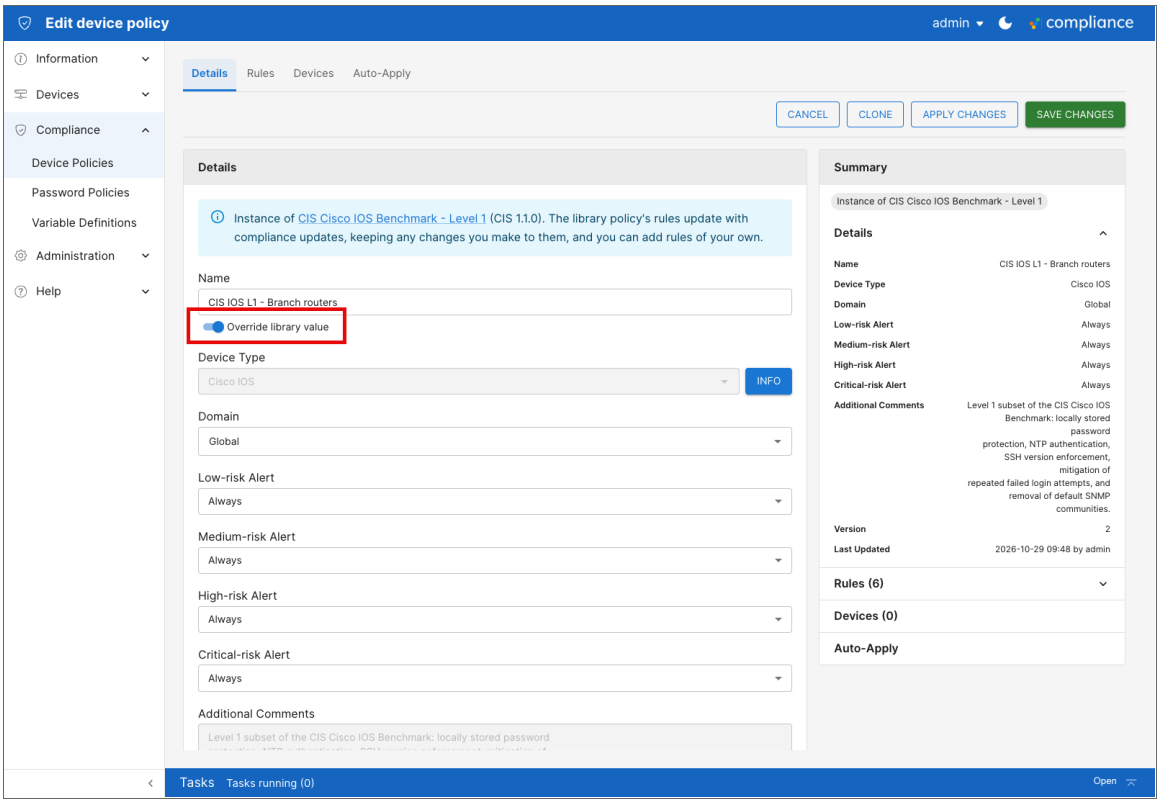
You edit an instance the same way as any other device policy, with the differences described in this section.

Instance Name and Comments

The ***Override library value*** switch under the ***Name*** and ***Additional Comments*** fields controls where each value comes from:

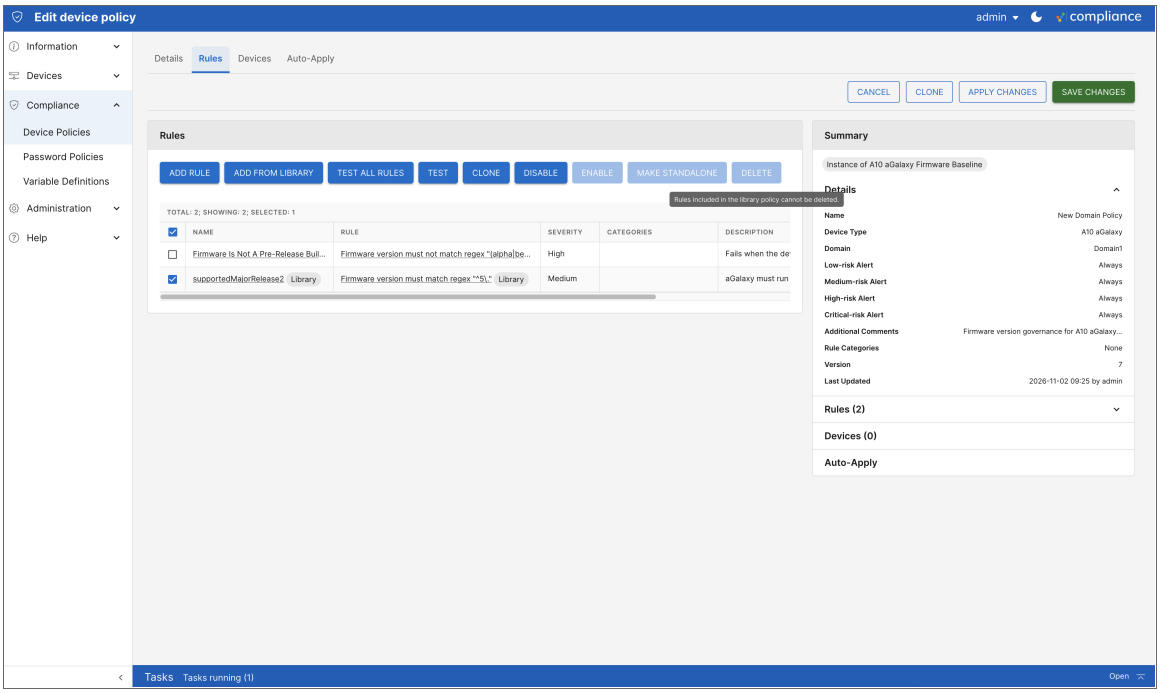
- *Off*. The field shows the library policy's name or description, and you cannot edit it. When an update renames the library policy or changes its description, the instance follows.
- *On*. The field holds your own value, and updates do not change it.

If you turn the switch off again, the field returns to the library policy's current value.



Rules from the Library Policy

On the **[Rules]** tab of an instance, the rules that come from the library policy have a *Library* tag. You cannot delete these rules. When one of them is selected, the **[Delete]** button is unavailable.

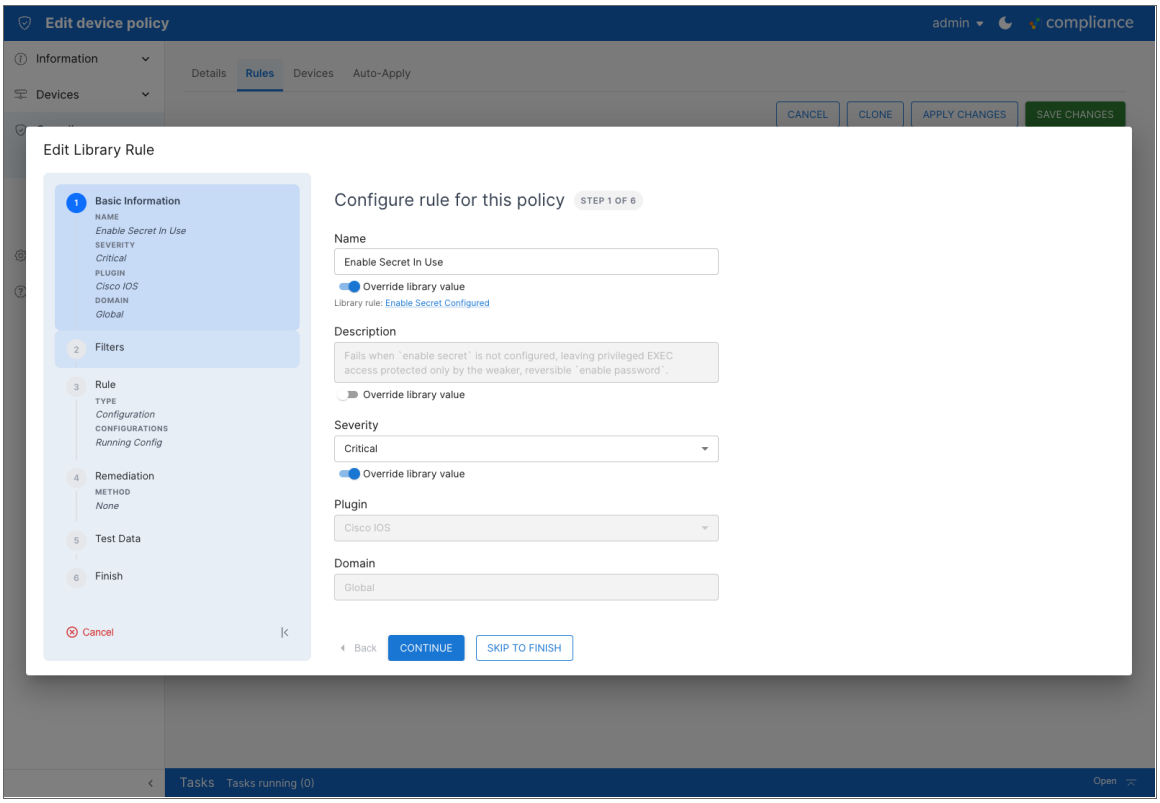


Instead of deleting a rule from a library policy, you can:

- Disable a rule that does not apply to your network. For more information, see *Disabling Rules*.
- Change how a rule is applied in this policy. Select the rule's name to open the **Edit Library Rule** window. Each setting that you can change has an ***Override library value*** switch. While a switch is off, the setting comes from the library and follows updates. Turn a switch on to give the setting your own value in this policy. You can override the rule's name, description, severity, and remediation. Depending on the rule, you can also change its files and ignored lines, and add your own filters, configuration types, and test data. Work through the steps, or click **[Skip to Finish]**, and then click **[Save]**.

  Your changes apply only to this policy. The rule itself, and other policies that use the rule, are not affected.

  If the library policy already renames the rule or changes its severity, the switch for that setting is already on, and the rule's name in the Rule Library appears under the ***Name*** field.



You can also add rules of your own to an instance with **[Add Rule]** or **[Add from Library]**. These rules belong to the instance: you can edit or delete them, and policy library updates do not change them. **[Make Standalone]** is not available for rules from the library policy, because they are already library rules.

Cloning an Instance

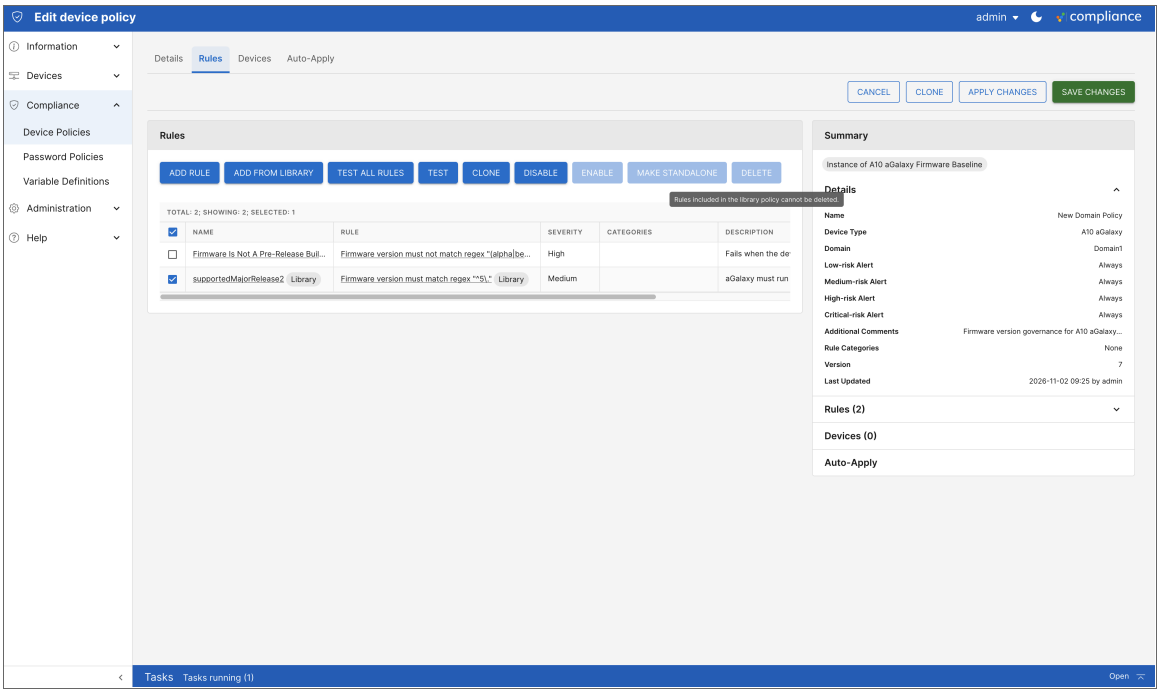
When you click **[Clone]** at the top of an instance's page, you create another instance of the same library policy. The new instance starts with a copy of the source instance's rules, including your changes to the library policy's rules and which rules are disabled. Until you save the new instance, you cannot disable or delete its library rules.

Disabling Rules

You can disable a rule in any device policy, including an instance, to stop the rule from being checked without deleting it. Disabling is useful for rules in a library policy that do not apply to your network.

To disable or enable rules:

1. Open the device policy and select the **[Rules]** tab.
2. Select the checkbox for one or more rules.
3. Click **[Disable]** or **[Enable]**. In a saved policy, the change takes effect immediately.



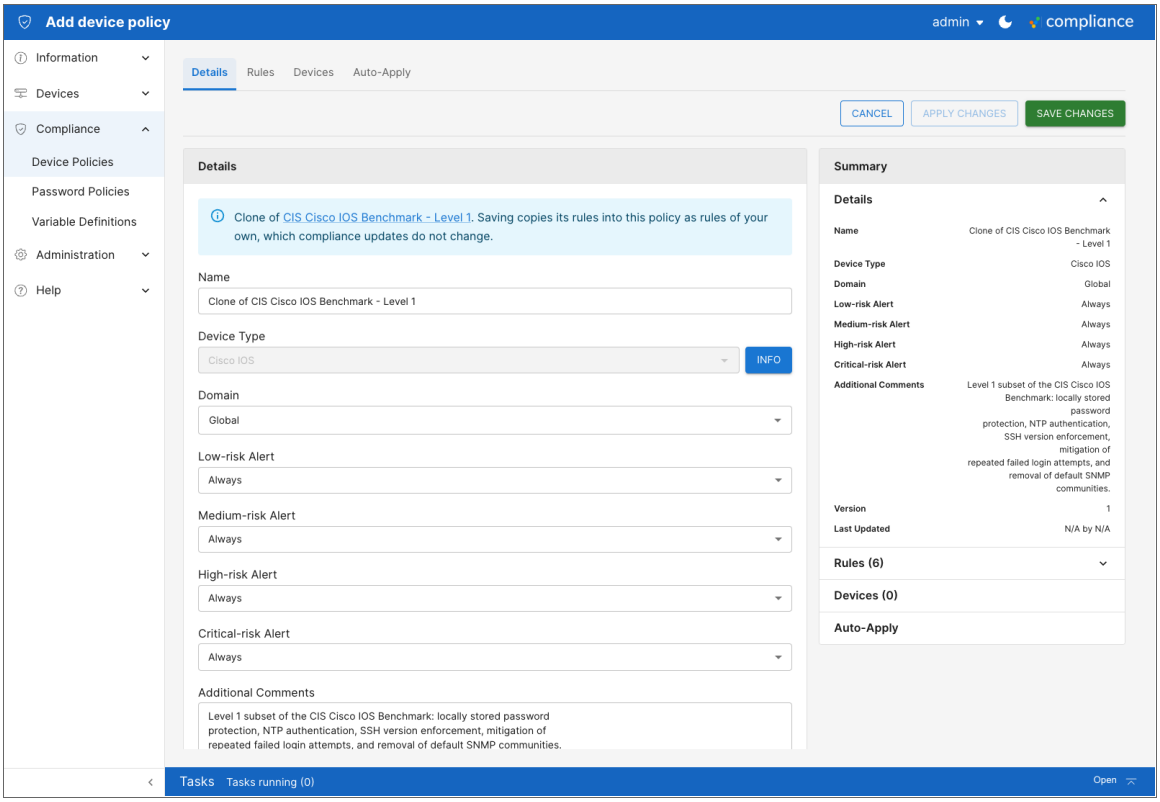
A disabled rule:

- Appears dimmed, with a *Disabled* tag.
- Is skipped by the compliance checks that run during backups and scheduled actions. Backups also stop running device commands that only disabled rules need.
- Does not count toward a device's compliance score or violations, or in compliance reports. The rule's earlier results are kept, and they count again as soon as you enable the rule.
- Is skipped by **[Test All Rules]**, which notes that disabled rules are not tested. You can still test a single disabled rule with **[Test]**, for example to check the rule before you enable it.
- Stays disabled through policy library updates, and when you clone, export, or import the policy.

Cloning a Library Policy

To clone a library policy:

1. Go to the **Device Policies** page (Compliance > Device Policies) and select the **[Policy Library]** tab.
2. Select the checkbox for the library policy and click **[Clone]**. You can also click **[Clone]** on the library policy page. The **Add device policy** page appears. The ***Name*** is "Clone of" followed by the library policy's name, and a banner names the library policy being cloned. The ***Device Type*** is set to the library policy's device type.



3. Edit the name and the other fields as needed. The **[Rules]** tab lists the rules that will be copied.
4. Click **[Save Changes]**. The library policy's rules are copied into the new policy as rules of its own.

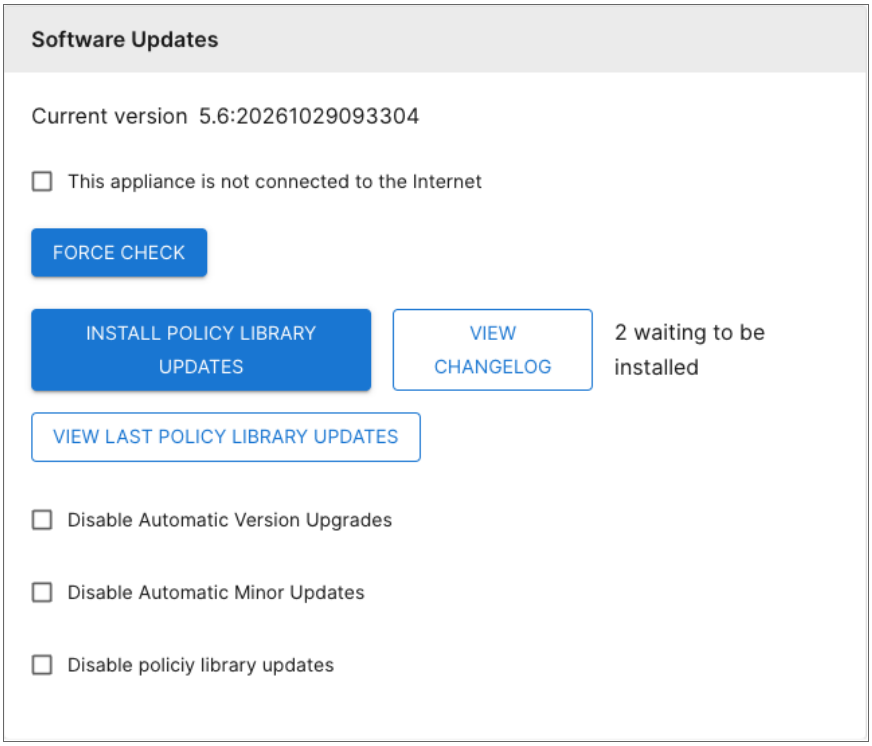
The clone is a standard device policy. You can edit or delete any of its rules, and change its device type as you would for any policy. The clone is not linked to the library policy: it has no *Library* tag, it is not listed among the library policy's instances, and policy library updates do not change it.

Policy Library Updates

ScienceLogic publishes new library policies and rules, and changes to existing ones, in policy library updates. Some windows call them compliance updates. The appliance receives policy library updates with its software updates:

- An appliance that is connected to the Internet receives them when it checks for updates. They are installed automatically, unless ***Disable Automatic Minor Updates*** is selected. If it is selected, the updates wait for you to review and install them.
- On an appliance that is not connected to the Internet, they are included in the update file that you upload, and are installed with it.

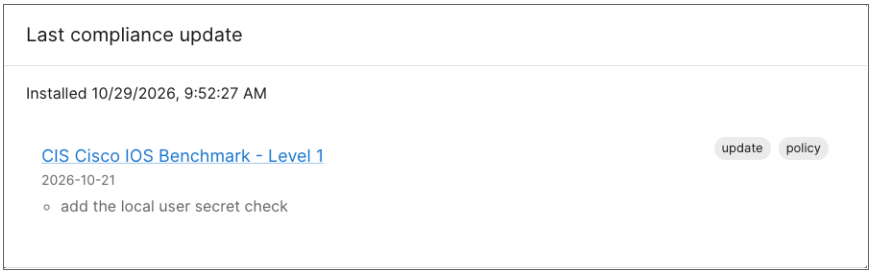
To manage policy library updates, go to the **System Settings** page (Administration > System Settings), click the **[Appliance]** tab, and use the **Software Updates** section.



When updates are waiting to be installed, the **Software Updates** section shows how many are waiting, and the following buttons:

- **[Install policy library updates]**. Installs the waiting updates. The installation runs as a task.
- **[View changelog]**. Opens the **Compliance updates ready to install** window, where you can review the waiting updates before you install them.

[View last policy library updates] is always available. It opens the **Last compliance update** window, which shows when the most recent installation ran, and lists each library policy and rule that it added, updated, or removed, with the changelog entries for each.



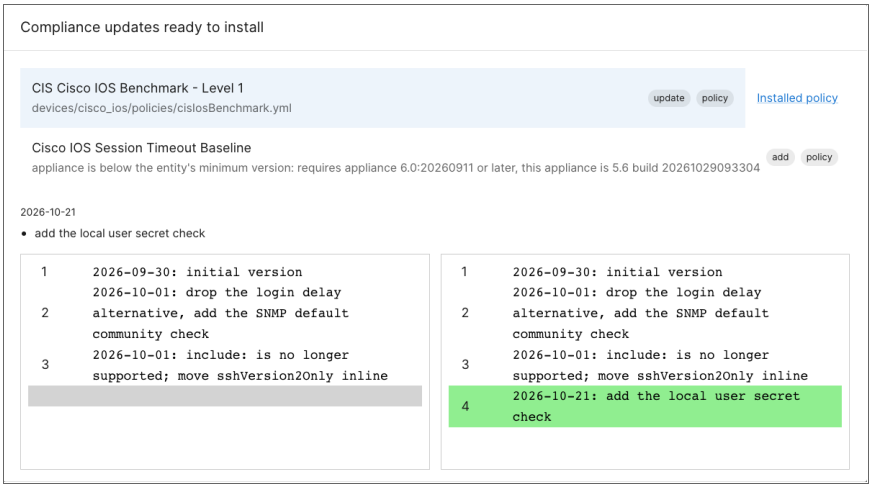
NOTE: You need the *View Sysadmin* permission to review policy library updates, and the *Update Sysadmin* permission to install them or change update settings.

Reviewing Updates Before You Install Them

In the **Compliance updates ready to install** window, each waiting library policy or rule has two tags: the kind of change (*add*, *update*, or *remove*), and what is changing (*policy* or *rule*). Select an entry to see:

- The changelog entries that the update adds.
- The installed changelog (left) next to the changelog in the update (right), with the new entries highlighted.

For an update or a removal, select **Installed policy** or **Installed rule** to open the version that is installed now.



Some updates cannot be installed yet, because they require a newer version of Skylar Compliance or a device plugin that is not installed. An update that requires a newer version shows the version it needs, as "Cisco IOS Session Timeout Baseline" does in the figure above. These updates stay waiting, and are installed by the first installation after the appliance meets the requirement. The rest of the updates install normally.

Turning Off Policy Library Updates

To stop receiving policy library updates, select ***Disable policy library updates*** in the **Software Updates** section and click **[Save]**. When you do so:

- Any updates waiting to be installed are discarded.
- The library policies and rules that are already installed, and the instances you created from them, do not change.
- If you clear the option later, the appliance receives the complete current set of library policies and rules with its next update.

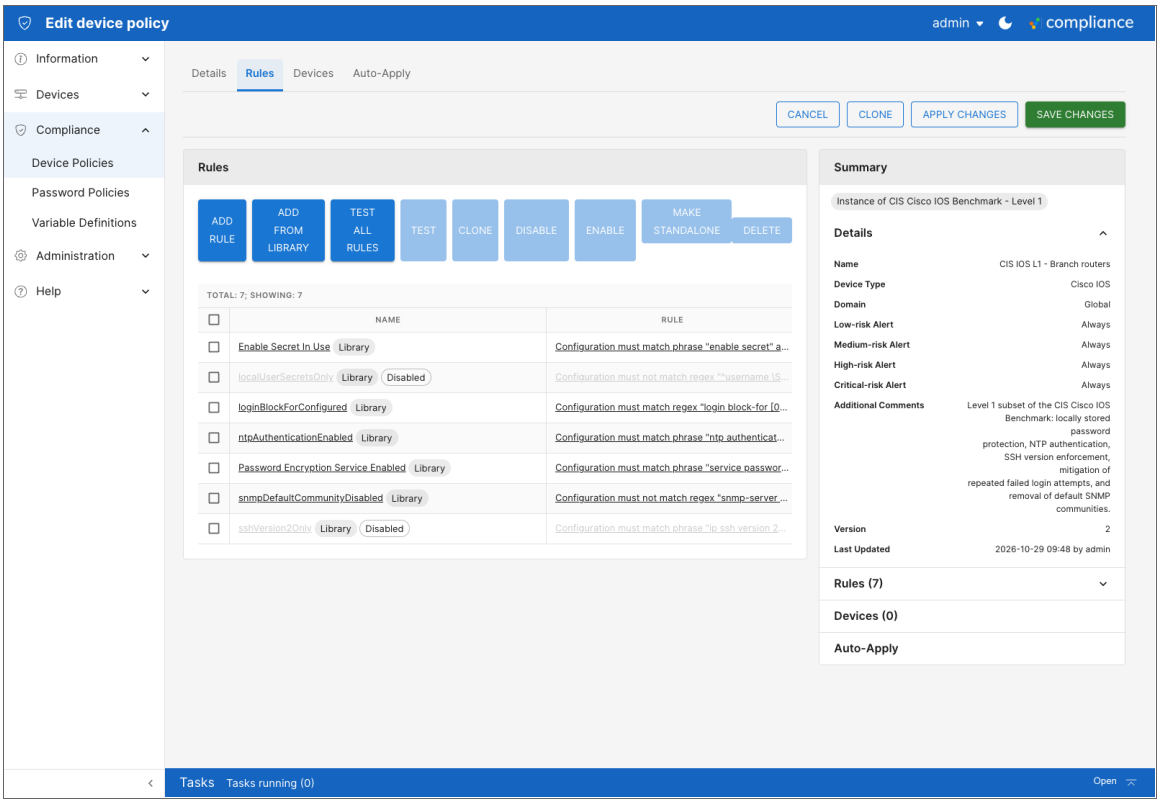
How Updates Change Your Instances

When a policy library update changes a library policy, the changes are applied to every instance of the policy, and the changes you made to each instance are kept. Clones never change.

When the update...	Each instance...
Adds a rule to the library policy.	Gets the new rule *disabled*, so that the rule does not report violations before you review it. Review the rule, and enable it if it applies to your network. Instances that you create after the update start with all of their rules enabled.
Removes a rule from the library policy.	Loses the rule, along with the rule's compliance results.
Renames a rule or changes its severity in the library policy.	Follows the change, unless you changed that setting in the instance. The name and the severity are handled separately.
Changes how a rule checks devices, such as its patterns, filters, or remediation.	Uses the new version of the rule from the next compliance check. The settings you overrode in the instance still apply.
Renames the library policy or changes its description.	Follows the change, unless ***Override library value*** is on for ***Name*** or ***Additional Comments***.
Withdraws the library policy.	Is not affected. The appliance does not remove a library policy while the policy has instances. The removal waits until all of the instances are deleted.

An update never changes the rules you disabled or enabled, the rules you added to the instance yourself, or the instance's devices, Auto-Apply settings, alert thresholds, and domain.

For example, after an update adds the "localUserSecretsOnly" rule to "CIS Cisco IOS Benchmark - Level 1", the instance below has the new rule, disabled. The "sshVersion2Only" rule stays disabled, as the user left it.



Packaged Rules in the Rule Library

The rules that ScienceLogic publishes appear on the **[Rule Library]** tab, next to the rules you create. Packaged rules:

- Cannot be edited or deleted.
- Can be added to any of your device policies with **[Add from Library]**, where you can override their settings for that policy.
- Are updated by policy library updates. For a packaged rule, the Rule Library shows the revision, and you can view the rule's changelog and earlier versions.

Rules that a library policy defines for itself are not listed in the Rule Library. You can view them on the library policy page.

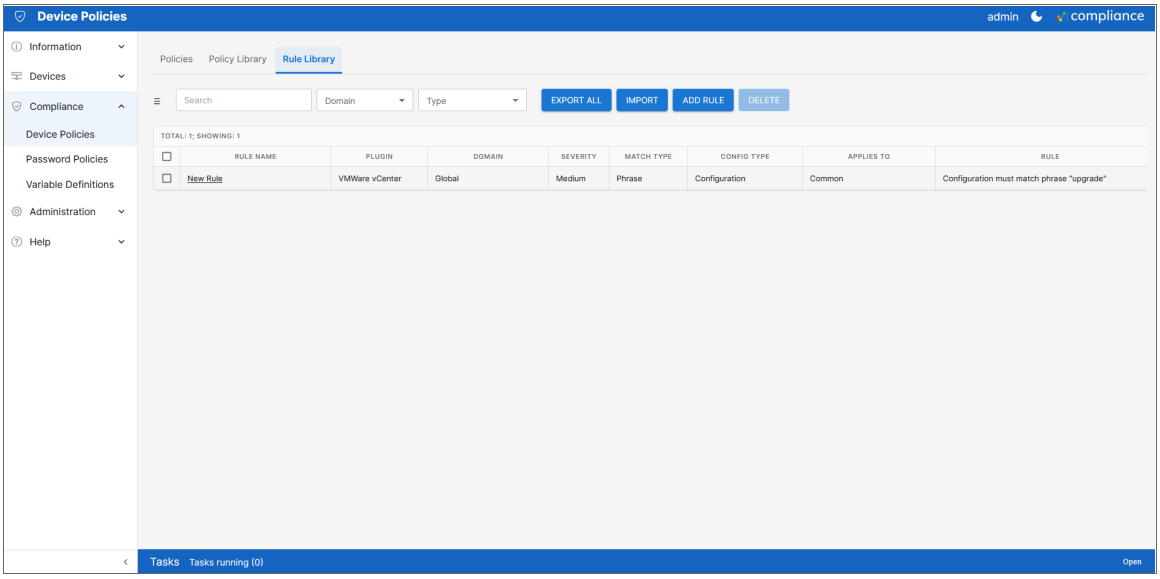
Exporting and Importing Instances

You export and import instances the same way as other device policies. The export contains the instance's link to its library policy, your changes to the library policy's rules, and which rules are disabled. It does not contain the library policy's rules themselves.

Before you import an instance on another appliance, make sure that the same library policy is installed on that appliance. Any rule of the library policy that is not in the export is added disabled, as it would be by an update.

The Rule Library Tab

The **[Rule Library]** tab on the **Device Policies** page lists all ***library rules***, which are rules that can be used with any device policy. Like a library policy, a library rule is reusable, and a library rule is not tied to just one specific device policy.



The process for creating a device-specific rule or a library rule uses the **New Skylar Compliance Rule** wizard. The type of rule depends on where you are in the user interface when you create the rule:

- To create a rule that is specific to a device policy, go to the **Policies** page (Compliance > Device Policies) click **[Add Policy]** to create a new policy or select an existing policy. On the **[Rules]** tab for the policy, click the **[Add Rule]** button.
- To create a library rule, go to the **[Rule Library]** tab (Compliance > Device Policies > Rule Library tab) and click the **[Add Rule]** button

For both situations, the **New Skylar Compliance Rule** wizard appears.

Creating a New Rule

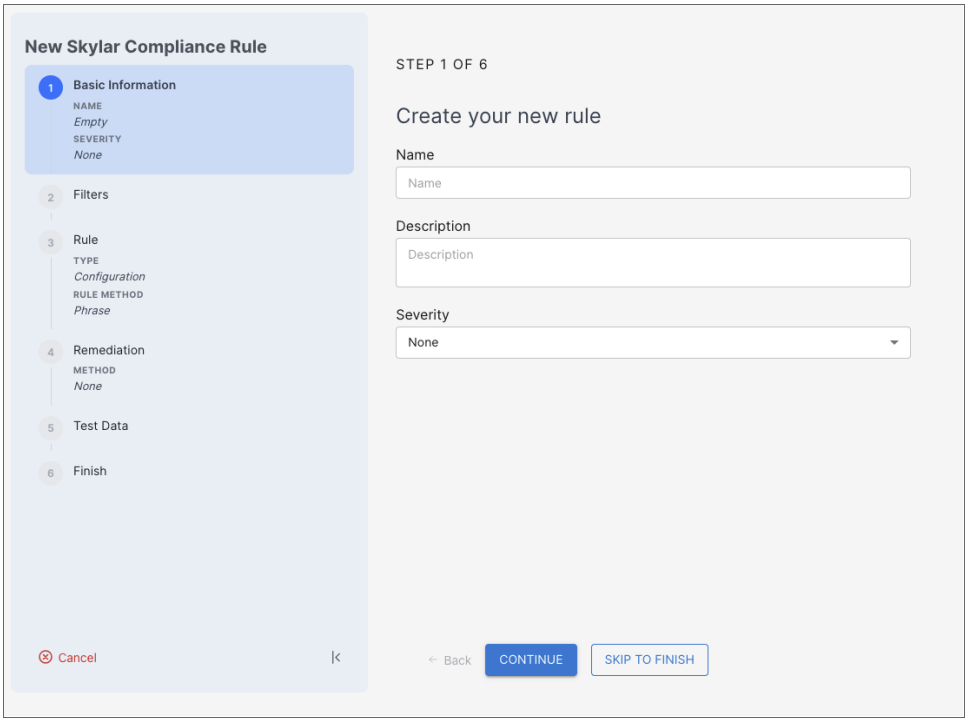
After you create a rule, you can edit, remove, clone, or test it against an existing backup with the appropriate buttons on the **[Rule Library]** tab

To create a new rule specific to a device policy:

1. Go to the **Device Policies** page (Compliance > Device Policies) and click the name of the device policy to which you want to add the rule and click the **[Rules]** tab.

> **IMPORTANT:** If you want to create a library rule, go to the **[Rule Library]** tab (Compliance > Device Policies > Rule Library tab) instead.

2. Click **[Add Rule]**. The **Rule Builder** appears and displays step 1, ***Basic Information***.



3. On the ***Basic Information*** step, complete the following fields:
   - ***Name***. Type a name for the rule. Reports and email alerts use this name to identify the rule.
   - ***Description***. Type a description of the rule.
   - ***Severity***. Select the alert level for a violation of the rule from the drop-down list: *None*, *Low*, *Medium*, *High*, or *Critical*. The severity feeds the alert thresholds and scoring of the policy.The default is *None*.

4. Click **[Continue]**. The ***Filters*** step appears. Filters are pre-conditions that are evaluated before the rule runs. If a filter is not met, the rule is skipped and counts as a pass. Multiple filters are combined with AND. The values within one filter are combined with OR. Complete the following fields as needed:

    - ***Filter Type***. How each value is matched: *Phrase* (substring) or *Regex*.
    - ***Data Type***. The device data to test against: *Asset*, *Additional Info* (the output of a device command), or *Label*.
    - ***Data***. The specific asset field or Additional Info command. This field is hidden when ***Data Type*** is *Label*.
    - ***Requirement***. *Must Match* or *Must Not Match*.
    - ***Value***. One phrase or regular expression per line. The filter passes if any line matches.

5. Click **[Continue]**. The ***Rule*** step appears. Complete the following fields as needed:
    - ***Type***. Select the type of data that the rule test: a configuration, software version, runtime command, or the output of a scheduled action. If you select a runtime command or a scheduled action, select the command or schedule in the new field that appears below this field.
    - ***Process line-by-line***. Select this toggle to evaluate the output of a runtime command line by line instead of as a whole string. This field appears only for older rules that still evaluate the output as a whole string.
    - ***Rule Method***. Phrase, regular expressions, Lua function, device, or device templates. The *Phrase* match type matches any (case sensitive) number of characters, including multi-line. The *Regex* match type (see *Regular Expressions*) takes a Perl-flavoured regular expression, and applies it to the whole configuration, or firmware string.
    - ***Must Match*** / ***Must Not Match***. If you select the *Phrase* or *Regex* rule method, enter the pattern values. You can enter both *Must Match* and *Must Not Match* values.
        - ***Case Insensitive***. Select this toggle to ignore case. You set this for each pattern.
        - ***Match Type*** / ***Subtype***. For multi-line patterns: *All (Consecutive)* (default), *All (Unordered)*, *All (Ordered)*, *All (Consecutive, once)*, *Any*, or *One* (*Must Match* only).
        - ***Scan Entire File***. For *Must Not Match* patterns with an *All* subtype, collect and report all occurrences.
    - ***Condition***. If you select the Lua function or device rule method, select *Must Match* or *Must Not Match*.
    - ***Lua Function***. If you select the Lua function rule method, enter the Lua source code to evaluate.
    - ***Device***. If you select the device rule method, select the peer device to compare the configuration against.
    - ***Template***. If you select the device templates rule method, select the template to match. The rule always uses *Must Match*.
    - ***Files***. If you select a configuration rule, restrict the rule to specific file paths within the backup.
    - ***Ignore Lines***. If you select the device rule method, enter the lines to remove before matching.
6. Click **[Continue]**. The ***Remediation*** step appears. Complete the following fields as needed:
    - ***Remediation***. *None*, *Manual*, *Automatic*, or *Command*. For more information, see *Remediation*.
    - ***Command***. If you select *Command*, select the stored command that runs to remediate.
    - ***Value***. If you select *Manual* or *Automatic*, enter the remediation instructions or commands text.

    For more information, see *Remediation*.

7. Click **[Continue]**. The ***Test Data*** step appears. Test data are named test inputs that validate the rule. They are not evaluated against real devices. Test data is not supported for the device and device templates rule methods. Complete the following fields as needed:
    - ***Test Name***. An identifier for the test case.
    - ***Should Pass***. A toggle for the expected outcome.
    - ***Description***. Optional notes.
    - ***Data***. The sample text that the rule runs against (up to 10 KB).
    - **[Run Tests]**. Runs all test cases against the current, unsaved rule and displays a badge with the result of each case.
8. On the ***Test Data*** step, test the rule before you save it. Click **[Continue]**. The ***Finish*** step appears.
9. The ***Finish*** step displays a read-only summary of all your entries for review before you save the rule. Click **[Finish]** when you are done reviewing the data for the rule and click **[Save Changes]** if you are working in a device policy.

    The device-specific rule appears on the **[Rules]** tab of the device policy or the library rule appears on the **[Rule Library]** tab.

Remediation

You can use remediation when a compliance rule is not met, generally intended to rectify the violation. The following remediation types can be configured:

- ***Manual***. The remediation text is appended to the notification email to signify that the recipient should take the appropriate action.
- ***Command***. One of the stored **Actions** on the device is executed. For more information, see *Device Control*.
- ***Automatic***. The text specified in the textbox is used as a command and executed on the device.

If the rule match type is *Regex*, the remediation can make use of the **Capture** feature, whereby parts of the pattern in brackets can be captured and then referred to in the remediation text (as `$1`, `$2`, etc.). For example, a rule may state that a configuration must not contain the regex:

```
set telnet (\d+\.\d+\.\d+\.\d+)
```

Where the command in brackets is a match for an IP address. If this rule is violated, the configuration can be remedied using the phrase:

```
unset telnet $1
```

In this case, the brackets in the rule will capture the IP address, and apply it when the command is performed. The rule is then expanded:

```
unset telnet 1.2.3.4
```

Regular Expressions

A regular expression specifies a set of strings as a pattern, rather than a list. For example, the pattern `C(o|as?)t` matches the strings *Cot*, *Cat*, and *Cast*, but not *Coast*. Skylar Compliance uses Go's RE2 regular expressions.

Most characters can be used in a regular expression. Some characters, called *metacharacters*, have special meanings:

- `()` denote grouping: *(a|b)b* matches *ab* and *bb*
- `|` denotes an alternative (see above)
- `^` matches the beginning of a line
- `$`matches the end of a line
- `.` matches any character
- `+` denotes one or more occurrences of the previous character: `a+b` matches *ab*, *aab*, *abb*, but not *b*
- `*` denotes zero or more occurrences of the previous character: `a*b` matches *b*, *ab*, *aab*, *aaab*
- `?` denotes zero or one occurrences of the previous character: `a?b` matches *b* and *ab*, but not *aab* or *aaab*

Character classes are matches for sets of possible characters, rather than just a single character. For example:

- `[bcr]at` matches *bat*, *cat* and *rat*
- `-` can be used as a range operator in a character class. For example, `[a-g]` matches any character from *a* to *g*

There are some abbreviations for common character classes:

- `\d` matches a digit
- `\s` matches whitespace (a space or a tab)
- `\w` matches a word character (alphanumeric or a _)

For example, `\d\d:\d\d:\d\d` matches time in a *hh:mm:ss* format

Lua Functions

You can use Skylar Compliance to define rules using Lua functions.

Available functions for compliance rules are:

- `nextline()` returns the next line of text
- `getline(n)` returns the given line of text
- `numlines()` returns the number of lines
- `addmessage(m)` allows you to replace a series of variables in the remediation text. For example, `addmessage("Hello")` with a remediation text of `$1World!` would output *Hello World!*. The next addmessage call would replace *$2*, and so on.

This function checks that the number of lines containing *configure* matches the lines containing *port*:

```
num1 = 0
 num2 = 0
line, next = nextline()
 while next do
   if line:match("configure") then num1 = num1+1 end
   if line:match("port") then num2 = num2+1 end
   line, next = nextline()
 end
 if num1 > num2 then addmessage("more")
 else if num2 < num1 then addmessage("less") end
return num1 == num2
```

Remediation Text: `Config contains $1 configures than ports.`

Skylar Compliance Built-in Functions

The following functions can be used in a Lua applet:

- `timeout(seconds)` - set the maximum timeout when waiting for device output
- `sleep(seconds)` - do nothing for the given number of seconds.
- `send(command)` - send `command` to the device
- `wait(string)` - wait for timeout seconds for `string` from the device
- `sendget(command,output)` - combined send/wait
- `before()` - used after wait() or sendget(); it contains the output from the device up to the expected string.
- `print(string)` - displays the value of `string`
- `splitlines(string)` - split a multi-line string (for example, the output of a command) into an array of lines.

Other standard Lua commands that may be useful include, `string.match`, `string.gsub`. and `string.trim`.

NOTE: You do not need to write any code to connect and authenticate to the device. Skylar Compliance will automatically connect and authenticate the device for you.

CAUTION: Users are not permitted to run any “os” or “system” functions when making Lua scripts. This restriction is in place to maintain the security of your Skylar Compliance appliance.

Examples

Show Version (Cisco)

A basic example is to display the output of the `show version` command on a Cisco switch:

```
timeout(20)
send('show version')
wait('#')
out=before()
print(out)
```

The `send()` & `wait()` commands can also be combined into a `sendget()`:

```
timeout(20)
sendget("show version","#")
out=before()
print(out)
```

Show Interface (Cisco)

The following is a more complex example using control structures. It runs `show interfaces` on a Cisco switch and checks that all interfaces that are not connected (line protocol is down) are also administratively down. Note that everything after `--` is a comment, and is not executed:

```
timeout(20)                        -- set the timeout to 20 seconds
sendget("terminal length 0","#") -- send command to the device, and
                                   -- wait for the prompt
sendget('show interfaces', '#')
out = before()                     -- set "out" to the output
lines = splitlines(out)            -- split the output lines into array
for k,v in pairs(lines) do         -- loop over each line, and
                                   -- set k=number and v=text
```

```
int,st1,st2 = v:match(
"^(%S+Ethernet[0-9/]+) is ([a-z ]+), line protocol is ([a-z]+)"
)                                  -- extract the interface name,
                                -- interface status, and the
                                -- line protocol status
```

```
if int ~= nil and
( st1 ~= 'administratively down' and st2 == 'down' ) then
print("Interface "..int.." is disconnected but not shutdown")
end
```

```
end                                  -- end loop
```

IP Spoofing (ScreenOS)

For ScreenOS, use the following script to check for ip-spoofing:

```
timeout(5)
sendget("set console page 0",">")
sendget("get zone | inc L3",">")
ret = before()
sendget("get config | inc ip-spoofing",">")
conf = before()
```

```
for zone in ret:gmatch(" [0-9]+ (.-)%s+Sec") do
    if conf:match('zone "'..zone..'" screen ip%-spoofing') then
      print('Zone '..zone..': antispoofing enabled')
    else
      print('Zone '..zone..': antispoofing disabled')
    end
end
```

IP Spoofing (Palo Alto)

You can use the following script to check for ip-spoofing, but for Palo Alto devices:

```
timeout(5)
sendget("set cli pager off",">")
sendget("set cli config-output-format set",">")
waitprompt()
sendget("configure","#")
send("show zone")
sleep(1)
waitlast("#")
ret = before()
sendget("exit",">")
tbl = {}
```

```
for key in ret:gmatch("set zone (.-) ") do
  tbl[key] = true
end
for k, _ in pairs(tbl) do
  send('show zone-protection zone '..k)
  sleep(1)
```

```
  waitlast('>')
  ret = before()
  if ret:match('discard%-ip%-spoof:%s+enabled: yes') then
    print('Zone '..k..': antispoofing enabled')
  else
    print('Zone '..k..': antispoofing disabled')
  end
end
```

Chapter 15

Password Policies and Variable Definitions

Overview

On the **Password Policies** page (Compliance > Password Policies), you can use password policies to configure various rules to enforce password strength for devices and users.

On the **Variable Definitions** page (Compliance > Variable Definitions), you can define variables that can be used in compliance rules as replacements.

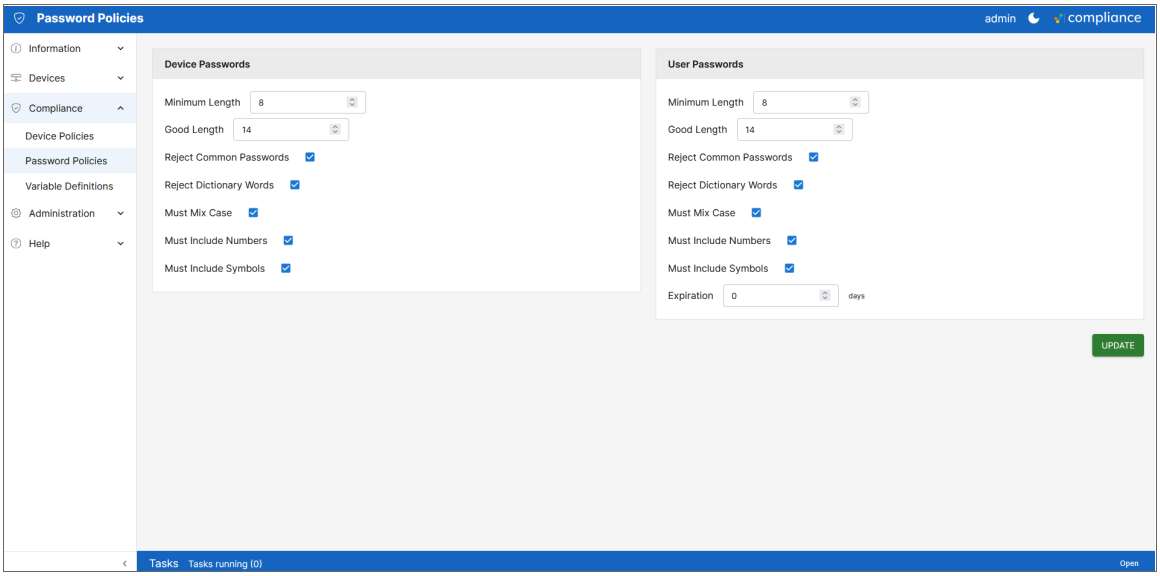
This chapter covers the following topics:

Password Policies *129*

Variable Definitions *130*

Password Policies

On the **Password Policies** page (Compliance > Password Policies), you can use password policies to configure various rules to enforce password strength for devices and users.



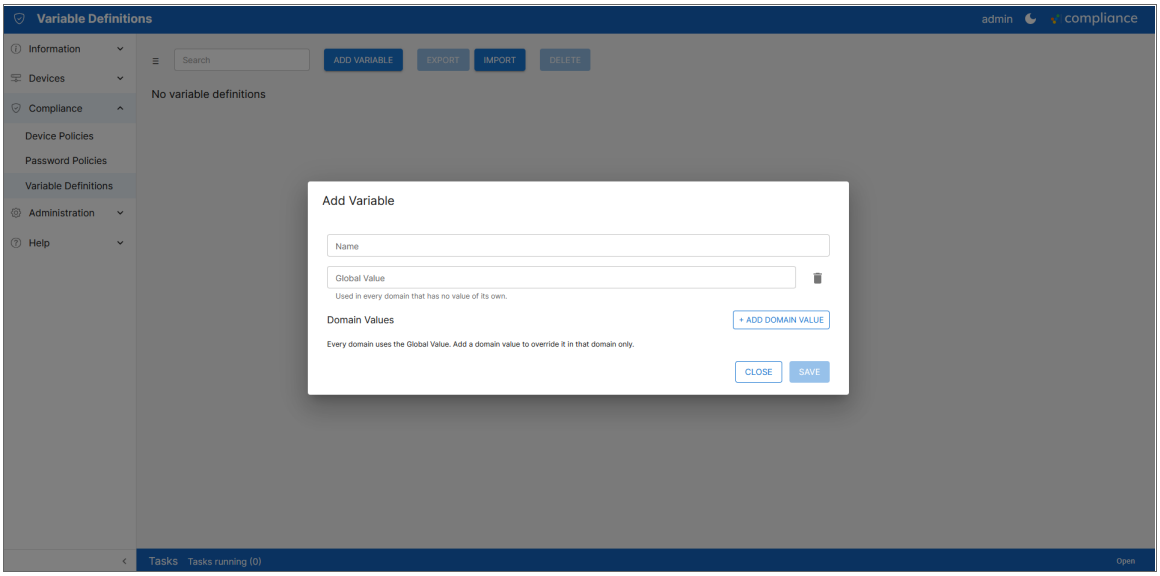
You can use password policies to configure various rules to enforce password strength for devices and users. These settings are used in the **strength meter** that is displayed in all password fields : the background of the field will change color, from red for an unacceptable password, to yellow for a weak password, to green for a good password. Password Strength reports are available on the **Reports** page.

You can use the following rules for device passwords and user passwords:

- ***Minimum Length***. Type a minimum number of characters for a password to be accepted.
- ***Good Length***. Type a recommended number of characters to be considered *good*.
- ***Reject Common Passwords***. Select this checkbox to reject easy-to-guess passwords, such as *1234* or *password*.
- ***Reject Dictionary Words***. Select this checkbox to reject common words from the dictionary, such as *backup* or *admin*.
- ***Must Mix Case***. Select this checkbox to require users to use mixed-case passwords.
- ***Must Include Numbers***. Select this checkbox to require users to include numbers in their passwords.
- ***Must Include Symbols***. Select this checkbox to require users to include symbols in their passwords.
- ***Expiration***. User Passwords only. Type the number of days until the user passwords expires.

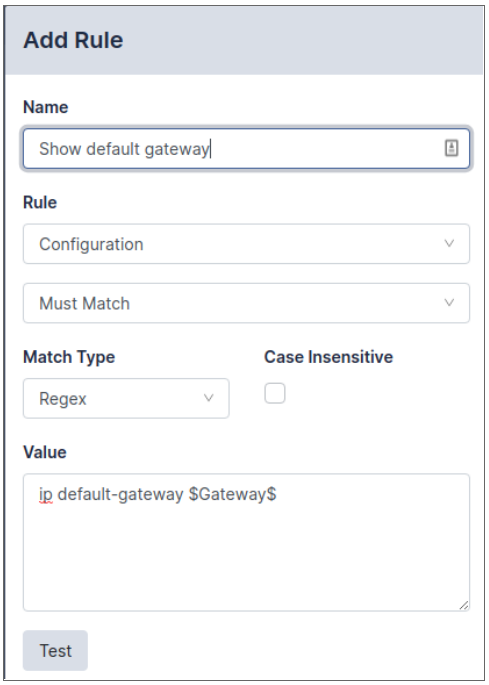
Variable Definitions

On the **Variable Definitions** page (Compliance > Variable Definitions), you can define variables that can be used in compliance rules as replacements.



Items defined in this section can be used in compliance rules as variable replacements, referenced with the `$replace$` format, where `replace` is the variable you have defined. This enables you to use a variable as shorthand for configuration elements, that are likely to be referenced multiple times.

For example, if you create a definition for *Gateway*, and assign it a ***Value*** of *192.168.0.1*, you can then use it in a compliance rule, as shown below:



This rule will be expanded to `ip default-gateway 192.168.0.1`. If the gateway address changes, update the **Value** in the *Gateway* variable definition and all rules that use the `$Gateway$` variable will be automatically updated.

NOTE: A variable name can only consist of letters, numbers, and the underscore character `_`. If the value contains escape sequences (such as `\n`), the sequence must be double-escaped (`\\n`).

Chapter 16

System Settings

Overview

The **System Settings** page (Administration > System Settings) allows you to configure appliance-related settings, such as networking parameters and date/time settings.

This chapter covers the following topics:

The Network Tab *133*

The Appliance Tab *135*

The Archive Tab *140*

The Logs / Alerts Tab *142*

The SNMP Tab *144*

The Security Tab *145*

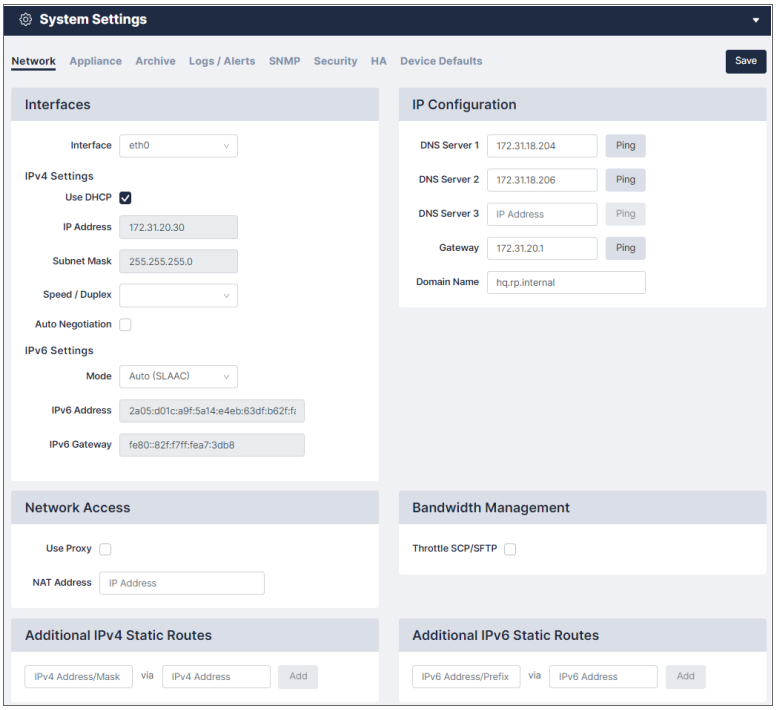
The High Availability (HA) Tab *151*

The Device Tab *153*

Advanced Settings *159*

The Network Tab

On the **[Network]** tab (Administration > System Settings > Network tab), you can configure your interfaces, network access, IP configuration, manage bandwidth, and configure additonal IPv4 and IPv6 static routes.



Interfaces

The options in this section let you set or update the network address for Skylar Compliance. The initial settings are entered when you first set up your appliance. Select your **Interface** first and then supply values in the following fields.

- Use the ***Interface*** drop-down menu to override the default auto-detect setting of the Ethernet interface(s).
- ***Use DHCP***. Select this checkbox if you use DHCP for your interface. When you select the checkbox, all other options on the page are disabled.
- ***IP Address***. Complete the specific address fields for your ***IPv4*** and/or ***IPv6 Settings***.
- ***Subnet Mask***. Enter the subnet mask associated with the IP address.
- ***Speed/Duplex***. Select the link speed and duplex from the drop-down list.
- ***Auto Negotiation***. Check whether or not you'd want to include ***Auto Negotiation*** for your interface.

- ***Mode***. Select your ***Mode*** type from the drop-down list. If you select this checkbox, ***Speed/Duplex*** is disabled, and the ***Auto-Negotiated Speed*** field appears. This contains a value showing the value it set.

Click **Save** when all updates have been made.

IP Configuration

To set up your IP routing configuration, complete the following fields:

- ***DNS Server***. The DNS server addresses for your network. You can configure up to three servers. The DNS servers must be able to resolve public names (for example, *support.restorepoint.com*), or the Skylar Compliance appliance cannot retrieve software updates and license details. This option is for IPv4 addresses only.

> **NOTE:** ScienceLogic recommends that you ping the servers you entered to ensure they are reachable.

- ***DNS Sever 2***. (Optional) A second DNS server. This option is for IPv4 address only.
- ***DNS Sever 3***. (Optional) A third DNS server. This option is for IPv6 address only.
- ***Gateway***. The default gateway for your network. You can **Ping** these servers to check connectivity.
- ***Domain Name***. The default domain name of the network where this appliances is hosted.

Network Access

Skylar Compliance needs internet access (HTTP/HTTPS) to retrieve software and plugin updates. If a proxy is required for Internet access, select **Use Proxy**, and supply the following information:

- IP address of the proxy server. Complete the specific address fields for your servers.
- Proxy port. Type the port for your proxy port.
- Username/password, if your proxy requires authentication. Otherwise, leave this field empty. Use the **Test Proxy** button to verify that the configuration is correct.

Network Address Translation (NAT)

Skylar Compliance may use back connections (typically TFTP or FTP) to backup certain devices. If Skylar Compliance is accessing a device using back connections through a NAT router or firewall, back connections will fail because the device will attempt to connect to the original, untranslated IP address. To avoid this problem:

- On your firewall, create a 1:1 NAT mapping (often referred to as Static NAT or Mapped IP) to translate the Skylar Compliance IP address to a public/routable IP address.
- Enter the public IP address for Skylar Compliance in the **NAT Address** box. The system-wide NAT IP address defined here can be overridden in the Domain settings, or in each individual device's settings.

The **Back Connection NAT** option needs to be selected in any device that is accessed by Restorepoint through NAT. For more information, see *Adding a New Device Manually*.

> **IMPORTANT:** Skylar Compliance supports multiple NAT addresses. The NAT IP address defined in this page can be overridden by the Domain or Device NAT IP setting.

Additional IPv4 and/or IPv6 Static Routes

If the devices that you want to add to Skylar Compliance are located on different networks, you might need to define additional IPv4 or IPv6 static routes.

To define a static route:

1. **IP Address / Mask length**: Enter the network address/netmask (in CIDR notation).
2. **Via IP address**: Enter the destination gateway IP address.
3. Click **Add**.
4. Click **Save**.

To remove a static route:

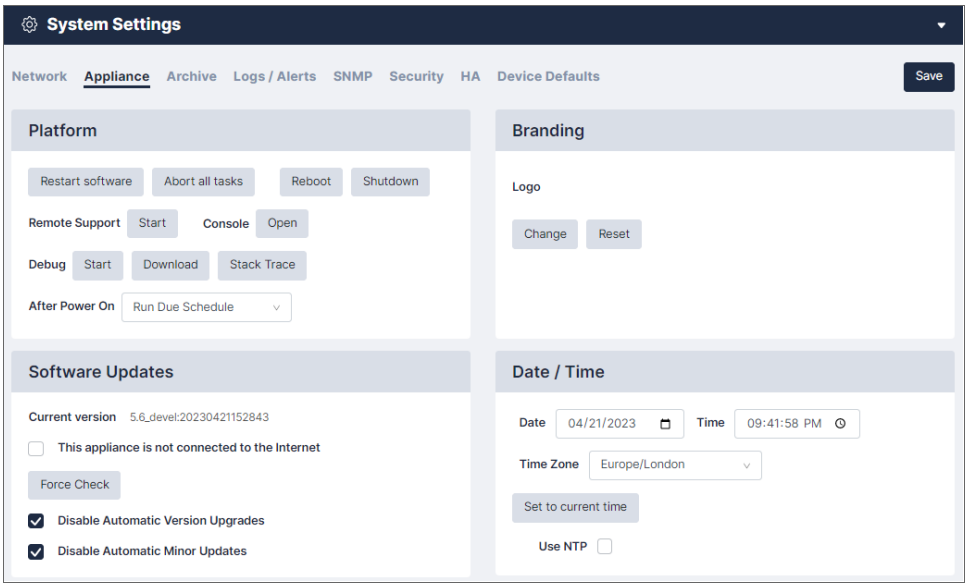
1. Click **Delete** next to the static route you want to remove.
2. Click **Save**.

Bandwidth Management

You may limit the amount of network bandwidth Skylar Compliance uses by selecting **Throttle SCP/SFTP** and specifying a speed (in kbps).

The Appliance Tab

You can manage your appliance operations on the **[Appliance]** tab (Administration > System Settings). Complete your desired platform, software updates, branding, and date/time operations, and click **[Save]**.



Platform

To manage your platform, enable the following buttons and/or complete the following fields:

- ***Restart Software***. Restarts the Skylar Compliance domain. May leave the system in an unstable state, use when directed by Skylar Compliance support.
- ***Abort All Tasks***. Aborts all currently-running tasks. This could leave network devices in an unstable state.
- ***Reboot***. Enables you to reboot your Skylar Compliance appliance. However, try to **Restart software** first.
- ***Shutdown***. Enables you to shutdown and power off your Skylar Compliance appliance. This is the safest way to shut down your Skylar Compliance appliance. Wherever possible, avoid using the front panel buttons to reset or shutdown Skylar Compliance.
- ***Remote Support***. Click **Start** to enable Technical Support to securely connect to your Skylar Compliance appliance for troubleshooting. To stop the remote support tunnel, click the **Stop** button on this page, or click the running task in the *Activity Display.* Then, click **Stop Remote Support** to terminate the secure connection.

> **Note:** The **Remote Support** feature requires that your firewall allows SSH connections (TCP port 22) from Skylar Compliance to *jmp1.restorepoint.com* and *jmp2.restorepoint.com*. For more information, see *Firewall Requirements* for notes on firewall configuration.

- ***Open Console***. Opens a console terminal to Skylar Compliance's shell menu to allow users to access the terminal via HTTPS.

- ***Debug***. Generates an appliance debug file that may help Technical Support diagnose your issue. Click the **[Start]**, **[Stop Debug]**, **[Stack Trace]**, or **[Download]** buttons to debug your appliance.
    - The **[Start]** button launches the debug process, removing any previous debug logs and setting the log level of the application to debug. It also starts collecting logs and system information like memory usage, CPU usage, stack trace, and so on.
    - The **[Stop Debug]** button only appears after the debug process has started. It stops the debug collection by changing the log level back to the information level logs.
    - The **[Stack Trace]** button generates and downloads the file containing the stack trace of all the running routines in the application.
    - The **[Download]** button allows users to download the debug log that was written as the debug process was started.
- ***After Power On***. Defines what Skylar Compliance should do when returning from a power-off state. If Skylar Compliance should *Run Due Schedules*, and treat any missed backups as Overdue, or *Recalculate Schedule* and just return to the normal backup schedule.

Branding

You can replace the Skylar Compliance logo with your company's logo in the upper-left corner of the appliance user interface. Click **[Change]** and then **Browse** to locate a suitable image file on your PC. For best results, the logo should be exactly 30 pixels tall and up to 150 pixels wide, and no more than 40KB in size. Click **[Revert]** to return the logo to the default Skylar Compliance logo.

You can further customize the user interface for Domain users in the Domains page. For more information, see *Managing Domains*.

Software Updates

System updates are managed centrally by Skylar Compliance from the **Software Updates** section of the **[Appliance]** tab (Administration > System Settings > Appliance).

By default, the appliance checks and automatically installs any available software upgrades and updates, including:

- The current Skylar Compliance version.
- The appliance's connection to the Internet. If your system is air-gapped, the checkbox ***This appliance is not connected to the internet*** should be selected. In this case, click **[Manual Upgrade]** to check for appliance updates and to perform a manual upgrade of the version. A license statement will be displayed that indicates the license status and the installed plug-in(s).
- Click **[Update Now]** to update to the version listed in the ***Available version*** field.
- Click **[Force Check]** to check for the latest version.
- Click **[View Last Policy Library Update]** to see if any updates were installed on the appliance.

- You can control the configuration of your appliance updates by selecting one of the check boxes that follow. To accept all updates, do not select the check boxes:
    - ***Disable Automatic Version Upgrades***.
    - ***Disable Automatic Minor Updates***.
    - ***Disable policy library updates***.

Ensure that your firewall is configured correctly to allow system updates. For information on firewall configuration, see *Firewall Requirements*.

Disabling Automatic Updates

Although Skylar Compliance strongly recommends that all updates are automatically applied, you can override this behavior and disable automatic version upgrades:

1. Navigate to the **Software Updates** pane (Administration > System Settings > Appliance).
2. Select the ***Disable Automatic Version Upgrades*** checkbox.
3. Click **[Save]**.

Minor software updates that do not change the user interface or modify any Skylar Compliance functions are automatically downloaded and applied, to override this behavior and disable automatic minor updates:

1. Navigate to the **Software Updates** pane (Administration > System Settings > Appliance).
2. Select the ***Disable Automatic Minor Updates*** checkbox.
3. Click **[Save]**.

Manual Updates

Use the **[Force Check]** button to manually check for updates. To force check for updates:

1. Navigate to the **Software Updates** pane (Administration > System Settings > Appliance).
2. Click **[Force Check]**.
3. A notification appears that an appliance is checking for an update and the task is added to the task bar.
4. If an update is available, an **[Update Now]** button displays. Click **[Update Now]**.
5. Once the update downloads, you are redirected to a **Service** page while Skylar Compliance verifies the update.
6. Once the update is verified and complete, you are redirected to the **Login** page.

Offline Updates

If Skylar Compliance is deployed on an isolated network and cannot connect to the update server, you can also use the **Software Updates** pane to manually update the appliance offline. To update the appliance offline:

1. Navigate to the **Software Updates** pane (Administration > System Settings > Appliance).
2. Select the ***This appliance is not connected to the Internet*** checkbox.
3. A **[Manual Upgrade]** button displays. Click **[Manual Upgrade]**.
4. Instructions display on how to download an update package using a computer without an internet connection and upload it to the appliance. Follow these instructions to manually update your appliance.

NOTE: When this option is enabled, all update and upgrade operations (including enabling software features or applying new license details) must be manually performed by the administrator.

Date / Time

Use the selectors to set the Time Zone on the appliance. Alternatively, you can choose to use a Network Time Protocol server by selecting ***Use NTP*** and entering up to two NTP servers.Network Time Protocol (NTP) and enter up to two NTP servers, such as *pool.ntp.org*.



OS Updates

In this section, administrators can manage Oracle Linux packages directly from the **[Appliance]** tab, removing the need for shell access. In the **OS Updates** section, you can check for available updates, apply an update, review full transaction summaries (security fixes, dependencies, and download sizes) and run an "OS Update" job to apply the reviewed updates as a tracked background job.

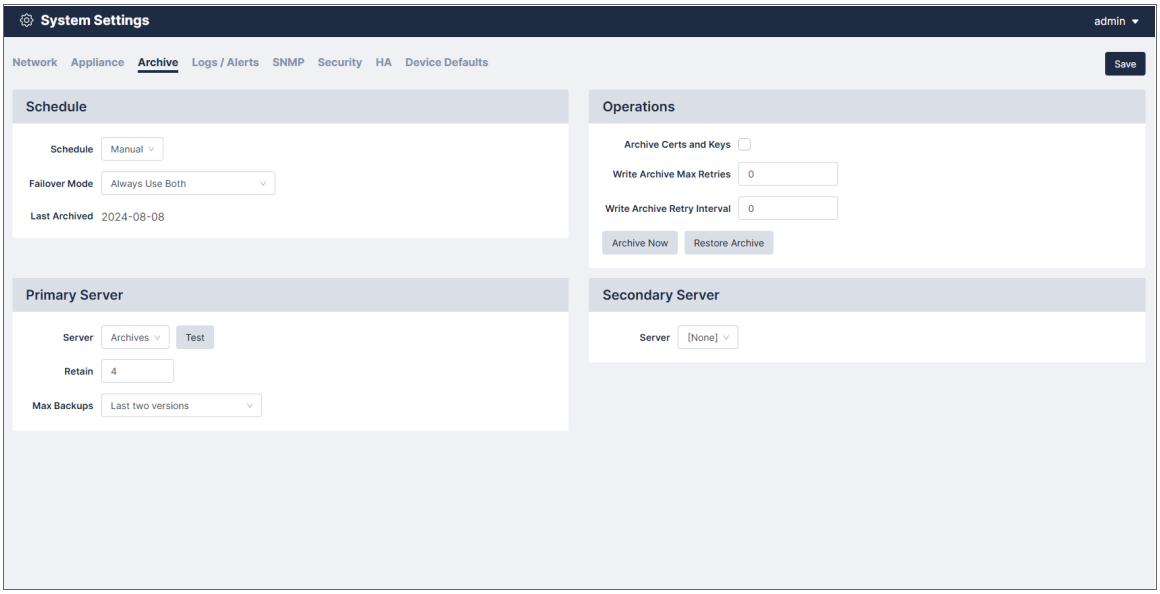
The **OS Updates** section displays the results of the update, including the last check, the last update, whether a reboot is needed, the running kernel, and any duplicate packages left behind. The system maintains a comprehensive update history, provides real-time status on reboot requirements, and includes diagnostic logs in the system debug zip.

IMPORTANT: To use this feature, whitelist the following domains on HTTPS (443/tcp): **yum.oracle.com** and **updates.sciencelogic.net**.

OS updates apply to this appliance only. Update the other High Availability node from its own address. Oracle Linux 8 and 9 are supported for both RHCK and UEK kernels. In Docker or on another operating system, the **OS Updates** section is hidden.

The Archive Tab

On the **[Archive]** tab (Administration > System Settings) you can configure your schedule, set the primary and secondary server archiving, and set the operations archive.



You can prepare for disaster recovery scenarios by archiving the Skylar Compliance configuration from the **Administration > System Settings > Archive** tab. Archiving the Skylar Compliance configuration allows you to back up the Skylar Compliance appliance automatically to up to two remote servers, including all device configurations stored on Skylar Compliance.

Taking an Archive

You can define the following settings for archiving:

- For Primary and Secondary Archive servers, you can use a pre-defined server, or select *[New Server]* to enter the details for a server that you have not defined. For details on how to define a file server, See *File Storage.*

- For each Archive Server, you can define the following:
    - ***Retain***. Enter the maximum number of archives to keep on the chosen fileserver. As you reach this number, older archives will be removed.
    - ***Max Backups***. Select the maximum number of backups that will be stored in the archive.

> **NOTE:** To be clear, ***Retain*** settings control the number of archives while ***Max Backups*** pertains to the number of backups in a particular archive.

Then , you have the options to:

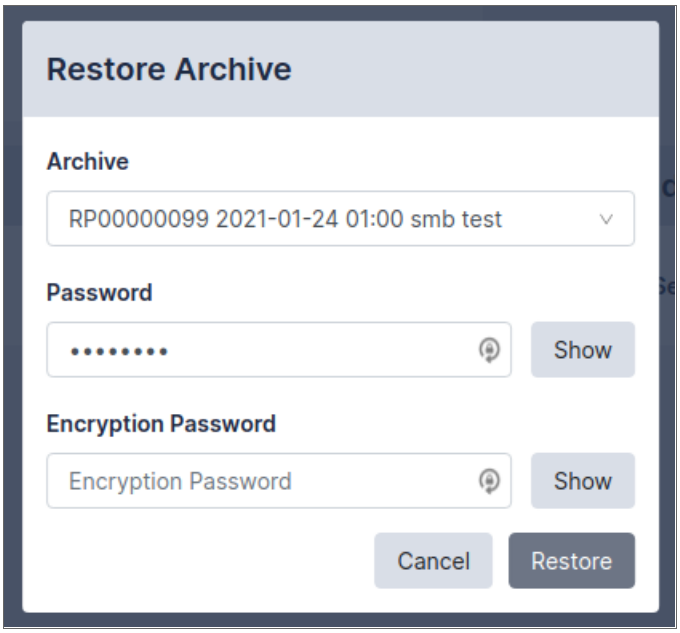
- Click **[Save]**.
- Click **[Archive Now]** to start a manual archive operation.

Restoring from an Archive

Restoring from an archive allows you to quickly recover from a failure. For example, when installing a replacement appliance after a hardware problem. To restore the appliance from an archive:

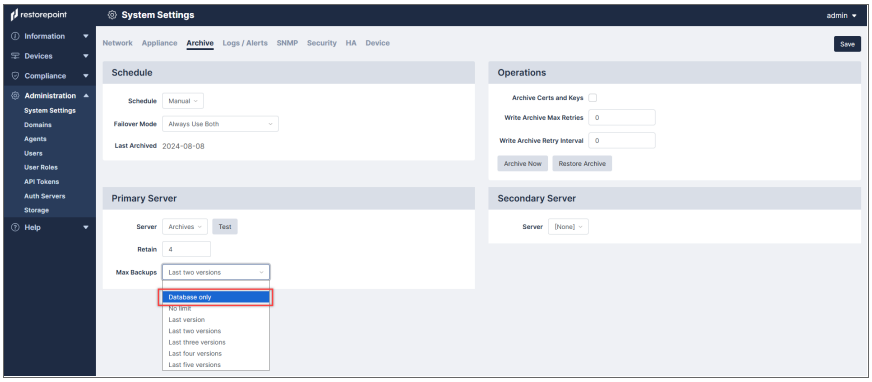
1. Click the **[Restore Archive]** button on the **System Archive** page to display the list of available archives.
2. Select the archive to be restored.
3. Click **[Restore]**.

> **NOTE:** You will need the password and encryption password for the origin's *admin* account in order to complete the operation.



Workstation DB Archives

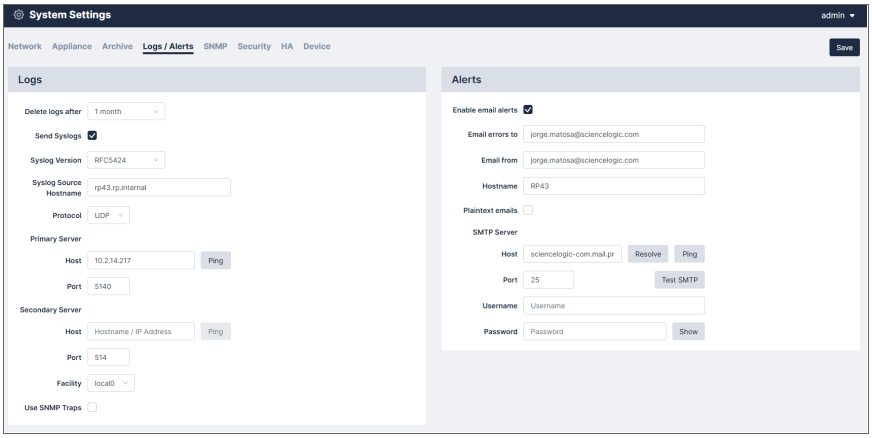
You can also execute a database-only export/import to a workstation instead of a fileserver. While not suitable for most disaster recovery scenarios, it allows for a quick migration of your Skylar Compliance settings from one appliance to another. You can filter the number backups you want to include in the archive with the *Database only* option in the ***Max Backups*** drop-down menu on the **[Archive]** tab (Administration > System Settings > Archive > Primary Server).



The Logs / Alerts Tab

You can use the log settings and alerts section to define your default log retention policy and the email address for system error notifications.

Navigate to the **[Logs/Alerts]** tab (Administration > System Settings) and supply values in the given fields. Then, click **[Save]** when finished.



Logs

- ***Delete logs after***. Enter a maximum age for events. Events older than this value are permanently deleted from the system. The default value is one month.
- ***Send Syslogs***. Select this checkbox to forward all log messages to an external syslog server. Log entries will still be available by clicking on **Information > Logs** or **Information > Syslogs**. If you use a syslog server, you will need to enter its IP address and choose the syslog facility. If you want to use the Skylar Compliance hostname as the syslog message source, add the hostname to Syslog Source Hostname. Note that the facility setting only applies to forwarded Skylar Compliance logs, not forwarded operating system events.
- ***Syslog Version***. Choose the syslog version from the drop-down menu.
- ***Syslog Source Hostname***. Type in the hostname for your Syslog source.
- ***Protocol***. Chose the protocol from the drop-down menu.
- ***Primary Server***.
    - *Host*. Type the Host name or IP address for your primary server. You can also click **[Ping]** to verify communication.
    - *Port*. Type the port you primary server will use. For more information, see *Firewall Requirements*.
- ***Secondary Server***.
    - *Host*. Type the Host name or IP address for your primary server. You can also click **[Ping]** to verify communication.
    - *Port*. Type the port you secondary server will use. For more information, see *Firewall Requirements*.
    - *Facility*. Select the facility for your server from the drop-down menu.

- ***Use SNMP Traps***. Select this checkbox to forward log messages as SNMP traps to a Network Management Server (NMS). You will need to enter the NMS IP Address, the SNMP Version, and the community string.

Compliance Retention Policies

- ***Transcripts Retention Policy***. Enter a value to define how long transcripts for compliance policies should be kept before being deleted automatically.

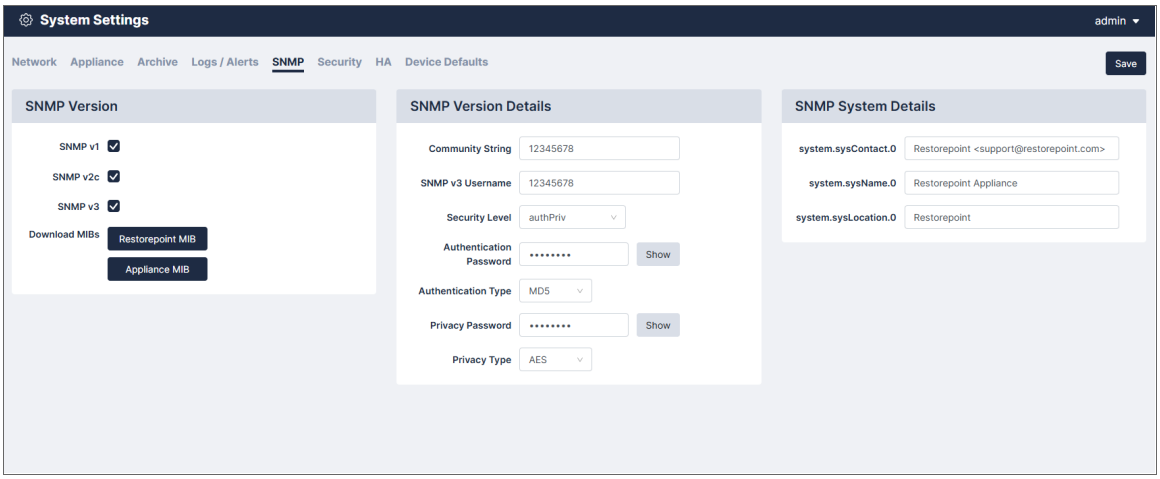
Alerts

- ***Enable Email Alerts***. Select this checkbox to receive emails if an alert is triggered.
- ***Email errors to***. Enter the email address to which emails should be sent if an alert is triggered.
- ***Email from domain***. Enter the domain from which emails should be sent if an alert is triggered.
- ***Hostname***.Enter the hostname that will be used for links generated by Skylar Compliance.
- ***Plaintext emails***. Check this box to remove any HTML formatting from email alerts.
- ***SMTP Server Host***. Enter the host of the SMTP email server that will be used to send email alerts.
    - **[Resolve]**. Click this button to try and resolve the defined host address.
    - **[Ping]**. Click this button to ping the defined host address.
- ***SMTP Server Port***. Enter the port of the SMTP email server that will be used to send email alerts. Clcik **[Test SMTP]** to send a test email to the defined SMTP server.
- ***Verify Certificate***. Check this box to check the SMTP server certificate against the certificates trusted by the appliance, including any chain marked *SMTP server* under **Trusted CA Certificates**. This option is always on when FIPS mode is enabled.
- ***Change Creds***. Check this box to display the username and password of the SMTP server so that you can update them, if needed.

The SNMP Tab

If your network has a Network Management System, you can use SNMP to perform some basic monitoring of your Skylar Complianceappliance. Skylar Compliance supports SNMP v1, v2c, and v3. To configure SNMP:

1. Navigate to the **SNMP** tab (Administration > System Settings > SNMP).
2. Supply values in the following fields:
    - Select which SNMP versions should be enabled by selecting the relevant checkbox.
    - If you enable SNMP v1 or v2c, you must enter a **Community String** in the appropriate field.
    - If you enable SNMP v3, you must define a username. Depending on the SNMP v3 security level, you may need to enter additional integrity/encryption passwords and integrity/encryption algorithms.
3. Click **Save**.

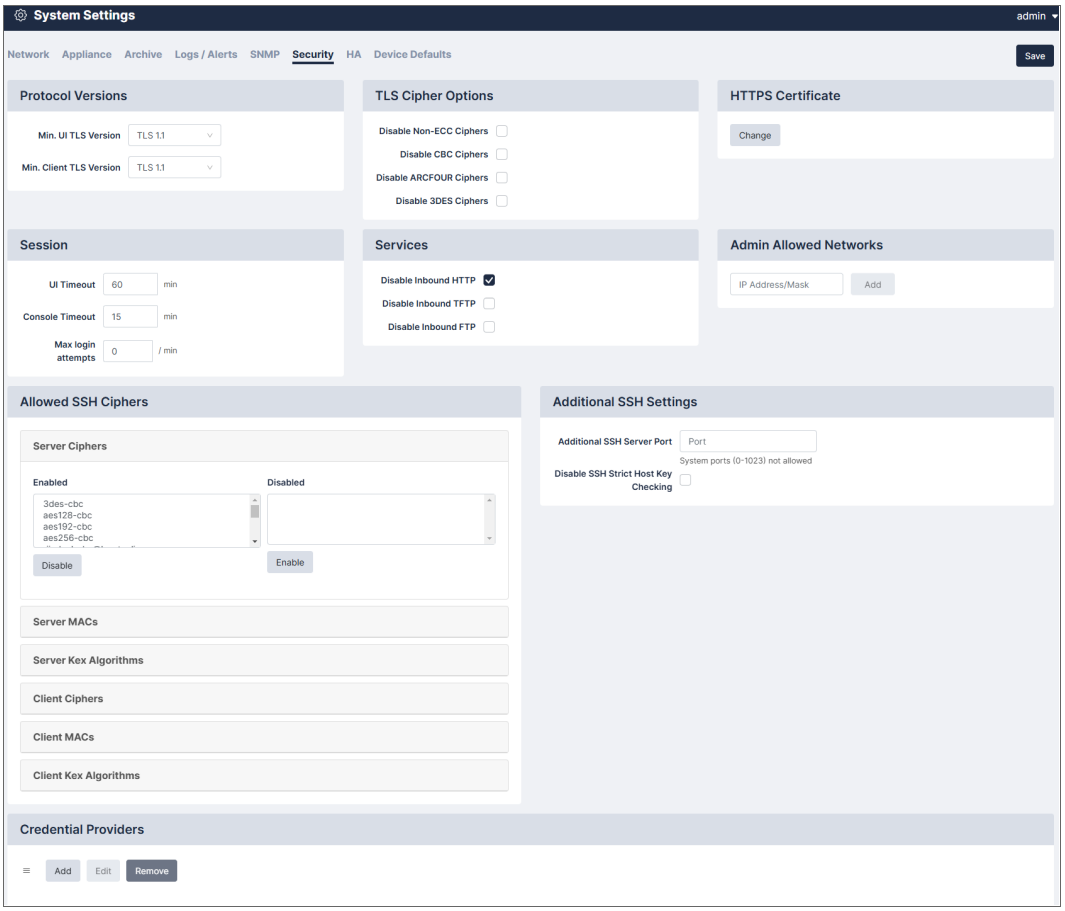


NOTE: **SNMP** settings (Administration> System Settings>SNMP) may need to be reset/updated after upgrading to 5.6.

The Security Tab

The **[Security]** tab (Administration > System Settings > Security tab) allows you to configure various global settings to mandate a higher level of network security for the Skylar Compliance appliance.

IMPORTANT: Applying some of these settings may cause compatibility problems with legacy devices and clients.



Protocol Versions

The Protocol tab allows you to specify the minimum version of TLS that the Skylar Compliance UI can use and can communicate with devices. You can also prevent Skylar Compliance from falling back to SSHv1, if TLS is unavailable.

TLS Cipher Options

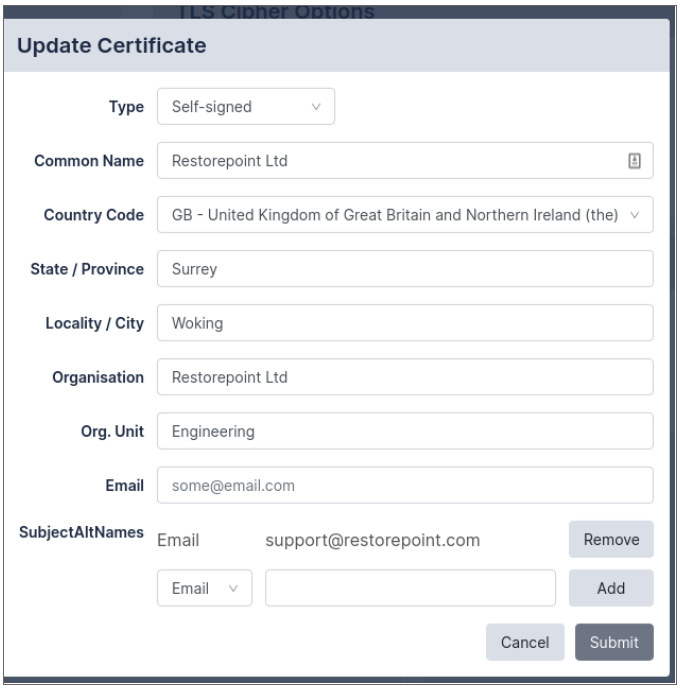
To set your TLS Cipher Options, select the checkbox that you desire.

Services

You may wish to disable some functionality of Skylar Compliance for reasons such as PCI Compliance.

HTTPS Certificate

Click **Change** to modify the HTTPS certificate used by Skylar Compliance. The following dialog appears:



The **Type** drop-down will show you the different options available:

- ***Self-Signed***. Generates a self-signed HTTPS certificate with the current keypair.
- ***New Key***. Allows you to generate a new private/public keypair of the given length.
- ***Create CSR***. Allows you to generate a Certificate Signing Request, which your Certificate Authority (CA) will need to produce a signed certificate.
- ***Upload Certificate***. Once you have a signed certificate from the CA, you can upload it here.
- ***Upload All***. Alternatively, if you have a key/certificate pair already from your CA, you can upload both of them here.

Session

To set the timeout values, complete the following fields:

- ***UI Timeout***. How long a user may stay logged-in to the Skylar Compliance user interface without making a change or initiating an action. Default value is *60 minutes*.
- ***Console Timeout***. How long to keep a session for the VM Console open without an action. The default value is *15 minutes*.
- ***Max login attempts***. Allows you to automatically set users' maximum login attempts per minute. Default value is *0 minutes*. For more information, see *Managing Users*.

Admin Allowed Networks

This pane allows you to set a range of IPs (in CIDR format) that administrator accounts can connect from. For a per-user setting, see *Managing Users*.

Allowed SSH Ciphers

Skylar Compliance allows you to configure several different SSH ciphers. The ***Allowed SSH Ciphers*** pane (Administration > System Settings > Security) contains the following allowed SSH ciphers:

- Server Ciphers
- Server MACs
- Server Kex Algorithms
- Client Ciphers
- Client MACs
- Client Kex Algorithms

Additional SSH Settings

The additional SSH Settings allow you to configure your system settings further.

- ***Additional SSH Server Port***. Enables users to define another SSH host port the appliance should listen to for incoming SSH connections. This allows the agent to establish the initial SSH connection to the appliance. Defining the value changes the `sshd_config` to listen on that port in addition to port 22 and adapts the firewall rule accordingly.
- ***Disable SSH Strict Host Key Checking***. Disables the SSH host key validation for all devices and logs when the key changed.

Request Settings

Request settings allows you to configure the maximum body size for requests. These new options enhance system security:

- ***Max body size*** (in MB). Sets the maximum requests for body size for all requests. The default is 100MB.
- ***Max file size*** (in MB). Sets the maximum file size for requests that upload files. The default is 10MB.

SSH

The SSH settings allow you to clear existing keys or to upload or generate new SSH keys.

Known Hosts

To clear existing SSH keys:

1. Click the **[Clear]** button if you want to delete all SSH keys from all previously known devices.
2. Click the **[Save]** button in the top right corner of the screen.

Key Management

To upload new SSH keys:

1. Select the ***Upload new SSH keys*** radio button.
2. Complete the following **RSA** fields:
   - ***Public Key***. Enter the new RSA public key.
   - ***Private Key***. Enter the new RSA private key.
3. Complete the following **DSA** fields:
   - ***Public Key***. Enter the new DSA public key.
   - ***Private Key***. Enter the new DSA private key.
4. Click the **[Save]** button in the top right corner of the screen.

To generate new SSH keys:

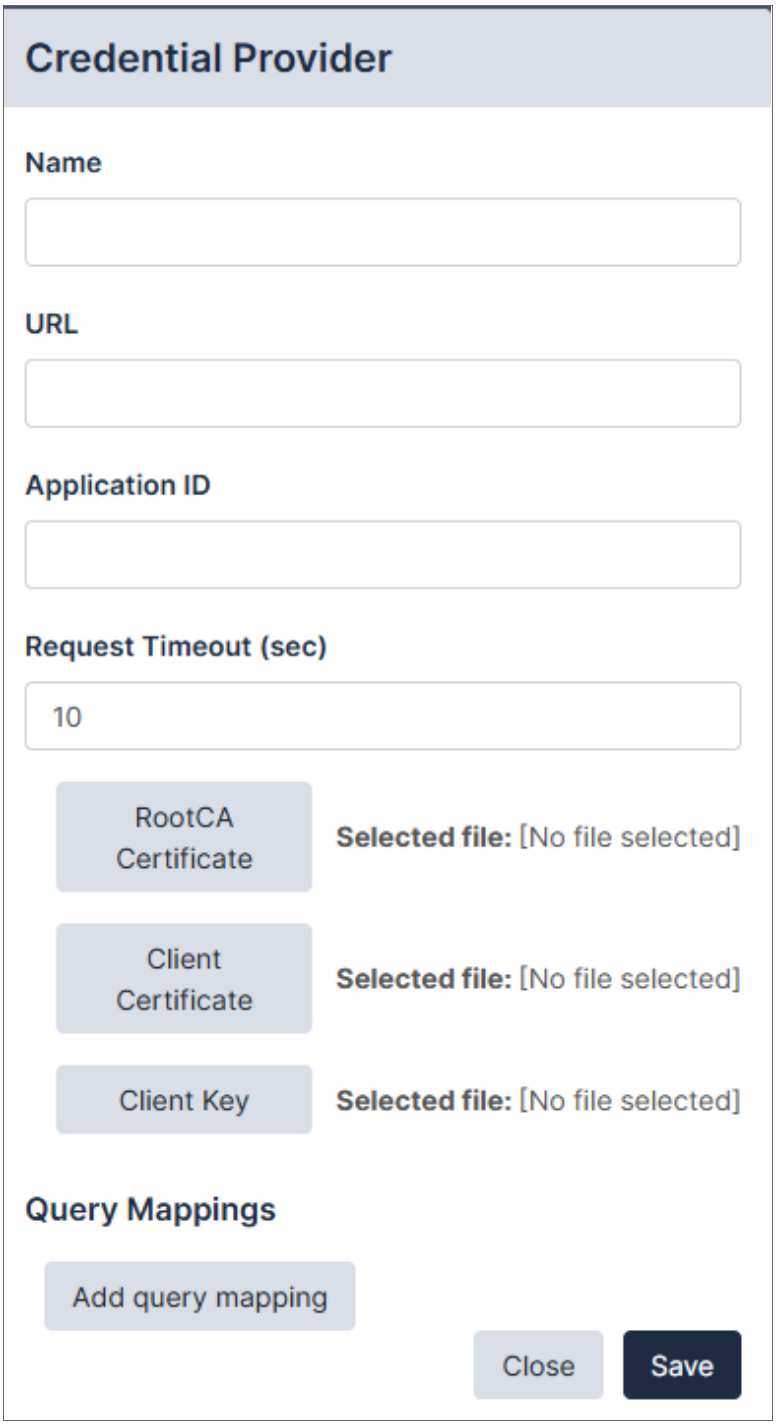
1. Select the ***Generate new SSH keys*** radio button.
2. Click the **[Generate new SSH keys]** button. A confirmation window appears.

> IMPORTANT: Generating new SSH keys will affect any device using the current RSA or DSA public key.

3. Click **[OK]** if you want to generate new SSH keys.
4. Click the **[Save]** button in the top right corner of the screen.

Credential Providers

The ***Credential Providers*** pane is currently only available for CyberArk users. The credential provider allows you to import credential sets and assign them to devices.



Trusted CA Certificates

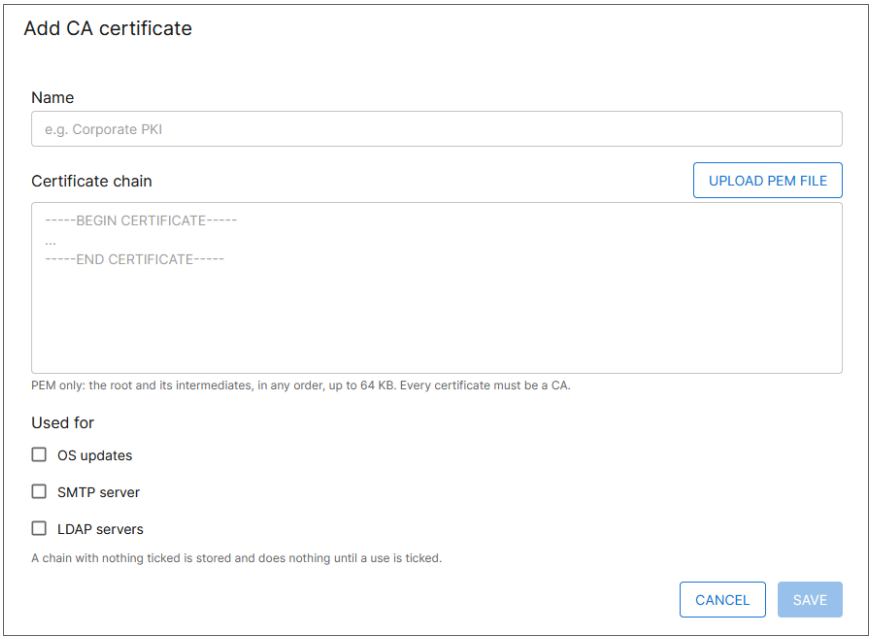
In this section, you can upload trusted CA certificate chains that Skylar Compliance should trust when connecting to your own servers.

This section lists all of the certificate chains on the system, and it displays the root subject, number of certificates, earliest expiry (amber within 30 days, red when expired), root SHA-256 fingerprint and uses for each certificate chain. You can expand a row to see every certificate.

Only CA certificates are accepted; a server certificate is rejected, and an incomplete chain is flagged but can still be saved. You can store up to 50 chains.

To add a certificate:

1. Click **[Add CA certificate]**. The **Add CA certificate** dialog appears.



2. In the ***Name*** field, type a name for the certificate.
3. In the ***Certificate chain*** field, paste the PEM chain or click the **[Upload PEM File]** to upload the PEM chain (root and intermediates, in any order, up to 64 KB).
4. In the ***Used for*** section, you can select OS updates, SMTP server, LDAP servers.
5. Click Save.

You can edit or delete a chain from this section; deleting asks for confirmation and lists the uses affected. These certificates do not change the operating system trust store. Changes are recorded in the system log.

The High Availability (HA) Tab

High Availability (HA) provides a way to minimize the effects of hardware failure, by configuring two Skylar Compliance appliances in a cluster.

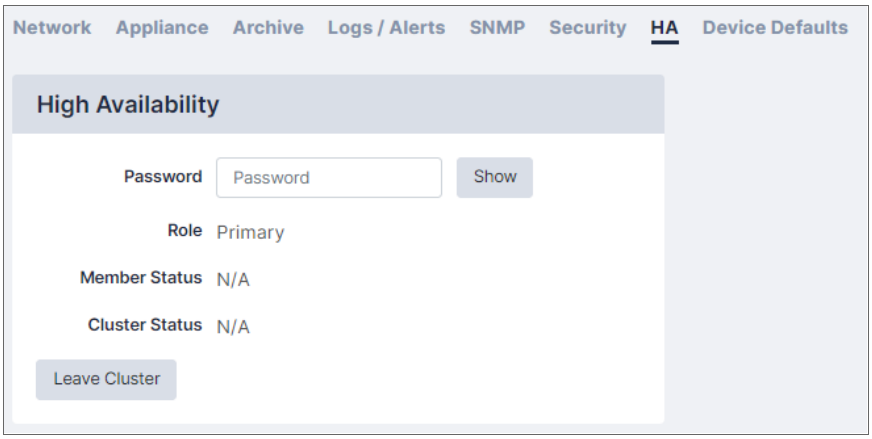
Under normal operating conditions, the primary cluster member is active and the secondary is in standby mode; the active appliance performs all network operations, and replicates all settings and device

configurations to the standby appliance. Skylar Compliance replicates data both incrementally (for example, just after a backup is retrieved from a device) and by performing full synchronizations on a regular basis.

If the primary member becomes unavailable because of a hardware failure, other network problem, or from losing power, the secondary member will automatically become Active, and carry on as normal. If the primary recovers, it will automatically take over from the secondary and become active.

HA does not require the appliance to be installed on the same network, as long as the traffic requirements are met (see below).

Software updates and upgrades are managed at the cluster level; updating the active appliance will automatically update the standby appliance.



HA Requirements

- HA is a separately licensed feature.
- Only appliances of the same model can be clustered and appliances must be running the same software version.
- Cluster members must be able to communicate over HTTPS to exchange heartbeat information and data synchronization. TCP/443 traffic should be permitted bidirectionally between the appliances.

Creating a Cluster

To create a cluster, on the Primary Skylar Compliance appliance:

1. Click **[Create Cluster]**.
2. Type a password to be used between appliances in the cluster.
3. Click **Save**.

On the secondary Skylar Compliance appliance:

1. Click **[Join Cluster]**.
2. Enter the same password you entered on the Primary appliance.

3. Enter the IP Address of the Primary appliance.
4. Click **[Save]**. The cluster will perform the initial full sync.

After the cluster is created, this screen can be used to monitor the status of the cluster or to leave the cluster.

- **Role** displays which position the appliance takes in the cluster (*Primary* or *Secondary*).
- The **Member Status** displays if the current appliance is *Active* or *Standby*.
- The **Cluster Status** displays the status of the Secondary appliance on the Primary or the amount of time between heartbeat synchronizations on the Secondary.

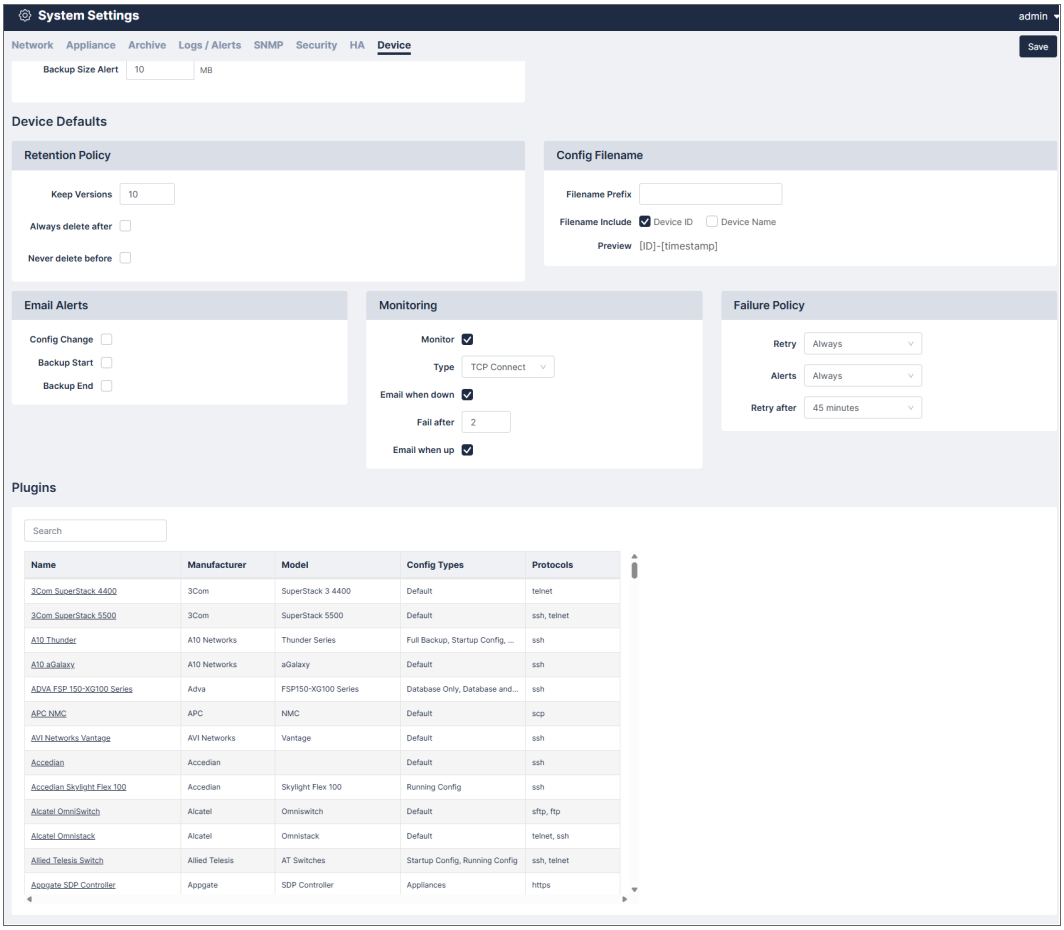
You can use the **Leave Cluster** button to break the cluster. When you click Leave Cluster, all synchronization will stop, the two appliances will keep the existing configuration, and the appliances will carry on independently.

The Device Tab

The **[Device]** tab allows you set the device defaults for your system. Complete the following fields in the **Device Defaults** section for your device's default settings:

- ***Global Device Settings***. Set the backup size alert when you have reached backup size limits. Available for administrators only. See *Global Devices*.
- ***Device Defaults***.
    - *Retention Policy*. First, select what versions to keep. Then, choose when to ***Always delete after*** (in days/weeks/months) and ***Never delete before*** (in days/weeks/months).
    - *Config Filename*. Enter your ***Filename Prefix***, what to include (***Device ID*** or ***Device Name***), and see your selection's ***Preview***.
    - *Email Alerts*. Choose whether or not you'd like an email to be sent when there is a ***Config Change***, ***Backup Start***, and/or ***Backup End***.
    - *Monitoring*. Choose your monitor device settings. These include your ***Type***, ***Email when down***, and ***Email when up***.
    - *Failure Policy*. Set when your failure policy should ***Retry***, ***alert*** (Always, First Failure, or Never), and/or when to ***Retry after*** (in minutes).

- ***Plugins***. Configure your plugin options and redact rules. See *Plugins*.

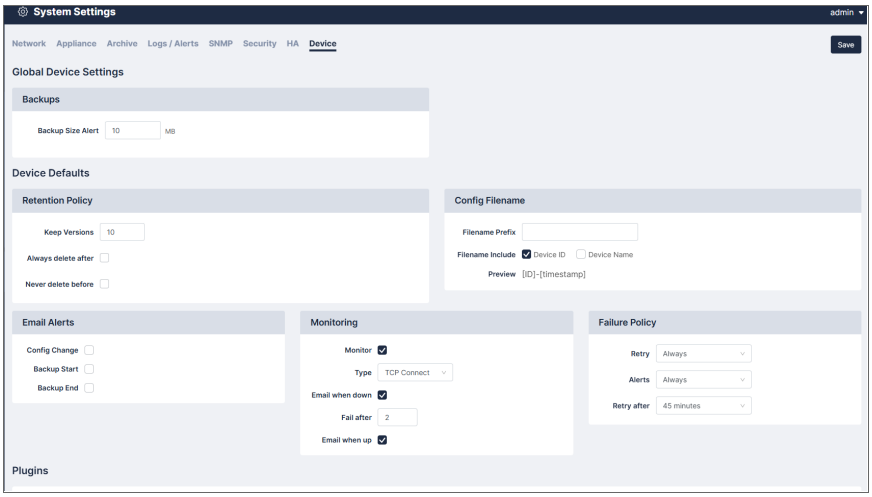


Global Devices

The **Global Device Setting** on the **[Device]** tab allows users to set backup size alerts when you reach the backup size limits.

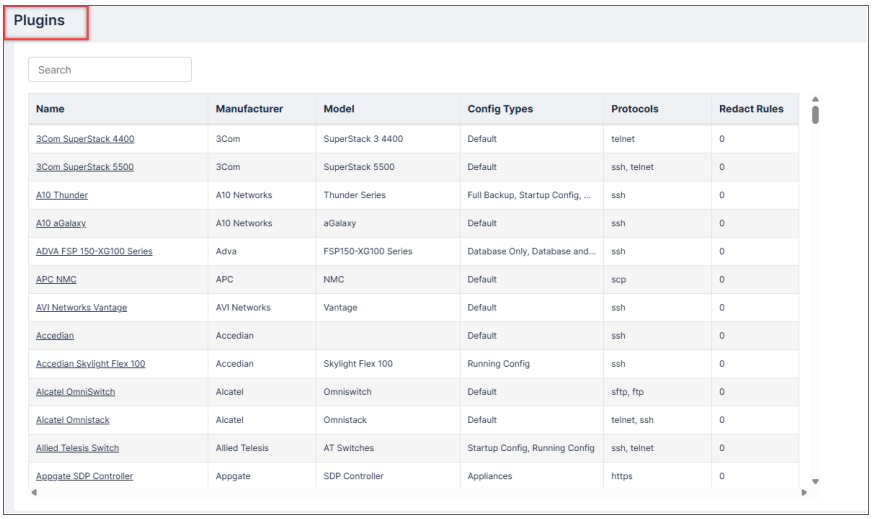
- ***Global Device Setting***. Select the ***Backup Size Alert*** to a value in megabytes (MB).
    - If the value is larger than 0, every new backup size will be compared against this value. If the backup size exceeds this value, an alert will trigger an email to the appliance owner.
    - If the value is 0, no alert will be triggered and no email will be sent.

Click **[Save]** when finished.



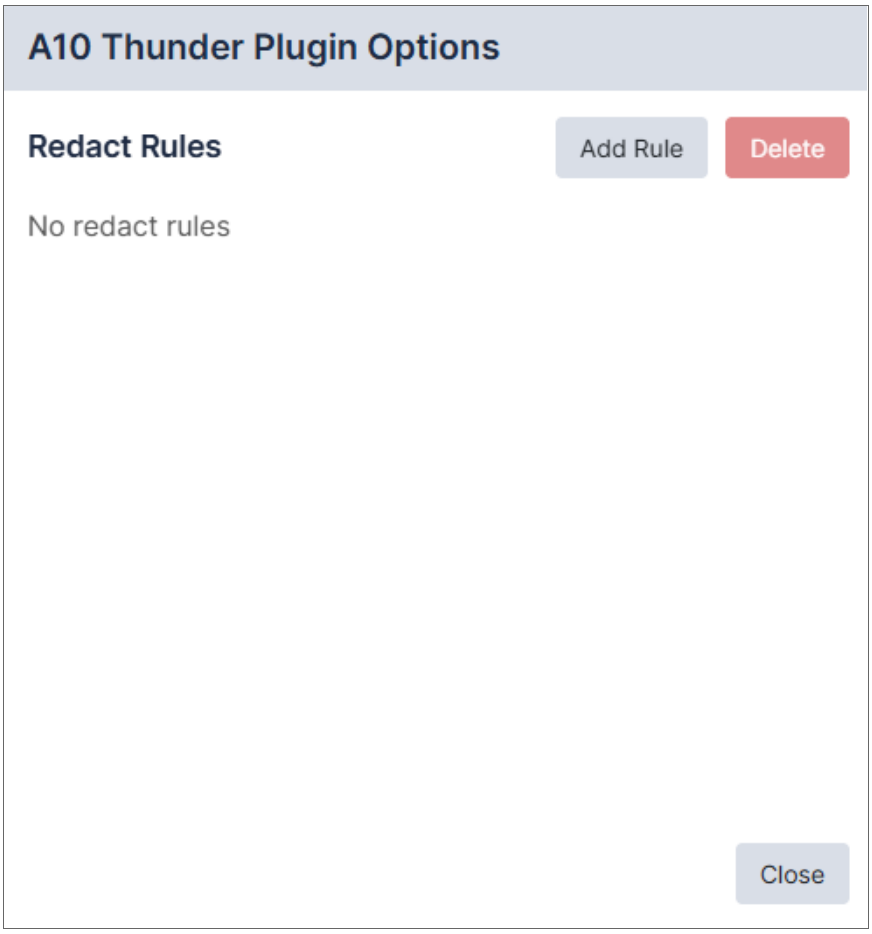
Plugins

The **Plugins** on the **[Device]** tab allows users to set the ***Redact Rules*** for each of your plugins. Users must have permissions for `ViewPluginOptions` and `ModifyPluginOptions` to view and edit the plugin options and the ***Redact Rules*** for the plugin.

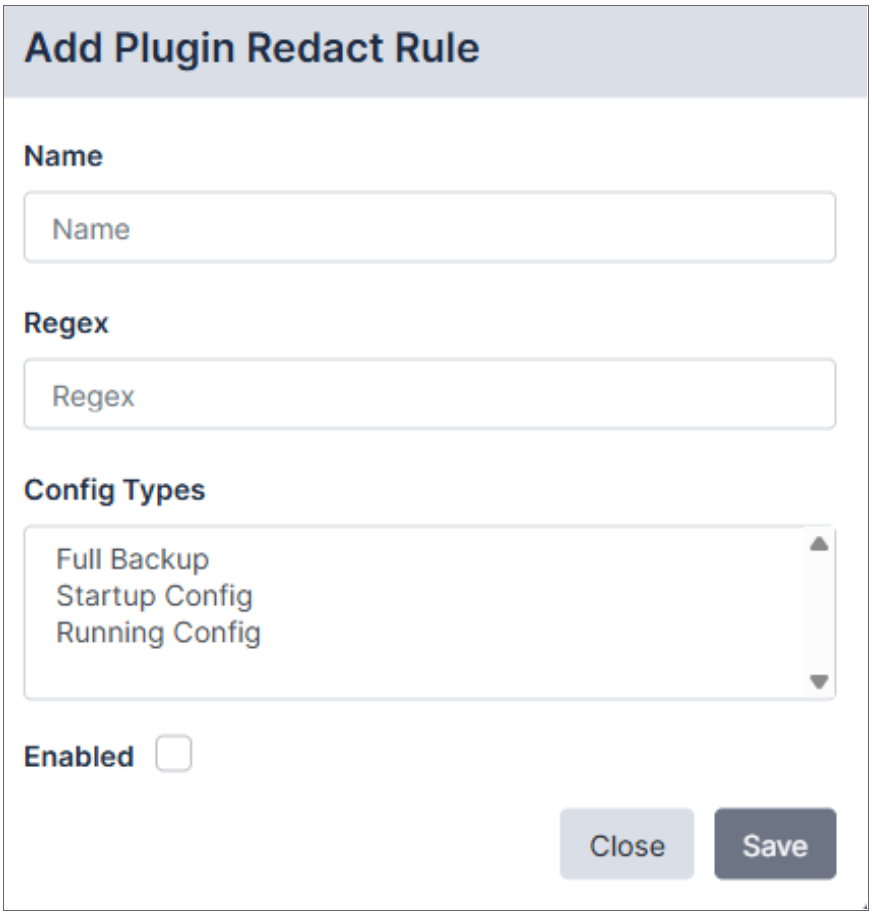


To add a ***Redact Rule***:

1. Go to **Plugins** on the **[Device]** tab.
2. Click on your plugin. The **Plugin Options** modal appears.



3. Click the **[Add Rule]** button for ***Redact Rules***. The **Add Plugin Redact Rule** modal appears.



4. Complete the following fields:
    - ***Name***. Type a name for your ***Redact Rule***.
    - ***Regex***. Choose the Regex Expression to redact the file. You can redact a whole or partial line.
        - To redact a whole line, use a Regex without a capture group. Any lines that match will be completely redacted. For example:

          Line: `Server IP: 1.2.3.4`

          Regex: `IP: \d+\.\d+\.\d+\.\d+`

          Result: `[REDACTED]`

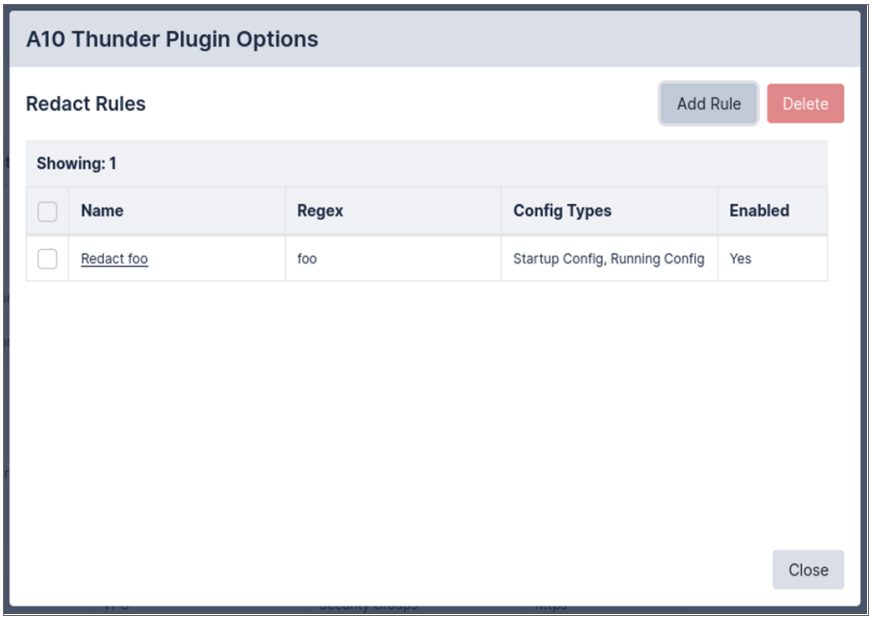
        - To redact part of a line, use a Regex with a capture group to specify the exact part of the line to redact. For example:

          Line: `Password = "secret"`

          Regex. `Password = "(.*)"`

          Result. `Password= "[REDACTED]"`
    - ***Config Types***. Select the type of configuration that applies to your ***Redact Rule***.
    - ***Enabled***. Select the checkbox to enable your ***Redact Rule***.

5. Click **[Save]**.
6. The ***Redact Rule*** will appear under your plugin options.



Plugin Redact Rules Caveats

The following permissions apply to the Plugin ***Redact Rules***:

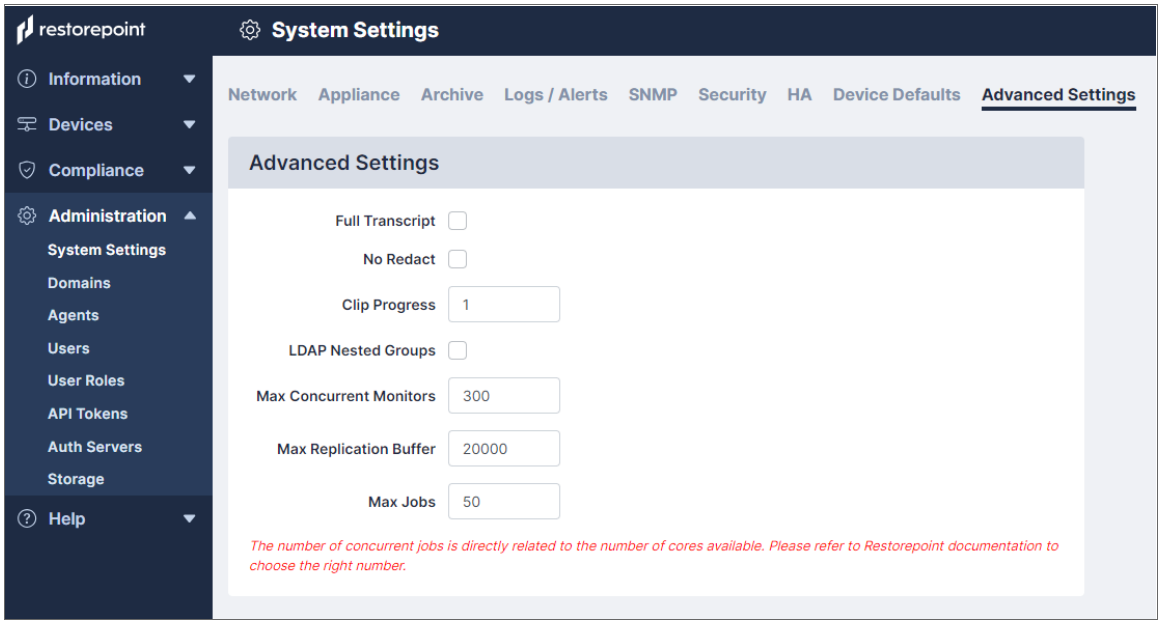
- Users can configure plugin ***Redact Rules*** on a plugin basis.
- All users with the `ViewBackup` permission also have the `ViewUnredactedBackup` permission which allows you to view unredacted backups.
- When you configure a rule, users without the `ViewUnredactedBackup` permission will see the backups redacted.
- Redaction rules were applied to the following backups:
    - View Backup
    - Compare Config
    - Download Config
    - View Config on the Global Search
- Emails are not redacted for email notifications when ta configuration is changed.
- Adding redaction rules to devices with large backups (>100mb) might significantly increase their download time.

Advanced Settings

You can configure several advanced settings on the **[Advanced Settings]** tab of the **Administration** page (Administration > System Settings > Advanced Settings).

TIP: To access the **[Advanced Settings]** tab, Skylar Complianceрequires that you contact ScienceLogic Support to enable it. Access will be restricted until you contact Support.

To configure your advanced settings, complete the following fields:



- ***Full Transcript***. Select this option to enable or disable the ability to write the entire transcript file or to maximize size buffer. The default is set to False.
- ***No Redact***. Select this option to enable or disable the ability to redact sensitive information from log messages, such as passwords. The default is set to False.
- ***Clip Progress***. Number of characters to clip from the beginning and end of a progress message. The minimum value is 0 and the maximum value is 500. The default value is set to 0.
- ***LDAP Nested Groups***. Select this option to enable or disable the use of nested LDAP groups. The default is set to False.
- ***Max Concurrent Monitors***. Maximum number of rpmonitors that can be enabled. The minimum value is 50 and the maximum value is 300. The default value is set to 300.
- ***Max Replication Buffer***. Maximum buffer size for jobs a replication worker can have. The minimum value is 15000 and the maximum value is 25000. The default value is set to 20000.

- ***Max Jobs***. Maximum number of concurrent jobs that you can run. The minimum value is 50 and the maximum value is 150. The default value is set to 50.

Chapter 17

Domains

Overview

The **Domains** page (Administration > Domains) lets you organize devices into separate domains and delegate their management to domain administrators.

Service providers typically use this feature to restrict the scope of administrators to a subset of network devices.

> **IMPORTANT:** Domains are only available with an Enterprise license.

This chapter covers the following topics:

Skylar Compliance Domains *162*

Managing Domains *167*

Administrator Roles *170*

Adding a New Domain User *171*

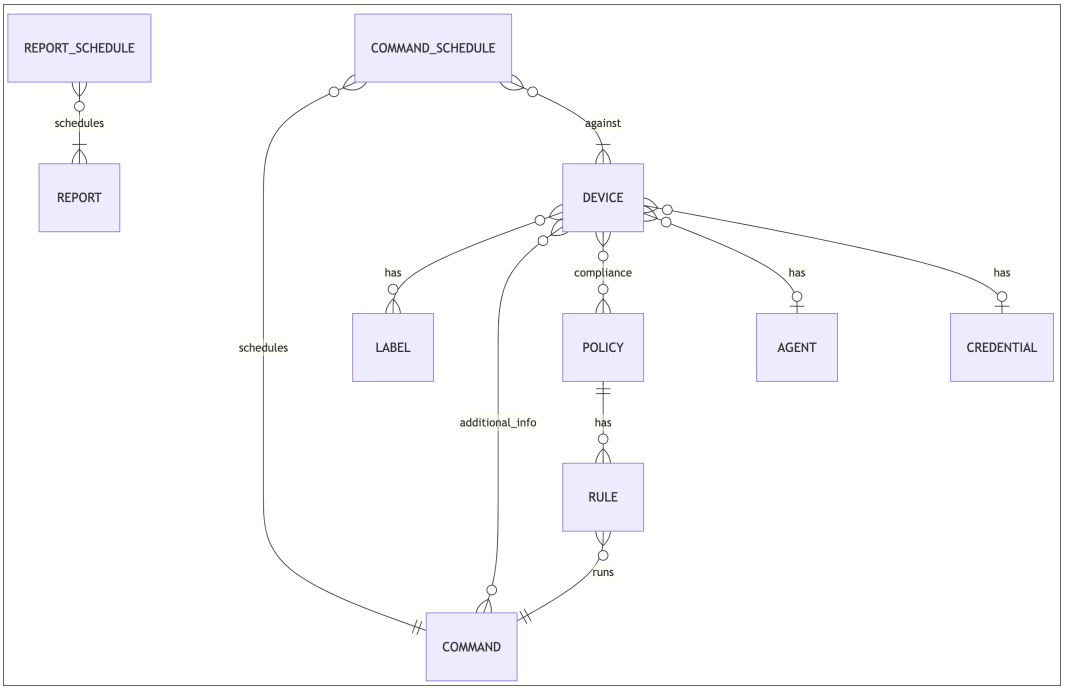
Editing Devices *174*

Skylar Compliance Domains

Access to administer Skylar Compliance domains is highly controlled by the use of different access permissions assigned to the user.

How Domains Work

Skylar Compliance has a concept of a global domain and domains specific to a customer or administrative group. This section explains the hierarchical nature of the elements controlled within a domain. As you can see in the diagram, control flows from the bottom elements to the top. For example, Rules are part of a Policy. A Policy is applicable to a Device, and so on. This is important to understand when configuring domain permissions, since domain permissions respect this hierarchy.

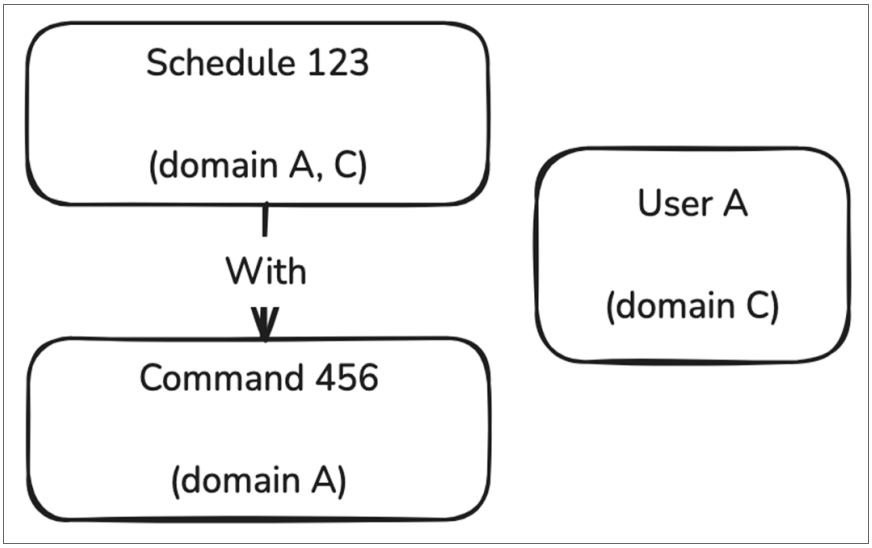


Rules That Govern Domains

The following rules and examples are provided to give you context into how domains work. This is not something that requires user configuration.

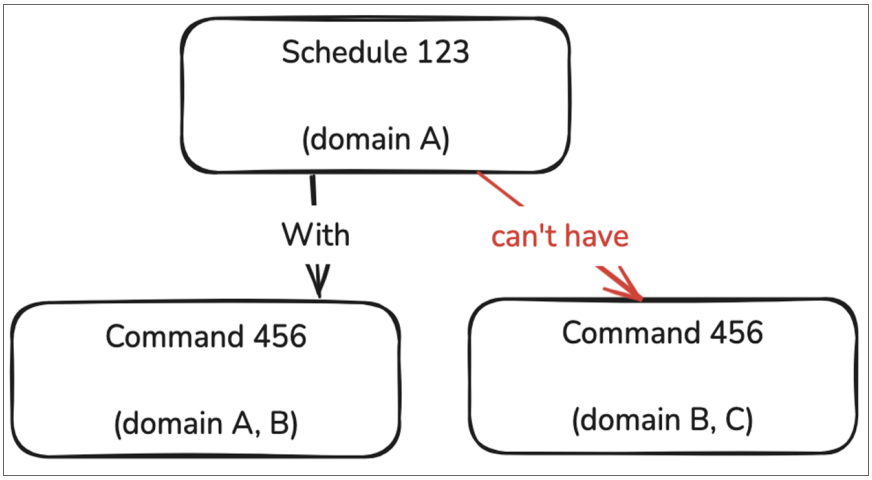
Rule: If any entity can be assigned other domain-specific entities, then the entity cannot belong to more than one domain.

Example: If a user and a schedule are in Domain C, but a given command is in Domain A ***and*** the schedule is also in Domain A, then the user cannot see a schedule that contains the command belonging to Domain A. This prevents the user from seeing anything that doesn't belong to the Domain to which the user belongs.



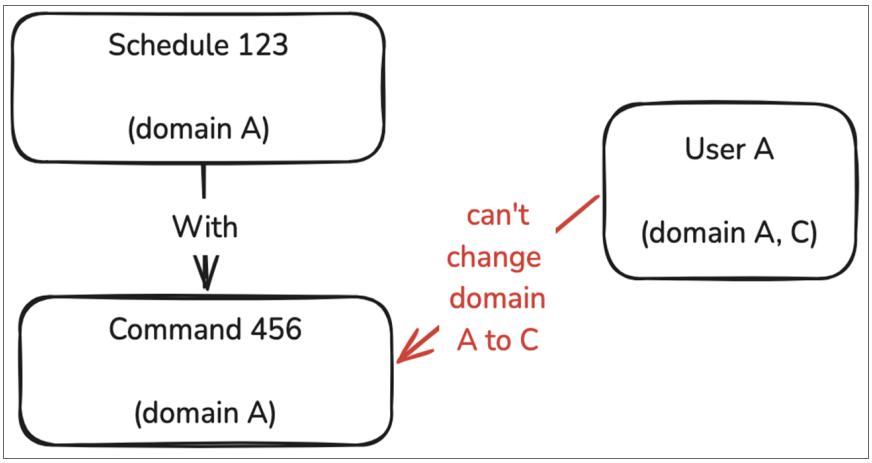
Rule: A relationship between non-global entities can only exist if they share a Domain.

Example: If a schedule belongs to Domain C, it cannot contain commands that belong to Domain A.



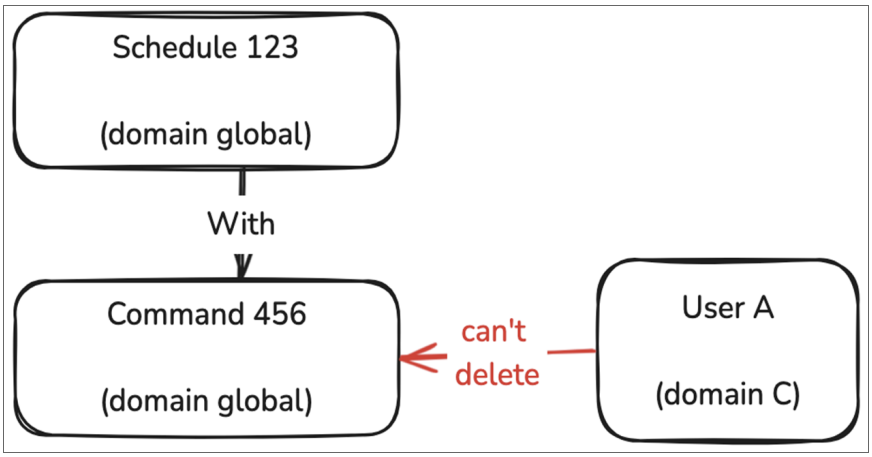
Rule: If two entities share a Domain, a user cannot remove the shared Domain without breaking the relationship. However, a user can change the shared Domain to global.

Example: If a command is in a schedule and both share Domain A, a user cannot remove Domain A.



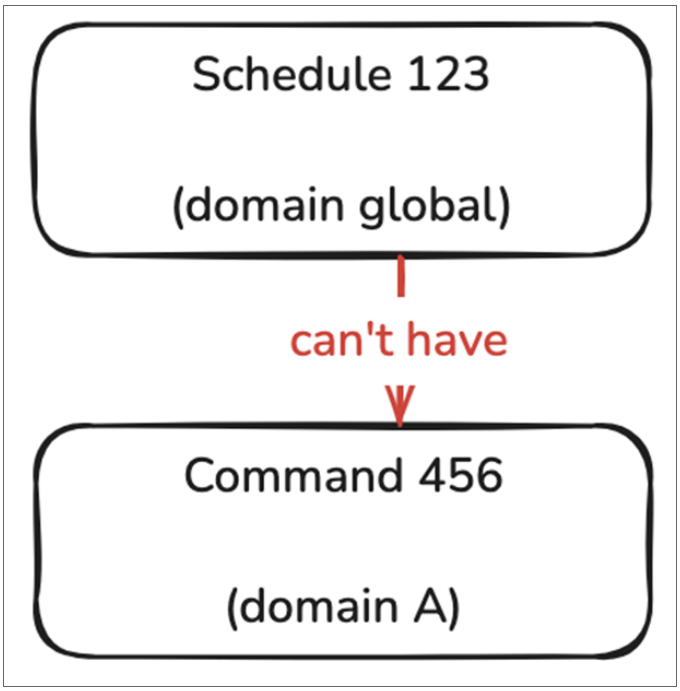
Rule: If a resource is assigned to another, the relationship must be removed before deleting the resource.

Example: A user cannot delete a command that is assigned to a schedule.



Rule: A non-global entity cannot be assigned to global entities.

Example: A non-global command cannot be assigned to a global schedule.



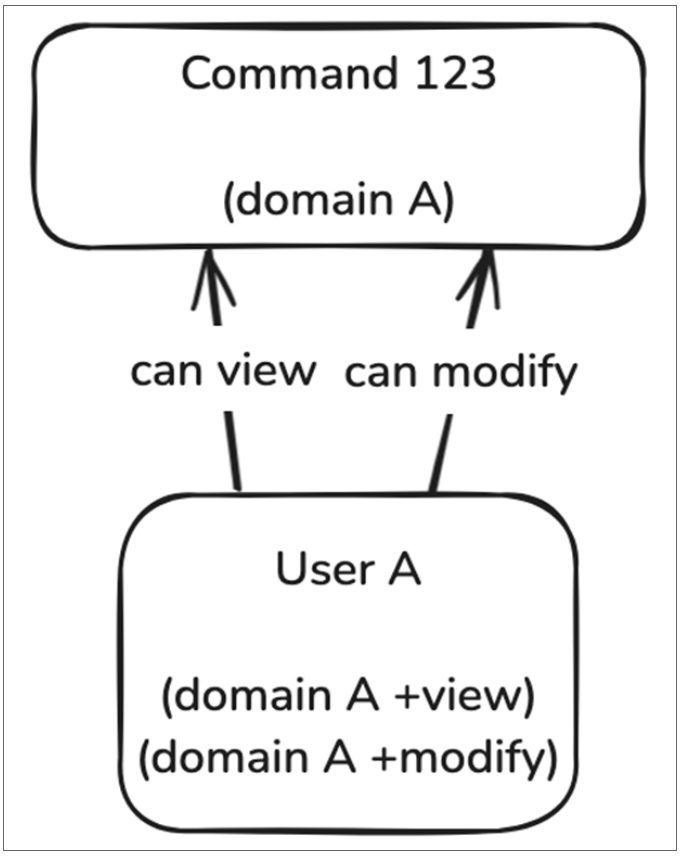
Domain Permissions

The following rules apply when you need to consider user permissions as they apply to domains:

Domain Permission Rules

- **Rule 1**: If a resource is assigned to a single domain, user permissions under that domain should be used to allow the user to view or modify the resource.

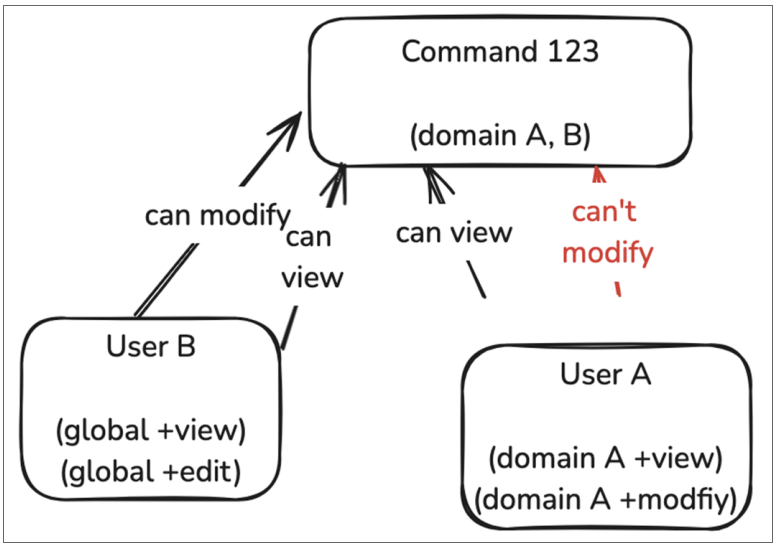
  Example: Because User A in Domain A has both the Command *View* and *Modify* permissions under Domain A, the user can view and modify every command assigned to Domain A.



- **Rule 2**: If a resource is assigned to more than one domain, only users assigned to the global domain (or users with the permissions to modify that resource on the specified domains) can modify the resource if they have the permissions. Users within the same domain as the resource can view it if they have the correct permission assigned in that domain.

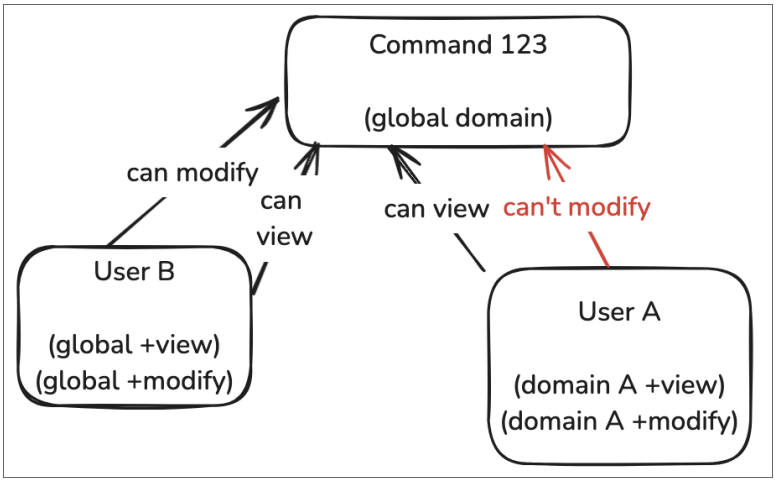
  Example: "Command 123" has both Domain A and B. User A (from Domain A) has both the Command *View* and *Modify* permissions and is able to see " Command 123", but not modify it.

  User B has Command *View* and *Modify* permissions under the Global domain, so they can both modify and view "Command 123".



- **Rule 3**: If a resource is assigned to the global domain, all users can see the resource but only users with the *Modify* permission in global domain can modify the resource.

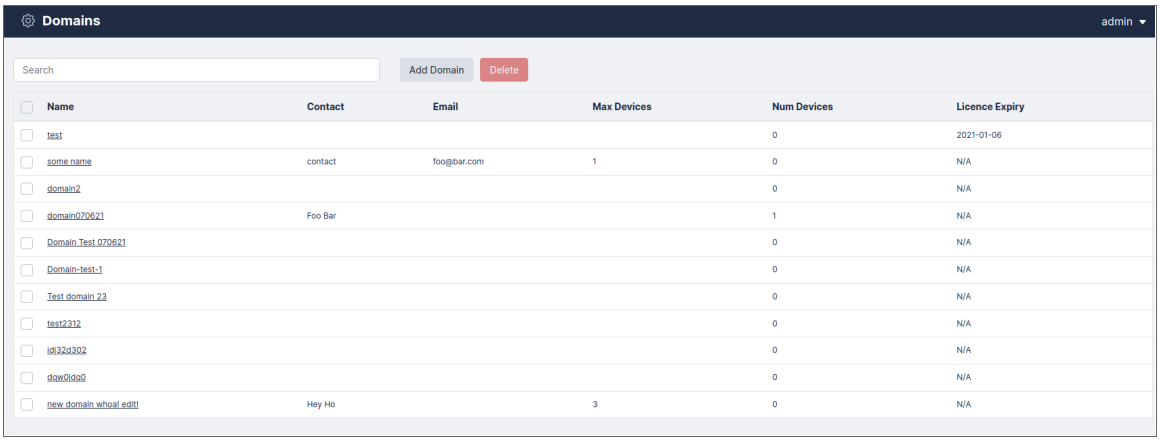
  Example: User A belongs to Domain A and can see the "global Command 123", but can't modify it even if they have the *Modify* permission because they are in Domain A. However, User B has the *Modify* permission and is in the Global domain, so they can edit the global "Command 123".



Managing Domains

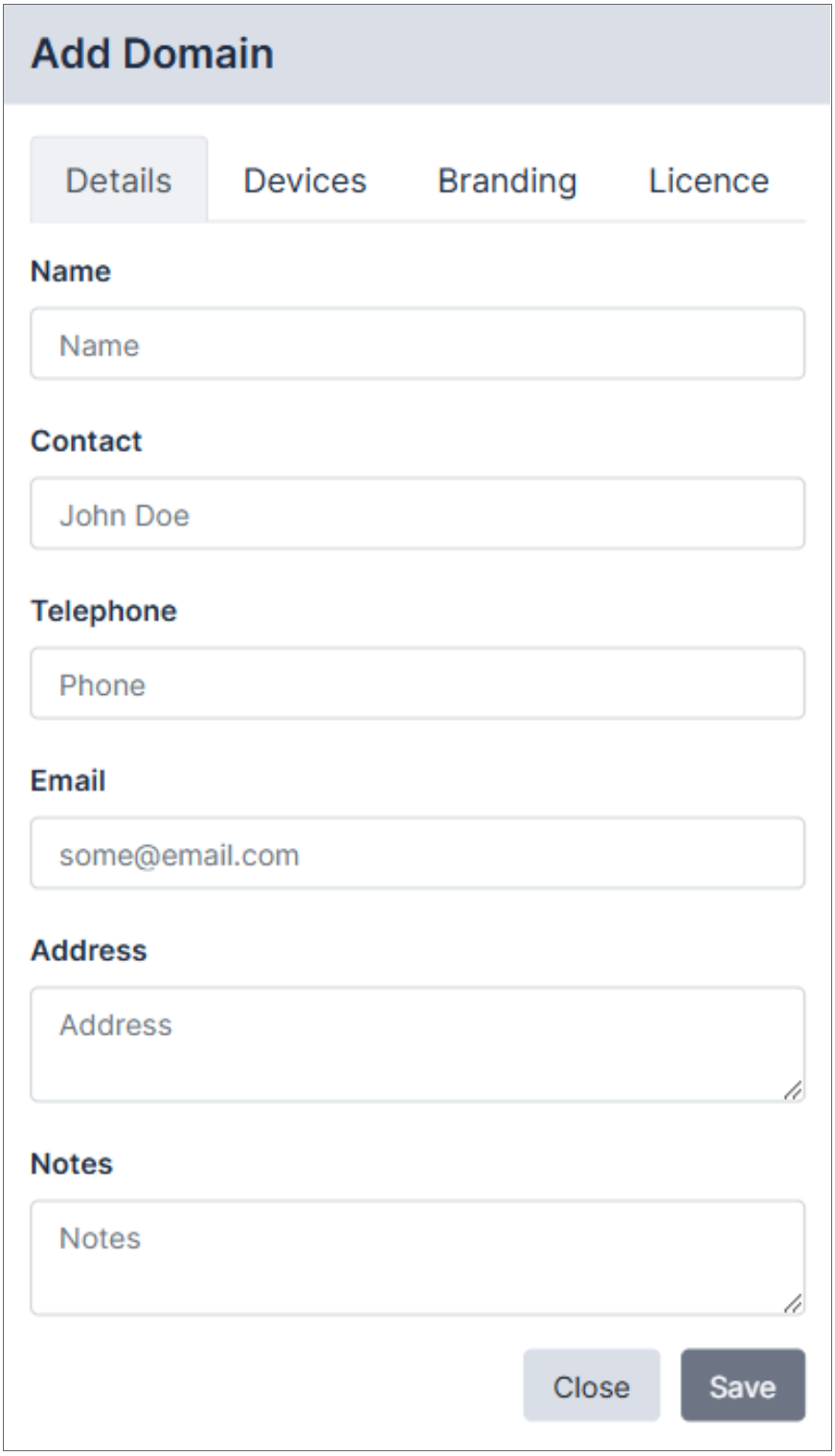
The **Domain Management** page allows you to create, modify, and delete Administration Domains. This page is only displayed if you are logged in as a Global Administrator.

Click **Administration > Domains** on the menu to display the domain list:



To add a new domain:

1. Click **[Add Domain]**. The **New Domain** page appears:



2. Complete the following details:
    - ***Name***. Type a name for the domain, for example Customer Name, Business Unit, and so on.
    - ***Contact***. (Optional) Type the name of the main contact for the domain.
    - ***Telephone***. (Optional) Type a contact telephone number.
    - ***Email***. (Optional) Type a contact email.
    - ***Address***. (Optional) Type a customer or Business Unit address.
    - ***Notes***. (Optional) Type any additional information.
3. Click the **[Devices]** tab to use the device selector and add devices to the domain. Additionally, you can configure the following:
    - **Max. devices**: the maximum permitted number of devices that can be added to this domain.
    - One or more IP address ranges that are allowed for this domain.
    - A domain-wide NAT IP address, which overrides the system-wide setting. For more information, see *Network Address Translation (NAT)*. This setting can be overridden by the device-specific setting.
    - The devices that are part of the new domain.
4. Click the **[Branding]** tab (optional) to customize the top left-hand side corner image that will be displayed to a Domain Administrator. Click **[Choose File]** to locate a suitable image file on your PC. For best results, the logo should be exactly 100 pixels wide and up to 100 pixels tall, and no more than 40KB in size.
    - ***Remove License Info***. Hides the expiration date for users in this domain.
    - ***Remove Serial Number***. Hides the appliance serial number for users in this domain.
    - ***Remove Help Menu***. Disables access to help for users in this domain.
5. Click the **[License]** tab (optional) to restrict the domain to expire on a certain date. Click **[Enforce License]** to enable the function, and choose a date.
    - ***Disable Schedule***. Stops all scheduled jobs for this domain when a defined date is reached.
    - ***Prevent User Login***. Disables users of this domain from accessing the appliance when a defined date is reached
6. Click **Save**. The system returns to the domain list.

To edit an existing domain, click the name of the domain.

Administrator Roles

If Administration Domains are enabled, administrators have either a global or a domain scope:

- ***Global Users***. Have visibility and can operate on all the devices on the system, regardless of the domain the devices are assigned to. Logs and status pages display information about all the devices defined on the system. Global users can also assign global credentials to a device that is assigned to a domain.

- ***Domain Users***. Users with at least one domain set. Their visibility is restricted to devices in their own domains. Logs and status pages only display information on the devices in the selected domains.

Skylar Compliance supports six built-in user roles:

- ***Global Admin***. A "Super User" that has full control on any aspect of the appliance:
  - create/modify/delete devices in any domain
  - create/modify/delete global and domain administrators
  - initiate backups and restores
  - change the appliance configuration
  - an encryption password that allows Skylar Compliance to transition from the lock-down state to the normal state
- ***Global Backup***. Backup Operator; can perform backups/restores of devices in any domain, but cannot modify devices, users, or appliance configuration.
- ***Global View Only***. Monitor Operator; can only view existing backups and verify that the system is operating normally.
- ***Domain Admin***. Has full control of devices and users in their domain. Does not have visibility of devices in other domains, cannot modify the appliance configuration, or transition the appliance from lock-down state to normal state. Logs and status screens only display information related to the domain.
- ***Domain Backup***. Can perform backups and restores of devices in their domain.
- ***Domain View Only***. Can only view existing backups, access logs, and status information of devices in their domain.

You can also define custom user roles. For more information, see *Custom User Roles*.

You can use the **Users** page to add or delete administrator or modify their password, scope, or permissions.

Adding a New Domain User

To add a new domain user:

1. Select **Administration > Users** from the menu. Skylar Compliance displays the **User Management** page.
2. Click **Add User**. Skylar Compliance displays the **New User** page as shown:

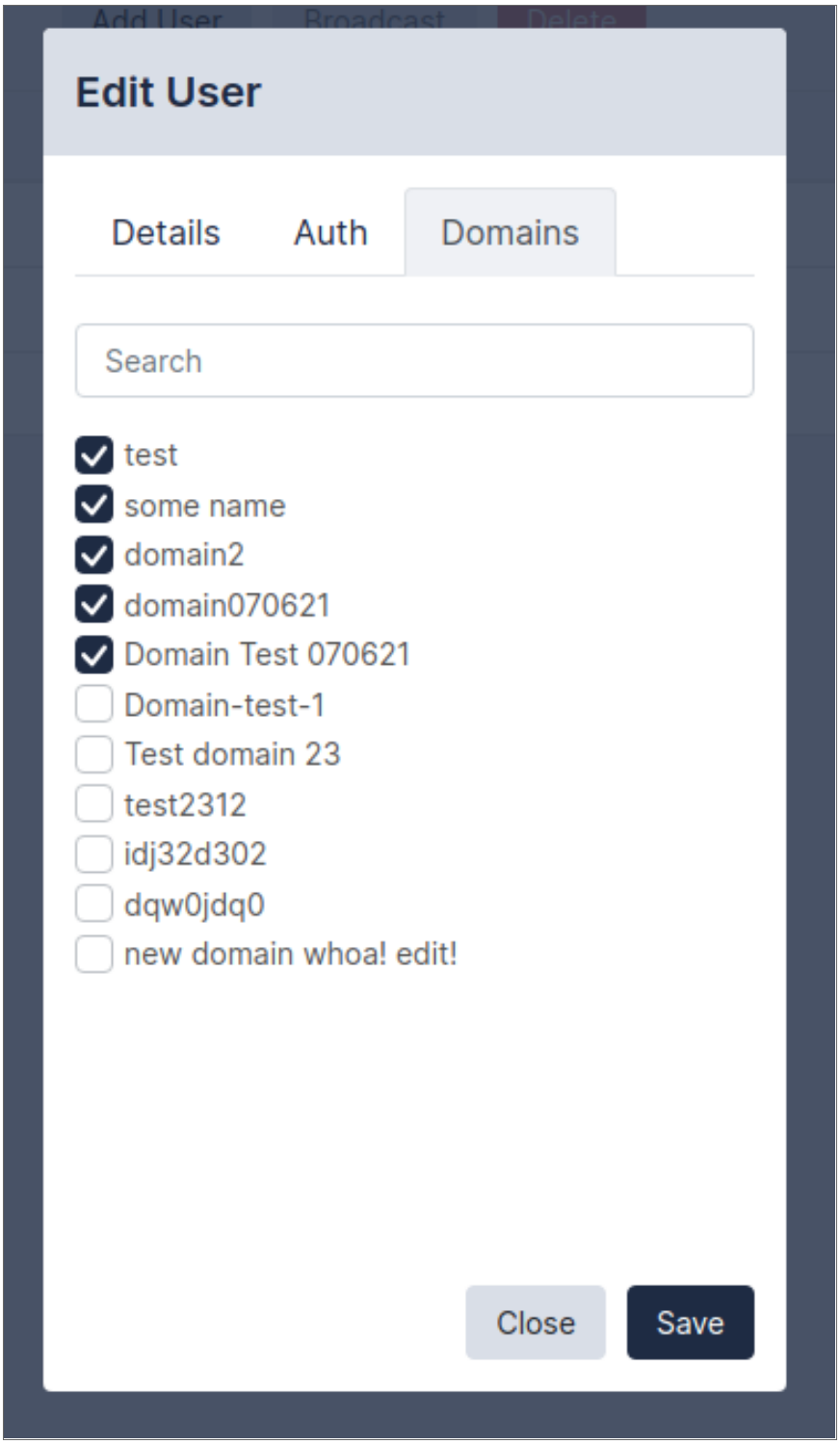
3. Complete the following fields:

   - ***Full Name***. Type the full name of the user.
   - ***Username***. Type the new username (up to 16 characters).
   - ***Password***. Type the password for the new user (passwords must be between 8 and 24 characters long).
   - ***Role***. Select the privilege level from the drop-down list. See for the privileges associated with each admin level.

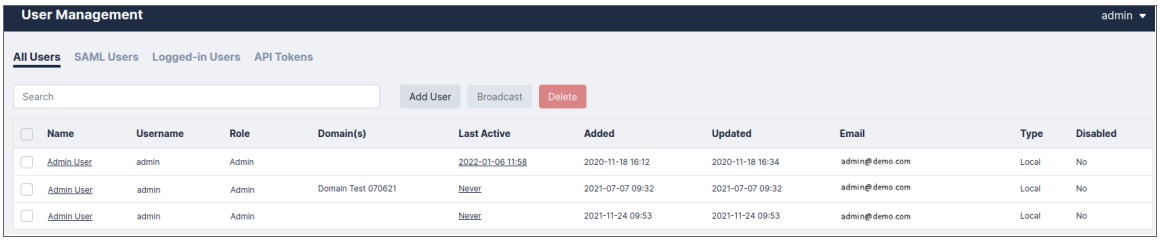
Privileges	View Only	Backup	Admin
View devices/configurations	Y	Y	Y
Run device operations	N	Y	Y
Add users/devices; modify system	N	N	Y

Table 4 : Default Administrator privilege levels (simplified)

Encryption Password	This field appears if an Admin-level administrator is selected. The encryption password must be between 8 and 24 characters long and must be different from the administrator password.
Domains	Assign the user to one or more domains to restrict the user's scope:

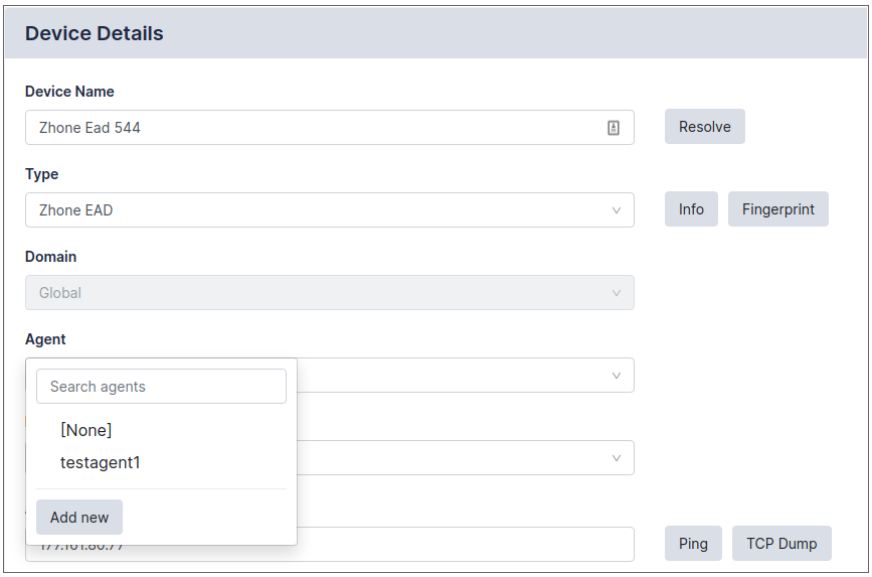


4. Click **Update**. The updated **Users** page appears:



Editing Devices

If Administration Domains are enabled, you can use the **Domain** drop-down menu in the **Edit Device** modal to move a device from a domain to another.



The domain selector will only be displayed if you are logged on as a Global Administrator.

Chapter 18

Agents

Overview

Agents allow a Skylar Compliance appliance to manage devices located on a remote or otherwise disjoint network, not directly routable by Skylar Compliance, without complex firewall changes, Network Address Translation, or VPNs. For instance, a Service Provider can set up a central Skylar Compliance appliance, deploy agents on customer networks, and enable device backups on remote sites.

You can deploy an agent as a virtual or hardware appliance on the remote network. The agent executes fast operations by performing all the tasks locally that would typically require extensive network interaction. Configurations, logs, and other processes, are handled locally by the agent, and are uploaded to the master Skylar Compliance appliance.

Agent support is provided for a variety of platforms. You can deploy the agent on VMware, AWS, Azure (available in the Azure Marketplace), via Docker, or through our RPM Agent for Linux. Support for a Hyper-V Agent is scheduled for a future release.

Agents are only available with an Enterprise license.

This chapter covers the following topics:

Agent Firewall Requirements 177

Agent Installation 177

Adding an Agent to Skylar Compliance 179

Changing the Master IP Address 181

Remote Operations Using Agents 182

Managing Agents 183

VMware Agent *184*
Amazon Web Services Agent *185*
Azure Agent *186*
Installing the Azure Agent *186*
HyperV Agent *187*
RPM Agent *188*
RPM Agent Limitations *188*
Installing and Updating the RPM Agent *189*
Configuring the RPM Agent *189*
Troubleshooting the RPM Agent *192*
Docker Agent *192*
Configuring CrowdStrike Using Agents *195*

Agent Firewall Requirements

An agent initiates and maintains an SSH connection to the master Skylar Compliance appliance to receive tasks to execute, upload and download device configurations, task output and logs, and download software updates.

Your firewall policy must allow SSH traffic (TCP port 22) from the agent to the master for an agent to function correctly.

Agent Installation

An agent virtual appliance is deployed in a similar manner to a Skylar Compliance appliance (for more information, see the section on *Virtual Appliance*). Agents are kept up-to-date with software updates using the connection to the master appliance. The software updates only cover the agent software; to update the agent operating system, see *Updating the Operating System for an Agent*.

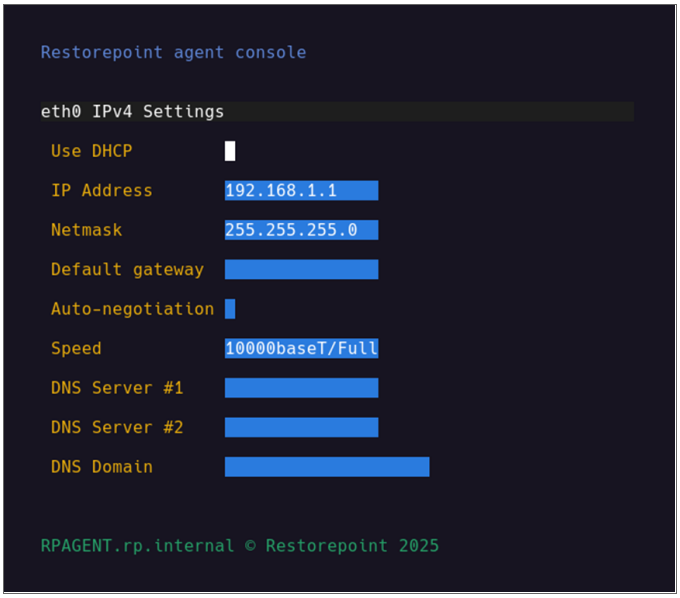
Initial Setup

Complete the following steps to define the agent in the user interface on the master appliance, and then configure the agent.

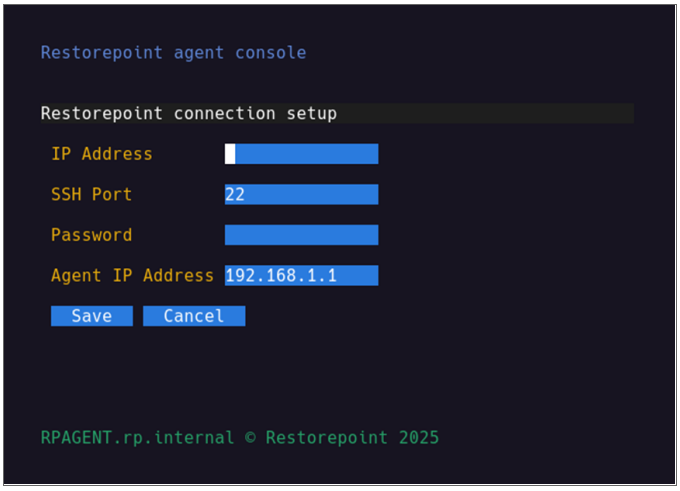
To set up an agent, configure the network parameters and the details of the connection to the master:

1. Open the virtual machine console in your Virtual Infrastructure client.
2. In the login prompt, enter the default username and password for the agent. If you are unsure which username and password to use, contact ScienceLogic Support.
3. Follow the prompts to change the agent shell password.

4. Select **IP Address Configuration** at the console menu:



5. Enter the settings for ***IP Address***, ***Netmask***, ***Default gateway***, and ***DNS Server and Domain*** settings as prompted.
6. Enter *Y* to confirm the settings. If the settings are applied successfully, the console menu will be redisplayed.
7. Next, select **Initial Restorepoint Master Setup**:



8. Enter the ***IP Address*** of the master Skylar Compliance appliance, and a one-time password to verify the agent to the master (used only for initial pairing). Optionally, you can also specify which ***SSH Port*** and ***Agent IP Address*** you want to use for the connection.

Enabling FIPS 140-3 Mode

You must enable FIPS mode before the agent has its initial setup with the Master. The setting is locked after the agent first connects to the Master, and it cannot be disabled after that.

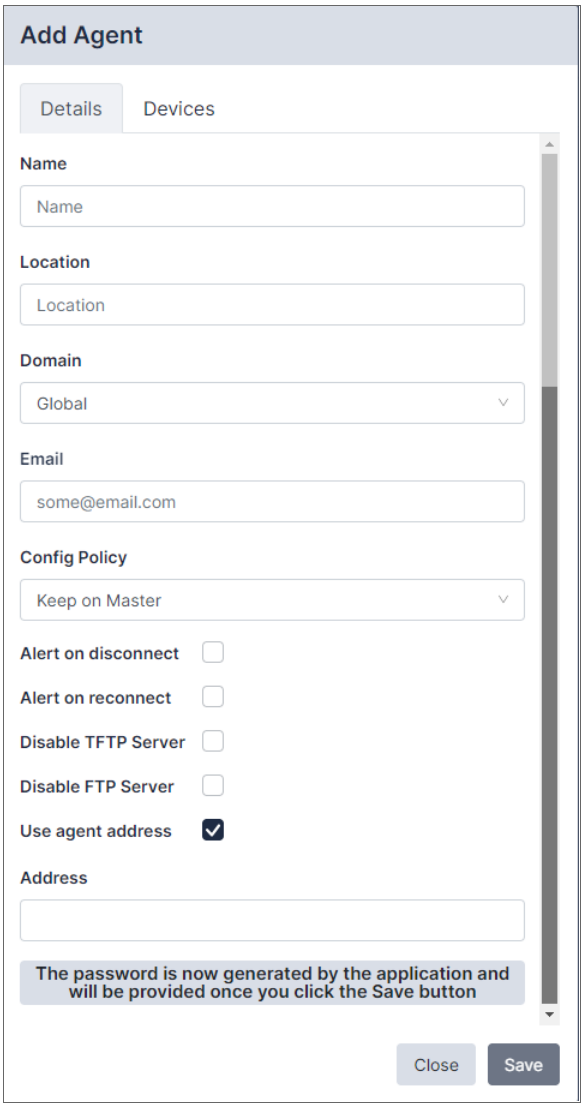
To enable FIPS on an agent:

1. Log in to the agent console.
2. From the main menu, select **Advanced** (7), then **FIPS 140-3 mode** (9). If FIPS is not yet active on the host, the screen shows a warning that the setting is permanent.
3. Select **Activate FIPS 140-3 mode** (1) and confirm. This reconfigures the operating system to use only FIPS-approved cryptography, and the agent reboots to complete activation.
4. After the agent comes back up, log in and return to **Advanced** > **FIPS 140-3 mode**. The screen now shows a checkbox.
5. Select **Report this agent as FIPS 140-3 enabled at registration**, then click **Save**. The agent saves its configuration and restarts its service.
6. Run **Initial Restorepoint Master setup** (main menu option 3) to connect the agent to the Master.

> IMPORTANT: Enabling FIPS mode is permanent. To revert it, you have to reinstall the agent. Also, if you complete the Master setup first, you cannot enable FIPS on that agent. The Master setup screen also reminds you to enable FIPS beforehand.

Adding an Agent to Skylar Compliance

To add a configured agent to Skylar Compliance, navigate to the **Agents** page (Administration > Agents) and click **[Add Agent]**. The **Add Agent** dialog appears:



Enter the following details:

- ***Name***. Type a name for the agent.
- ***Location***. Choose a new or existing location for the agent.
- ***Domain***. (Optional) The domain of the devices that this agent will manage. For more information, see *Administration Domains.*
- ***Email***. (Optional) The email for the user that is responsible for the upkeep of the agent.
- ***Config Policy***. Defines the backup storage policy. Select from one of the following options:
    - *Keep on master*. Backups are stored only on the master appliance.
    - *Keep on agent*. Backups are stored only on the agent appliance.
    - *Keep on both*. Backups are stored on both the master and the agent appliances.

- ***Alert on disconnect***. Select this checkbox to automatically email an alert if the agent goes offline. If the **Email** field is not filled in, the default notification address is used.
- ***Alert on reconnect***. Select this checkbox to automatically email an alert if the agent comes back online. If the **Email** field is not filled in, the default notification address is used.
- ***Disable TFTP Server***. Select this checkbox to disable TFTP servers.
- ***Disable FTP Server***. Select this checkbox to disable FTP servers.
- ***Secondary To***. Type the ID of an agent this agent is secondary to in a HA setup.
- ***Secondary Master IP Address***. Type the IP address of the secondary master IP in an HA setup.
- ***Use Agent Address***. Select this checkbox to enter the IP Address into the **Address** field.
- ***Address***. The specified address must be the address the agent uses to connect to the master. The address option for agents will not work if multiple agents use the same NAT address.

NOTE: Skylar Compliance will generate an eight-character password upon registering a new agent.

After the agent is added, Skylar Compliance will display the agent list. The address and port will be automatically filled in once the agent has connected successfully for the first time. Note that only one agent can be set up at a time.

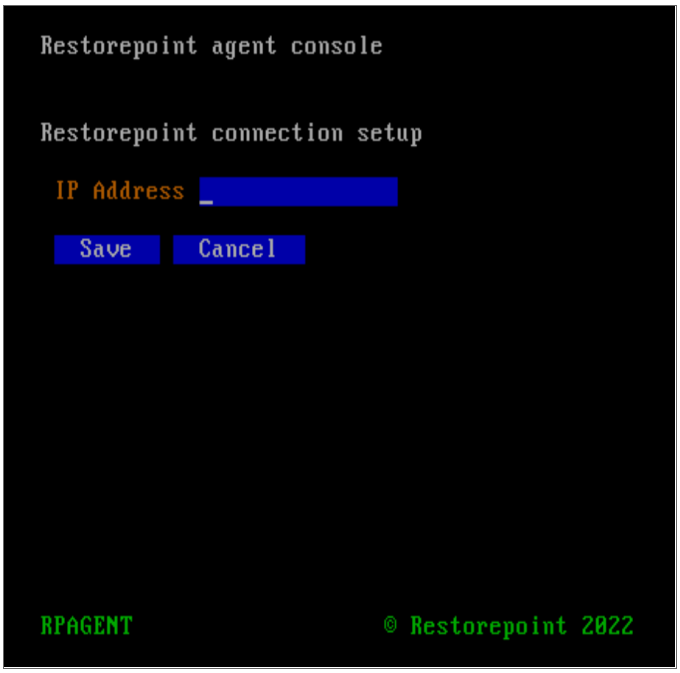


Changing the Master IP Address

If the IP address of the master Skylar Compliance appliance changes, any agents connected to that master need to be reconfigured with the new master details. To reconfigure an agent with the new master details:

1. SSH to the agent (or open the virtual machine console).
2. Log in using the agent's *admin* account.
3. Select **Change Restorepoint Master IP address** in the console menu, and apply the new master IP address.

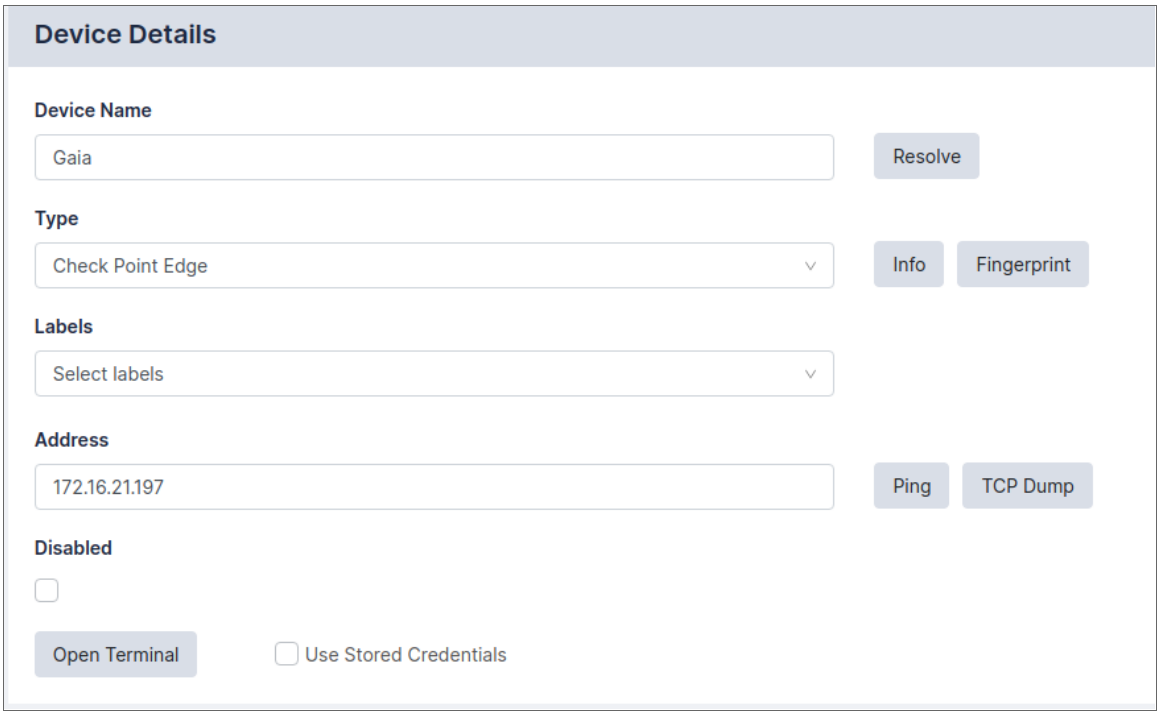
NOTE: Do not use the option **Initial Restorepoint Master Setup** to set the new master IP address. If you use this option, it invalidates the master-agent authentication and would require re-pairing the agent to the master Skylar Compliance appliance.



Remote Operations Using Agents

Once you configure an agent, you can perform any operation (backup, restore, control etc.) on a device via the agent. The Skylar Compliance appliance will not connect directly to the device, the appliance will instruct the agent to perform the operation on its behalf.

To move an existing device to an agent, select one or more devices from the **Device Management** List, and click **Edit**, then select the correct Agent in the drop-down menu as shown:



Operations using agents are completely transparent for the user. For instance, bulk operations can be started for agent-managed and directly-managed devices simultaneously.

Managing Agents

You can view a list of the paired agents from the **Administration > Agents** page. To edit an agent's settings, click the name of the agent.

The settings include the **Name**, **Location**, **Domain**, **Email**, whether to **Alert on Disconnect/Reconnect**, or allow you to factory **Reset** the Agent for re-pairing. There are additional settings for Debugging agent connections.

- **Debug > Start** works similarly to Appliance Debugging. It records a debug log that can be viewed using the **Debug > View** button.
- **Debug > Info** collects and displays a series of system information from the Agent, such as RAM usage, Disk usage, and Uptime.
- **Debug > Remote** allows remote management of an agent. This option will displays a port number. You can connect to that port on your Restorepoint master appliance to redirect to the agent so that trickier issues can be diagnosed.

Updating the Operating System for an Agent

The table on the **Agents** page contains three new columns: ***Platform***, ***OS updates*** (Up to date, Behind master, Reboot required, Failed) and ***OS updated***.

Prerequisites and other considerations:

- You need to update the OS for the master first.
- You need the *Update Sysadmin* permission in the **Global** domain (such as a Global Admin).
- Agents on the other Oracle Linux version need the master to have Internet access.
- While a run is in progress, the master will refuse a restart, reboot, shutdown, its own updates, an archive restore, and certificate changes.
- For a High Availability (HA) setup, after a failover, the new active appliance can update agents only once its own OS is updated.
- This action is not available for CentOS agents and for agents older than 5.6.

To update the operating system (OS) for one or more agents:

1. On the **Agents** page, select one or more agents and click **[Update OS from master]**. You can update five agents at a time.
2. After reviewing the preview, click **[Apply]**. The OS update progress and results display.
3. If you need to reboot an agent, click **[Reboot required]**.

VMware Agent

The VMware agent is a standalone agent that you can deploy onto your operating system to connect to various devices.

Installing and Configuring the VMware Agent

You can download the Skylar Compliance agent as a .ZIP file from the ScienceLogic Support Center (Skylar Compliance > Agent > Skylar Compliance VMware Agent). The following steps refer to VMware ESX vSphere 6.7U2 or later:

1. Expand the Skylar Compliance .ZIP file in a suitable location on your PC.
2. Launch the vSphere HTML Client.
3. Right-click on the desired destination in the left-hand column and choose **Deploy OVF Template**, select **Deploy from file** and browse to the OVA file inside the extracted folder.
4. Select the OVA file in the folder. Click **[Next]**.

NOTE: If you cannot use an OVA to deploy, extract the OVA file and select all the extracted files. There should be a .mf file, an .ovf file, and 2 .vmdk files. Then, click **[Next]**.

5. Enter a name (or keep the default name) for the agent and select the inventory location, then click **[Next]**.
6. Choose the host or cluster, then click **[Next]**.
7. Select which datastore should be used, then click **[Next]**.
8. Choose **Network Mapping**, then click **[Next]**.

9. Check the summary information, then click **[Finish]**.
10. The agent will now deploy. After completion, click **[Close]** in the completion dialog box.

IMPORTANT: Skylar Compliance is encrypted-at-rest for the secure storage of backups and databases. Any use of third-party tools to perform a scan of Skylar Compliance backups or databases may result in an error message.

IMPORTANT: ScienceLogic provides this procedure as a courtesy and does not offer support for third-party systems. For more information, including troubleshooting procedures for a VMware vSphere system, see the VMware documentation at https://vmware.com.

Amazon Web Services Agent

The Amazon Web Services (AWS) agent is a standalone agent that you can deploy onto your operating system to connect to various devices.

Installing and Configuring the AWS Agent

To install the AWS agent:

1. Log in to the EC2 Console and click **[Launch Instance]**.
2. Give your instance a name and tag your instance, if needed.
3. On the ***My AMIs*** tab, select the *Share with me* radio button, and then select the Skylar Compliance agent AMI by searching "Restorepoint" in the ***Search*** field.
4. Select an **Instance Type**. You can change the sizing at a later stage. Click **[Next]** after you make your selection. Note the following guidelines:
    - For evaluation purposes, t3.micro is usually sufficient
    - For production purposes, t3.medium or t3.large are recommended
5. **In the Key pair (login)** pane, create an SSH key pair or select an existing one from the ***Key pair name*** drop-down field. After you select the SSH key pair, you can configure the instance details on the next screen.

WARNING: Skylar Compliance uses DHCP for private IP address assignment. Ensure that the VPC/Subnet are configured to auto-assign the instance private IP address or enter the instance IP address in the **Advanced Details** section. ***You will not be able to change the instance IP address after you create it.***

6. On the **Network settings** pane in the **Firewall (security groups)** section, select the *Select existing security group* radio button or select the *Create security group* radio button. Ensure that you can communicate to the instance via SSH (port 22). For more information, see the *Firewall Requirements* section in the ***Skylar Compliance User Guide***.
7. In the **Configure storage** pane, two volumes are listed: *Root volume* and *EBS volume*. Both are 40GB by default. If you want to change the size of your appliance, ScienceLogic recommends you change the second volume, labeled ***EBS volume***.
8. Review your settings, and if they are correct, click **[Launch instance]**. The instance will launch. The first boot will take longer to launch than usual due to the initial volume encryption.
9. Follow the procedure under *Initial Setup* to set up the agent.

IMPORTANT: ScienceLogic provides this procedure as a courtesy and does not offer support for third-party systems. For more information, including troubleshooting procedures and updates for a HyperV system, contact Microsoft Support at https://support.microsoft.com/

Azure Agent

The Azure agent enables you to perform post-deployment configurations of virtual machines, collect data for monitoring, and facilitate communication and management between Skylar Compliance and Azure.

Installing the Azure Agent

To install the Azure agent:

1. Log in to your Azure account at https://portal.azure.com/#home.
2. On the **Azure Services** page, click the **[Virtual Machines]** button. The **Virtual Machines** modal opens.
3. On the **[Virtual machines]** tab, click the ***+ Create*** drop-down menu and select *Virtual machine*.
4. On the **[Basics]** tab on the **Create a virtual machine** page, complete the following sections:
    - ***Project details***. Select the *Subscription* and *Resource Group* you want to use from their respective drop-down menus.

- ***Instance details***. The following options are required.
    - *Virtual machine name*. Enter the name of your Virtual Machine.
    - *Region*. Select the region in which your virtual machine is located from the drop-down menu.
    - *Availability zone*. Select the zone in which your virtual machine is located from the drop-down menu.
    - *Security type*. Optional. Select *Standard* from the drop-down menu.
    - *Size*. Select the size of your virtual machine. You can click the *See all sizes* link for a preview of your options. The minimum requirement for the Azure agent is 2vCPUs 8GiB memory.
    - *Image*. Select the virtual machine image you want. Click the *See all images* link under the ***Image*** drop-down menu to search for your options. The **Select an image: Marketplace** page appears.
        - In the **Marketplace** section, type *Skylar Compliance* into the ***Search*** field. Results for your search will appear in a tile below the ***Search*** field.
        - Click the ***Select*** drop-down menu at the bottom of your results tile and select *Skylar Compliance Agent -x64 Gen 2* from the drop-down menu.
    - ***Administrator account***. The following fields are required.
        - *Authentication Type*. Select the radio button for the type of authentication you want to use.
        - *Username*. Enter *azure* as the username for the administrator account. If you set any other username, you will not be able to connect to the Virtual Machine using SSH.
    - ***Inbound port rules***. The following fields are required.
        - *Public inbound ports*. Select the*Allow selected ports* radio button.
        - *Select inbound ports*. Select *SSH (22)*.
5. Click the **[Next: Disks>]** button.
6. On the **Disks** page, verify that you have multiple disks, and that *Pre-defined by the selected image* appears in the ***Data disks for {Virtual Machine}*** section.
7. Click the **[Review + create]** button to create your Azure agent virtual machine.

HyperV Agent

The HyperV agent is a standalone agent that you can deploy onto your operating system to connect to various devices.

Installing and Configuring the HyperV Agent

You can obtain the Skylar Compliance agent from the ScienceLogic Support Center (Skylar Compliance > Agent > Skylar Compliance Hyper-V Agent). Choose the ***Customer Operations Request*** option and the download will be provided.

1. Expand the Skylar Compliance .Zip file to a file location on your system.
2. Launch the HyperV Manager and select your system.
3. From the **Actions** drop-down menu, select *New*, and then select *Virtual Machine*.
4. From the **New Virtual Machine Wizard**, select **[Next]** and complete the following:
    - Specify the Virtual Machine Name, then click **[Next]**.
    - Select *Generation 2* as the Virtual Machine generation type, and then click **[Next]**.
    - Assign memory for the Virtual Machine in the ***Startup memory*** field and then click **[Next]**. Configure networking on the next pane of the wizard. Then click **[Next]**.
    - Select ***Use an existing virtual hard disk*** and browse to the location where you expanded the .ZIP file. Select either *restorepoint-master-disk001.vhdx* or *restorepoint-agent-disk001.vhdx* depending on whether you are running a master or an agent as the Virtual Machine hard disk. Then click **[Next]**.
    - Review the specifications for the new Virtual Machine and click **[Finish]**.
5. Right-click on the new Virtual Machine and select ***Settings***.
6. Go to **Security** and change the template from *Microsoft Windows* to *Microsoft UEFI Certificate Authority*.
7. Go to **SCSI Controller** to select **[Add new hard drive]**. Select either *restorepoint-master-disk002.vhdx* or *restorepoint-agent-disk002.vhdx* depending on whether you are running a master or an agent hard drive.
8. Click **[Apply]** to complete the setup. Your Virtual Machine is now ready to be started.

IMPORTANT: ScienceLogic provides this procedure as a courtesy and does not offer support for third-party systems. For more information, including troubleshooting procedures and updates for a HyperV system, contact Microsoft Support at https://support.microsoft.com/

RPM Agent

The RPM agent is a standalone agent that you can deploy onto your operating system to connect to various devices.

RPM Agent Limitations

The following features are not supported on the RPM agent:

- Storage on the agent
- Encryption on the agent
- Collection from plugins that use FTP or TFTP
- Auto-upgrade of the RPM Agent
- OS updates from the master are not supported; use the package manager for the host

Installing and Updating the RPM Agent

You can download the Skylar Compliance RPM agent as a .ZIP file from the ScienceLogic Support Center (Skylar Compliance > Agent > Skylar Compliance RPM Agent). To install or update the RPM agent, perform the following:

1. Set SELinux to permissive.
2. Run `rpm -Uvh rpagent_standalone.X.rmp`.
3. A new, unprivileged user will be created along with a new group `rpuser:restorepoint`. This user and group are the owner of the Restorepoint installation under `/var/restorepoint`.

Configuring the RPM Agent

To run the RPM agent you must configure `rpagent_standalone`. You can choose to keep `rpagent_standalone` under the default directory `/var/restorepoint/bin/agentconf.json` or you can store it in a directory of your choice. To configure the RPM agent, perform the following:

1. Follow the default configuration given in `agentconf.min.json` and store it under `agentconf.json`:

```
{
"SpoolDir": "/var/restorepoint/spool",
"BackupDir": "/var/restorepoint/backups",
"BinDir": "/var/restorepoint/bin",
"PluginDir": "/var/restorepoint/plugins",
"CertsDir": "/var/restorepoint/certs",
"ConfDir": "/var/restorepoint/bin",
"MasterAddress": "HOST",
"MasterPort": "",
"NATAddress": "",
"Password": "PASSWORD",
"ChangedAdmin": 0,
"SecondaryAddress": "",
"PushDevices": "",
"DisableTFTP": false,
```

```
"DisableFTP": false,
"RPPath": "/var/restorepoint"
}
```

2. Replace `HOST` and `PASSWORD` (one-time password) to connect the agent for the first time. Keep the remaining configuration as is.
3. A new service has been created for `rpagent`. Run the following:

```
systemctl enable rpagent
systemctl start rpagent
```

4. The agent's logs are stored under `/var/log/rpagent`. If desired, you are able to configure the agent service to show the logs directly in `journalctl`. The agent service is stored under `/usr/lib/systemd/system/rpagent.service`.

Optional RPM Agent Configurations

Device Back-Connection

> **NOTE:** The Device Back-Connection optional configuration is a Beta feature.

To set up a Device Back-Connection, perform the following:

1. Create a user with the correct SSH credentials and permissions. This user must be part of the `restorepoint` group to be able to access the `spool` directory.

> **IMPORTANT:** If you are using Cisco devices, the back connection username length must not exceed six characters.

2. Add the following configurations to `agentconf.json`:

```
"BackConnectionUser": "",
"BackConnectionPassword": ""
```

> **NOTE:** Back-connection has only been tested for `ssh/scp` protocols.

If you want to rotate the `BackConnectionPassword`, complete the following:

1. Add a new password to the agentconfig.json file in the form `"BackConnectionPassword": "{NEW_PASSWORD}"`.
2. Restart your agent service.

Initial Master SSH Connection Port

To connect to a port other than Port 22 when performing initial SSH connection to the master, add the following to `agentconf.json`:

```
"MasterSSHPort": ""
```

You can also connect to multiple ports using the agent configuration option `ADDITIONALMASTERSSHPORTS` when you add ports separated by commas:

```
"AddtionalMasterSSHPorts": "1,22,23"
```

NOTE: The port you choose must be outside of system ports range (>1023).

Back Connection NAT

If needed, the agent can have a NAT address set for back connection. Devices that are managed by the agent will use the NAT address you set unless it is already set in Skylar Compliance. To set the agent's NAT address, update the following configuration value in `agentconf.json`:

```
"NATAddress": ""
```

NOTE: Upon connection with the master, the agent will encrypt the back connection password. It will remove the plain text variant from the configuration file and replace it with the encrypted version in the form `"EncryptedBackConnectionUserPassword": "{ENCRYPTED_BACK_CONN_PASSWORD}"`.

TFTP and FTP Servers

This agent does not directly start TFTP and FTP servers. If you manually start a TFTP server on Port 69 on your appliance, these plugins may work as intended but they are untested.

Disable Strict SSH Host Key Configuration

To disable the Strict SSH Host Key configuration on the agent, enter:

`"DisableStrictHostKeyChecking":true`

System Temporary Directory

Some agent packages use the default system temporary directory to store some temporary data, such as the package used for HTTP plugins. If you want to configure a custom value, set `TMPDIR=yourfolder` on `/etc/environment` and reboot your machine.

Troubleshooting the RPM Agent

If you experience issues connecting the RPM agent, for example, by not correctly configuring SELinux before trying to connect the agent to the master, complete the following:

1. Delete the contents of the folder `/var/restorepoint/certs`.
2. Reset the agent in Skylar Compliance.
3. Setup the new password again on `/var/restorepoint/bin/agentconf.json`.
4. Delete the auto-generate port if it exists.

If you are using the back connection feature, perform the following:

1. After installing the RPM agent update, update your agentconf.json file.
2. Next, enter your plain text password for the `BackConnectionPassword` and delete the value posted for the `EncryptedBackConnectionPassword`.
3. Restart the rpagent to encrypt the back connection password.

Docker Agent

The Docker agent allows you to run multiple agents simultaneously and under any operating system you choose because you can run applications in different environments.

Installing and Configuring the Docker Agent

To install the Docker agent you must have a Harbor account so that you can acquire an API token to access the images contained in the ScienceLogic registry. OS updates from the master do not apply; replace the image.

Acquiring the API Token

To use the Docker agent you must first acquire an API token from Harbor to authenticate via CLI.

To get your API token:

1. Got to https://registry.scilo.tools
2. Click the **[Login with OIDC Provider]** button
3. The Harbor home page will load after authentication has been completed.
4. Click on your username, found in the top-right corner, and then choose **User Profile**. The User Profile prompt appears with your username to authenticate.
5. You will also see the ***CLI Secret*** field with contains your API key. Be sure to copy and paste this somewhere for later use.
6. After you have your API key, click the **[Close]**button to close the session.

You are now able to use this username and API token to authenticate with the Harbor services.

Configuring rpagent

To run an `rpagent` image:

1. Log in with your Harbor username and API token to authenticate to the ScienceLogic container registry:

   ```
   docker login registry.scilo.tools -u <USERNAME> -p <API_TOKEN>
   ```

2. Create an `.env` file (or any other name) and set the following two environment variables to run the image:

   ```
   MASTER=<hostname|address>
   PASSWORD=<password>
   ```

   - `MASTER`. Enter your Skylar Compliance appliance address or hostname.
   - `PASSWORD`. Enter the password generated by the Skylar Compliance appliance upon registering a new agent.

NOTE: Skylar Compliance will generate an eight-character password upon registering a new agent.

3. Run the container as follows:

   ```
   docker run \
       -d \
       -it \
       -v $PWD/tmp:/mnt/cryptfs:Z \
       --network=host \
       --tmpfs /mnt/ram \
       --env-file .env \
       --name rpagent \
       --restart unless-stopped \
       registry.scilo.tools/sciencelogic/rpagent
   ```

   - `-d`. Daemonizes the container
   - `-it`. Allocates an interactive terminal (good for initial verification)
   - `-v $PWD/tmp:/mnt/cryptfs:z`. Mounts `tmp` in the current directory in the container as `/mnt/cryptfs` (`tmp` must be writable)
     - `:Z`. Configures the SELinux label for hosts that support SELinux.

CAUTION: ScienceLogic recommends you use caution with the `:Z` option as you can render your host machine inoperable which may require you to relabel host machine files by hand.

- `--network=host` or `--network=bridge`. In host mode, the container will share the host's network stack. For more information, see *Host Networking*.
- `--tmpfs /mnt/ram`. This is the in-memory storage for runtime data.
- `--env-file <file>`. This file contains environment variables.
- `--name <name>`. Name the running container.
- `--restart unless-stopped`. This allows the container to keep running unless stopped by the Docker daemon.

Host Networking

ScienceLogic recommends that, because the Skylar Compliance agent container is required to accept incoming connections from other devices (SSH, SCP, SFTP), the preferred networking model is to assign an individual IP address to the container. When the container has its own IP address, you can run the SSH server on the standard Port 22 instead of Port 2222. It is possible to run with `--network=host`, however the Docker host firewall must be configured to forward the incoming connections to the container.

Additional Run Options

You have the option to override default options when configuring the Docker Agent. The following options can be set to override the defaults:

- `SSHDPORT`. This is the port for the SSH/SCP/SFTP server. Bind port for SSHD (default: 2222).
- `CONFDIR`. This is the path where the agent configuration file is stored (default: /var/restorepoint/bin)
- `SSHDHOSTKEYDIR`. This is the path where SSH host keys are stored (default: /etc/ssh)
- `DEBUG`. Setting `DEBUG=1` will enable debug mode. This is useful for testing the setup for the first time.
- `DISABLESSHSTRICTHOSTKEYCHECK`. Setting this option to `DISABLESSHSTRICTHOSTKEYCHECK=1` disables the SSH host key validation for all devices and logs when the key changed.
- `SECONDARY`. This is the secondary appliance address.
- `MASTERSSHPORT`. This option allows you to change the default port (Port 22) used to connect to the master appliance.
- `NATADDRESS`. This is the NAT Address option.
- `NOANONFTP`. Setting this option to `NOANONFTP=1` disables the anonymous FTP authentication.
- `ADDITIONALMASTERSSHPORTS`. This option expects a string with multiple comma-delimited ports. For example: Enter Port 1, Port 22, and Port 23 as `1,22,23`.
- `TMPDIR`. This option changes the default system temporary directory used to store some temporary data, such as the package used for HTTP plugins.

NOTE: The `CONFDIR` and `SSHDHOSTKEYDIR` parameters can be used to store configuration files on a mounted volume which makes them persistent if the container is replaced.

Troubleshooting the Docker Agent

If you experience a failed handshake between the agent and device, try resetting the agent in Skylar Compliance.

1. Go to the agent's configuration modal and select the ***Reset*** checkbox.
2. Re-enter the password you previously chose and click **[Save]**.

```
Retrying in 10 seconds ssh: handshake failed: ssh: unable to authenticate,
attempted methods
[none password], no supported methods remain
```

Configuring CrowdStrike Using Agents

If you have CrowdStrike Sensor installed, you can configure the Sensor on the agent console menu. To configure CrowdStrike using your Skylar Compliance agent:

1. SSH to the agent (or open the virtual machine console).
2. Log in using the agent's *admin* account.
3. Select **CrowdStrike Sensor** in the console menu and select ***Enter CS Customer ID***.
4. Type your CrowdStrike Customer ID and click **[Save]**.

> **NOTE:** If you type an invalid Customer ID, an error message appears.

5. Using the **CrowdStrike Sensor** menu, you can also select the following options:

- ***Enable/Disable CS at boot (currently disabled)***. Select this option to enable Crowdstrike to start when you boot the agent. The value changes to ***Enable/Disable CS at boot (currently enabled)*** when enabled.
- ***Start/Stop Crowdstrike Sensor (currently stopped)***. Select this option to start the CrowdStrike Sensor. The value changes to ***Start/Stop CrowdStrike Sensor (currently started)*** when enabled.

Chapter 19

Users and User Roles

Overview

This chapter describes how you can use the **Users** page (Administration > Users) to add administrators to Skylar Compliance and configure administrator roles.

Skylar Compliance supports three levels of user access:

- ***Admin***. Super User who has full access (can create/modify/delete devices and users, initiate backups/restores and change the appliance configuration). Admins also have an encryption password that allows Skylar Compliance to transition from the locked state to the normal state.
- ***Backup***. Backup Operator who can perform device backups and restores, but cannot modify devices, users, or appliance settings.
- ***View Only***. Monitor Operator who can only view existing backups, access logs, and verify that the system is operating normally.

This chapter covers the following topics:

Listing Logged-in Users *197*

Adding a New User *197*

Broadcasting to Users *199*

Editing an Existing User *199*

Custom User Roles *202*

Listing Logged-in Users

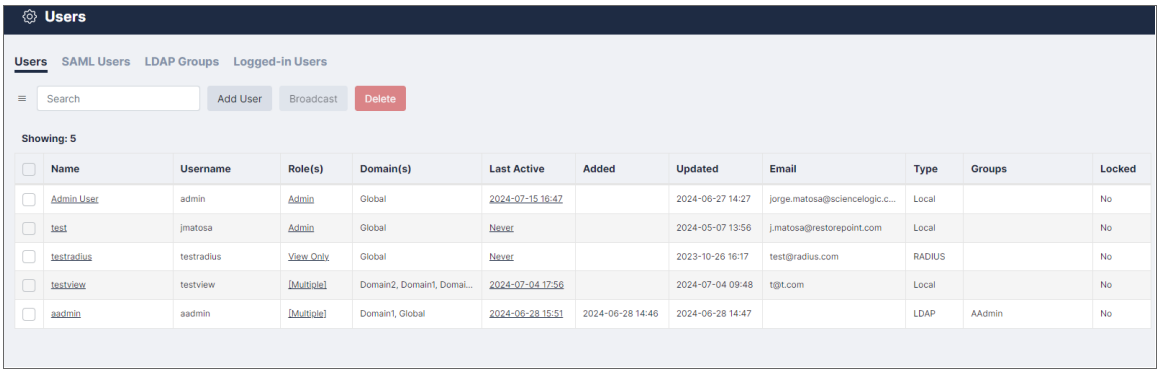
You can view a list of currently logged in users in the **[Logged-in Users]** tab (Administration > Users > Logged-in Users). The number of Logged-in users is also displayed on the **Dashboard** (Info > Status).

Adding a New User

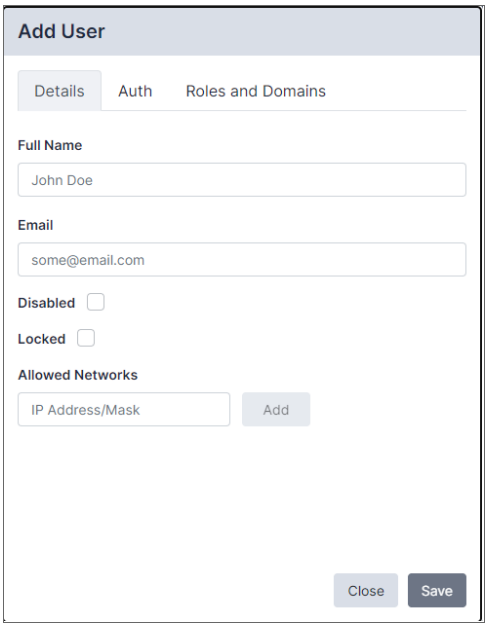
To add or modify administrators, navigate to the **Users** page (Administration > Users). Administrator passwords and encryption passwords, by default, must be at least 8 characters long. For more information, see *Password Policies*.

To add a new user:

1. Navigate to the **Users** page (Administration > Users). The **User Management** page appears.



2. Click **Add User**. The **New User** page appears:



3. Complete the following fields on the **Details** tab:
    - ***Full Name***. Type the full name of the user.
    - ***Email***. Type the user email address.
    - ***Disabled.*** Select this checkbox to prevent the user from logging in.
    - ***Allowed Networks***. If set, this field allows the user to connect to Skylar Compliance only from certain subnets. Enter an IP range in CIDR format in the IP Address/Mask box, and click **Add**.
4. Complete the following fields on the **Auth** tab.
    - ***Username***. Type the new username. Usernames may be up to 16 characters long.
    - ***Password***. Enter the password for the new user. By default, passwords must be between 8 and 24 characters long. The field color will range from red to green to indicate the password strength, according to the policy set in the **Password Policies** page. For more information, see *Password Policies.*
    - ***Encryption Password***. This field appears if an *Admin*-level administrator is selected. The encryption password must be between 8 and 24 characters long, and must be different from the administrator password. The field color will range from red to green to indicate the password strength.
    - ***Email Activation Link***. This field allows you to set up a user without specifying a password. The user will receive an activation email to let them set their own password.
    - ***Expire Password***. This field allows you to override the global password expiry rules for this user. See *Timeouts* for the global password expiry settings.
    - ***Use RADIUS***. Select this checkbox if you want the user to authenticate against an external RADIUS server. See *RADIUS Authentication* on how to configure a RADIUS server.
5. Complete the following fields in the **Domains** tab.

- ***Role***. Assign a role to one or more domains. Choose between No Role, View Only, Back Up, or Admin.
- ***Domain***. Assign a domain to each role. Choose from Global, Domain 1, Domain 2, Domain 3.

6. Click **[Save]**.

> **NOTE:** When a new administrator first logs in, they will be prompted to configure a password recovery question and answer. Skylar Compliance suggests that administrators assign an email and recovery question and answer in case you need to reset your password. For more information, see *Password Reset*.

Broadcasting to Users

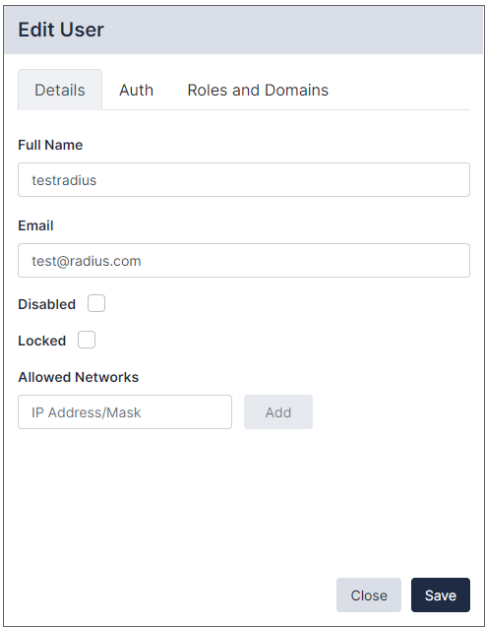
You can use Skylar Compliance to send a notification message to a user or group of users. Select the checkbox next to the users you want to message and click **[Broadcast]**. This opens the **Broadcast Message** dialog, where you can enter the message. When finished, click the **[OK]** button to send the message.

A message type appears as a pop-up in the user's session while logged into Skylar Compliance. If the user is not currently logged in, the message will appear when they log in to the appliance until the *Persist* time is reached. An *Email* message type will send the notification to the user's email address registered on the appliance.

Editing an Existing User

To edit the details of an existing user:

1. Navigate to the **Users** page (Administration > Users).
2. Click on the name of the user that you want to edit.
3. Edit the user as needed and then click **Save**.



4. When editing an administrator's user details, there are two additional fields in the **Auth** tab:
    - ***Recovery Question/Answer***. Type a Recovery Question / Answer for password recovery.
    - ***New Token***. Generates and emails a new recovery token to the user. This allows the user to recover their encryption password, if forgotten. For more information, see *Password Reset*.

NOTE: A new token is generated any time an administrator's recovery details are updated. Take note of the new token as this token will be used later if you forget your password.

Deleting a User

To delete one or more existing users:

1. Select the checkbox of the user you want to remove. You can remove multiple users at a time.
2. Click **[Delete]**.

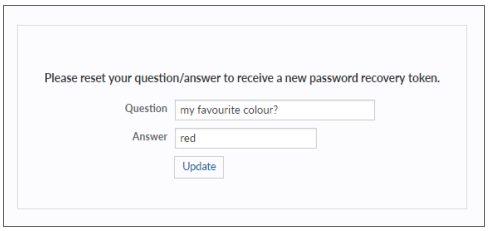
Password Reset

Skylar Compliance provides a password reset mechanism based on two-factor authentication.

Password Recovery Configuration

During the initial configuration procedure, or when an administrator logs in for the first time, the following information must be set:

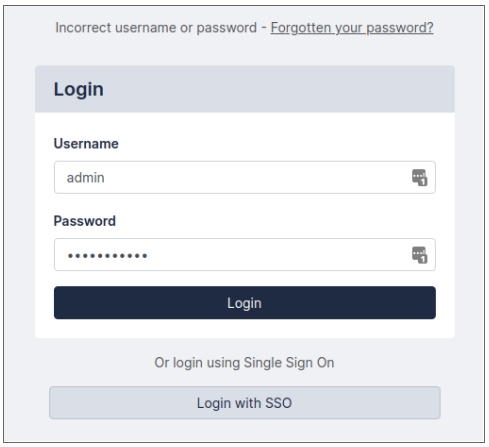
- A password recovery question and related answer. For security reasons, only an administrator should know these.
- The administrator's email address.



Skylar Compliance will then email a **recovery token**, which can be used by the administrator to reset their password and encryption password, if the administrator knows the recovery question and answer.

Recovery Procedure

When logging on with an incorrect password for the given account, the **Forgotten password** link displays:



To reset your password:

1. Click the **Forgotten password?** link and the **Reset Password** pane displays.
2. Complete the following fields:
    - ***Username***. Type your Skylar Compliance username.
    - ***Recovery Token***. Enter your recovery token. This field only displays and is only required for administrators.
    - ***Recovery Question***. Administrators should have entered a recovery question when you set up your Skylar Compliance account. Your recovery question displays then type your recovery question answer. This field only displays and is only required for administrators.
    - ***New Password***. Type a new password.
    - ***Confirm Password***. Type the same password you entered above.

- ***New Encryption Password***. Type a new encryption password. This field is only required for administrators.
- ***Confirm New Encryption Password***. Type the same password you entered above. This field is only required for administrators.

3. Click **[Reset Password]** and if your reset is successful, a notification appears.

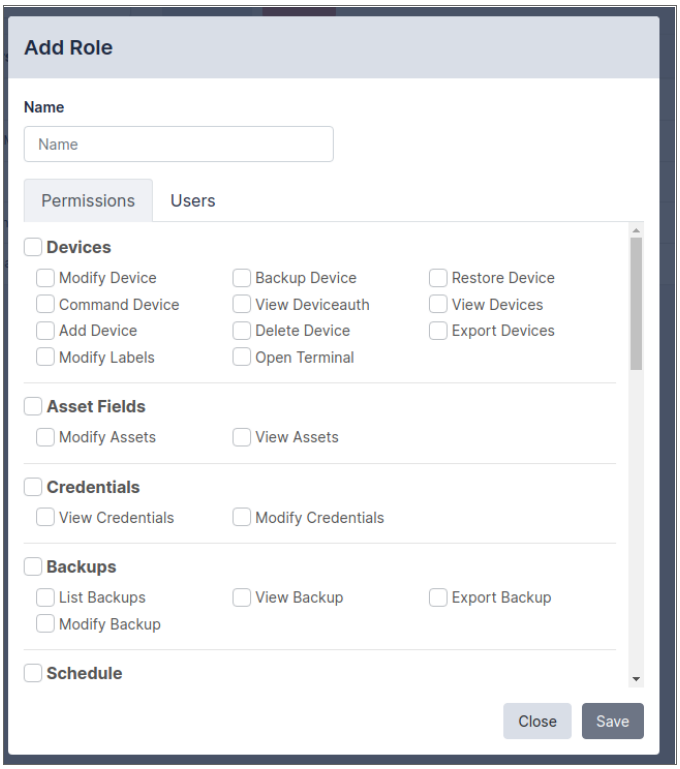
NOTE: Users with specific permissions can change another user's password.

Custom User Roles

In addition to the standard built-in administrator roles (**Admin**, **Backup**, and **View Only**), which cannot be edited, it is possible to define custom roles that define which product elements are accessible to the user. This feature is only available with an Enterprise license.

In order to define a custom role:

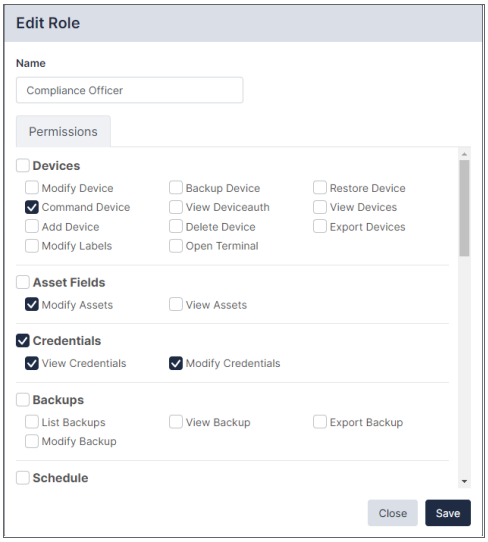
1. Navigate to the **User Roles** page (Administration > User Roles).
2. Click **[Add Role]**, and enter a name for the role.
3. Select the allowed actions for this role on the **[Permissions]** tab. Scroll down for a the full range of choices.



4. Click **Save**.

After you add a role, it is immediately available in the list on the **User Roles** page. Note that any changes to custom roles take effect immediately upon save.

For example, you can create a user role called *Compliance Officer* that can only create and modify compliance rules, and apply those to devices.



In addition to the global **View** (read-only) and **Modify** (read-write) permissions, you can allow the following actions:

Reports	
Backup	Allows backup reports
Config	Allows configuration reports
Assets	Allows assets reports
Compliance	Allows compliance reports
Admin	Allows administration reports
Monitor	Allows monitoring reports
Dashboard	Allows dashboard reports
Modify	Allows users to modify and schedule reports

Logs	
View Logs	Allows users to view the system log
View Syslogs	Allows users to view the device syslogs

Devices	
View	Allows users to view the device list and device details (excluding authentication details)
View Auth	Allows users to view device authentication details

Devices	
Backup	Allows device backup operations
Command	Allows device remote control

Configurations	
List	Allows users to view the device configuration list
Export	Allows users to export device configurations
Restore	Allows users to restore a configuration to a device

Templates	
List	Allows users to view the template list
Push	Allows users to push templates to devices

Firmware	
Push	Allows users to push firmware images to devices

Assets	
List	Allows users to view custom asset fields

Compliance Rules	
Apply	Allows users to apply compliance rules to devices

System	
Archive	Allows system archive operations

Users	
View	Allows user to view the user list and user details (excluding authentication details)
View Auth	Allows users to view user authentication details

Chapter 20

Auth Servers

Overview

This chapter describes how you can use the **Auth Servers** page (Administration > Auth Servers) to configure authentication for Skylar Compliance. You can set up RADIUS, SAML, or LDAP authentication.

External servers (such as RADIUS, SAML, LDAP, storage, SMTP, SNMP, NTP, Syslog, and/or DNS) can be v4 or v6. Host fields across Skylar Compliance can accept an IPv4/IPv6 address or a hostname (excluding DNS servers (IP address-only). If a ***hostname*** field is specified, it is resolved at run-time.

This chapter covers the following topics:

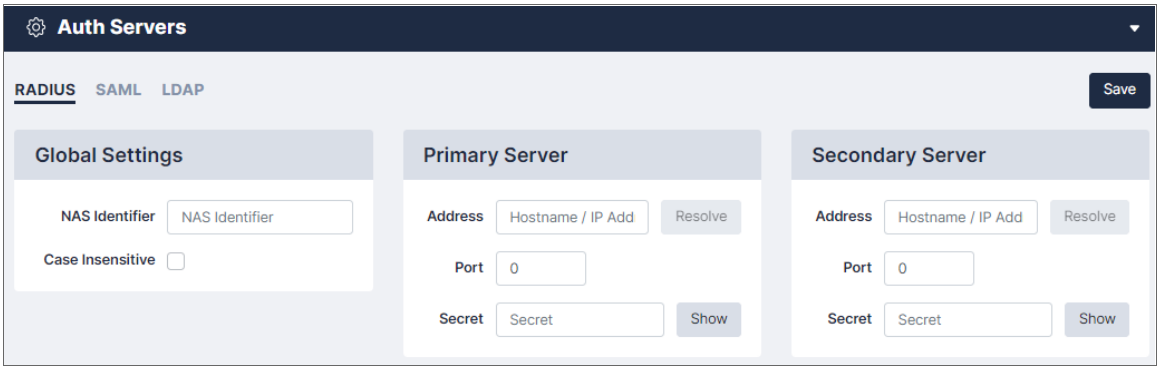
RADIUS Authentication *206*

SAML Authentication *206*

LDAP Authentication *210*

RADIUS Authentication

You can use this page to configure parameters for authenticating administrators via RADIUS. If **Use RADIUS** is selected for a user, Skylar Compliance will use RADIUS instead of the internal authentication database. Skylar Compliance supports the PAP and CHAP (not MS-CHAP) authentication protocols.



The following field are:

- ***NAS Identifier***. A string identifying Skylar Compliance to the RADIUS server
- ***Primary Server***.
    - *Address*. IP address of the RADIUS server
    - *Port*. UDP port used by the RADIUS server (usually 1812)
    - *Secret*. a string shared between Skylar Compliance and the RADIUS Server
- ***Secondary Server***. (optional) A second RADIUS server, configured as above.
- ***Resolve button***. The **[Resolve]** button is available for you to attempt DNS-resolution for hostname verification.

SAML Authentication

A single sign-on (SSO) option is available via Security Assertion Markup Language (SAML) authentication. You can configure SSO on the **[SAML]** tab of the **Auth Servers** page. (Administration > Auth Servers).

This page can be used to connect to a SAML authentication server. The following fields are:

- ***Service Provider Settings***.
    - *ACS URL*. The ACS URL to communicate with your SAML server.
    - *Entity URL*. The entity ID to communicate with your SAML server.

- ***Identity Provider Settings***.
    - *IdP Metadata*. The IdP metadata for your system.

To set up SAML take note of the following entries:

- ***ACS URL***. Enter this URL value into the relevant field of your SAML Identity Provider (IdP).
- ***Entity ID***. Enter this URL value into the relevant field of your SAML IdP.

> **NOTE:** If you want to change the host part of the URL in the ***ACS URL*** or ***Entity ID*** fields based on your current browser address, click the **[Update URLs]** button at the top of the Service Provider Settings pane.

- ***IdP Metadata***. Add the ACS URL and Entity ID to your SAML IdP to generate the IdP Metadata. Enter the IdP Metadata (usually XML) into the ***IdP Metadata*** field in the **Identity Provider Settings** pane.
- ***Groups Claim***. To use custom SAML groups, enter the groups claim according to your XML provider schema. If this claim remains unfilled, new users will be created without roles.
- ***Email Claim***.This field will populate the user's email address field on the **User** page.
- ***Given Name Claim***. This field will populate the user's given (first name) name field on the **User** page.
- ***Surname Claim***. This field will populate the user's surname (last name) field on the **User** page.

Click **[Save]** to store your input. The metadata is then uploaded to Skylar Compliance. For more information, see *SAML Authentication*.

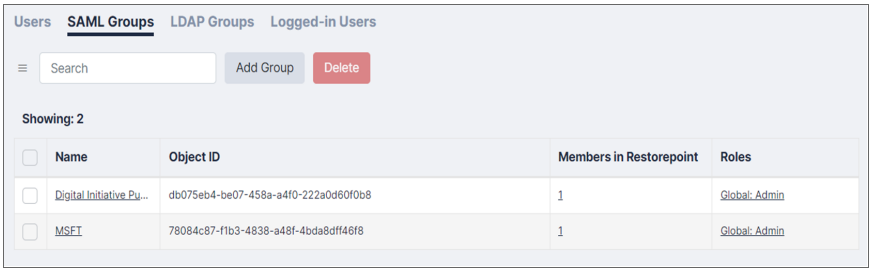
Once SAML is set up, a new button will appear on the login page called **[Login with SSO]**. You can click this button without entering values in the other fields and it will either:

- Redirect you to the SAML IdP to login
- Log you in to Skylar Compliance if you already have a valid SAML SSO session

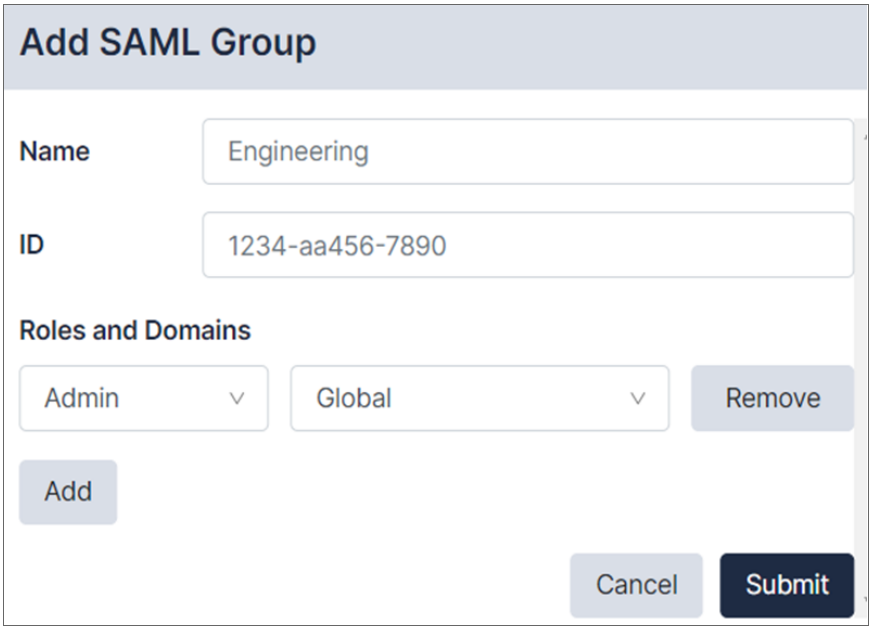
Adding a SAML Group

To add a new SAML Group:

1. Navigate to the **Users** page and click the **[SAML Groups]** tab (Administration > Users).



2. Click the **[Add Group]** button. The **Add SAML Group** dialog appears:



3. Enter the following information:

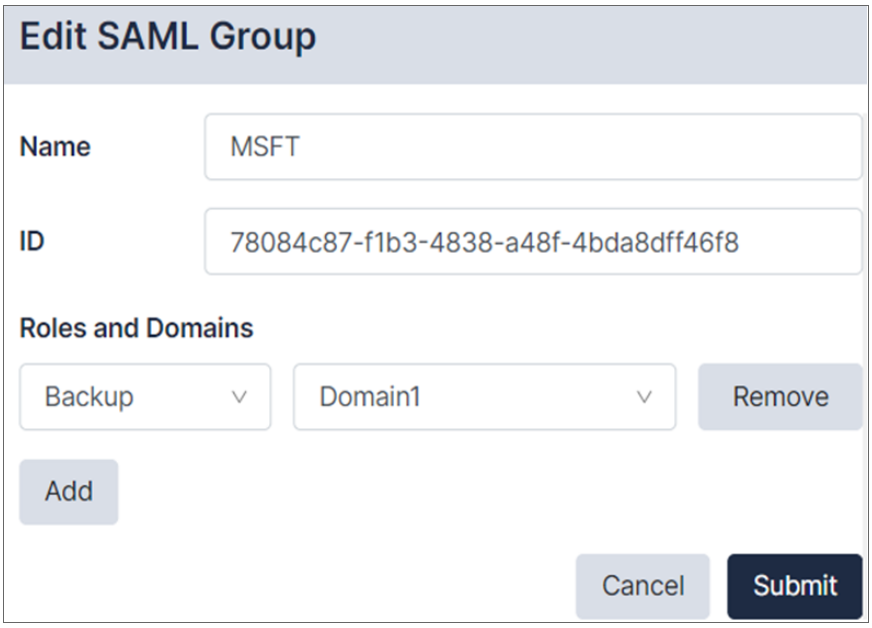
- ***Name***. SAML Group name. You can set any name to identify this group. You must specify the Group name as this is information Skylar Compliance cannot access from the SAML provider.
- ***ID***. Identifier of the SAML group. (e.g. Microsoft Entra ID uses the Object ID as the group identifier). The group identifier claim is set on https://yourapp/ui/auth-servers/saml.
- ***Roles and Domains***. Multiple roles and domains can be assigned to the SAML Group using the menu options.

4. Click **[Submit]** to save your changes.

Editing an Existing SAML Group

To edit an existing SAML Group:

1. Navigate to the **Users** page and click the **[SAML Groups]** tab **(Administration>Users>SAML Group)**.
2. Click on the SAML Group name that you want to edit. The **Edit SAML Group** dialog appears:



3. Enter the following information:

- ***Name***. SAML Group name.
- ***ID***. Enter the identifier for your SAML Group.
- ***Roles and Domains***. Multiple roles and domains can be assigned to the SAML Group using the menu options.

4. Click **[Submit]** to save your changes.

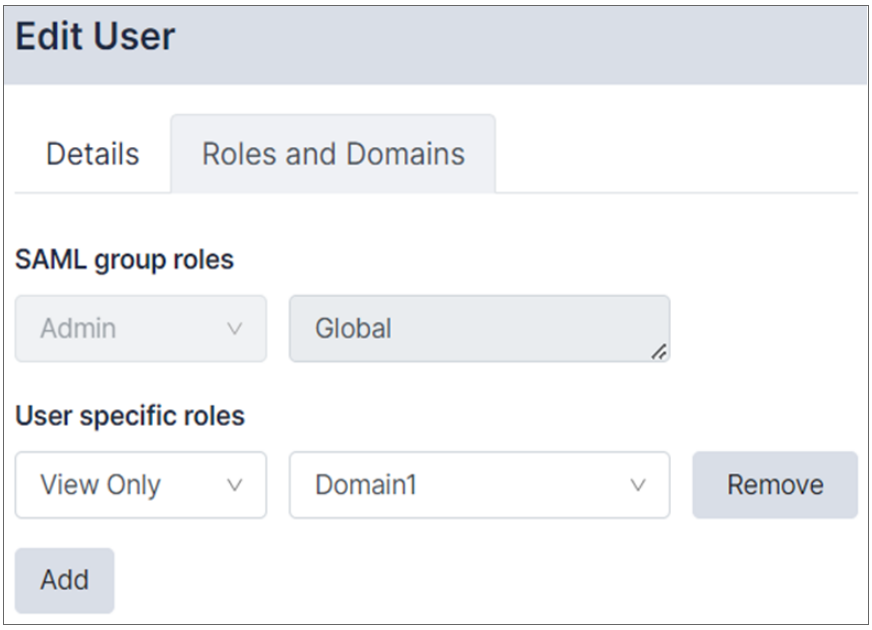
Editing an Existing SAML User

You can assign specific roles for each SAML user and see roles inherited from SAML groups. Roles assigned to SAML users remain intact even if the SAML group is changed or updated.

> **NOTE:** This feature is currently only available for SAML users.

To edit an existing SAML user:

1. Navigate to the **Users** page (Administration > Users).
2. Click on the user you want to edit. The **Edit User** dialog appears:



3. Click on the **[Roles and Domains]** tab.
4. Click the **[Add]** button to assign a new role and domain to the user. You can add or remove as many user specific roles as needed.
5. Click **[Save]** to update your user profile.

LDAP Authentication

This page can be used to connect to an LDAP (Active Directory) user authentication server.

The following fields are:

- ***Base DN***. The top-level LDAP DN. This is usually (but not always) the DNS domain name, such as *dc=company,dc=com*.
- ***User Search***.
  - *Base DN*. For example, *cn=users,dc=company,dc=local*.
  - *Username Field*. The LDAP field to use as the Skylar Compliance login id, for instance *uid* or *samAccountName*.
- ***Group Search***.
  - *Base DN*. For example, *cn=security groups,dc=company,dc=local*.
  - *Search String*. The group search filter, for instance *objectClass=Group* or *objectClass=posixGroup*, depending on the directory type.

- ***Primary Server***.
  - *Address*. The IP address of the LDAP server.
  - *Port*. UDP port used by the LDAP server (usually 389). LDAP over SSL may use 636. Use 3268 to query the Active Directory Global Catalogue (useful for multi-domain forests).
  - *Bind DN*. The DN to bind the LDAP with. For instance, gbh.
  - *Bind Password*. The the bind password for the LDAP Server.
  - *Use TLS*. Allows you to require encrypted connections to the LDAP Server.
  - *Verify certificate*. Check the server's certificate and host name against the certificates trusted by the appliance, including any chain marked *LDAP servers* under Trusted CA Certificates. Requires the *Use TLS* option, above. Always on when FIPS mode is enabled.
- ***Secondary Server***. (optional) A second LDAP server, configured as above.
- ***Resolve button***. The **[Resolve]** button is available for you to attempt DNS-resolution for hostname verification.

NOTE: LDAP groups will need user roles and domains configured on the **Administration >Users>LDAP Groups** tab before they can log in. You will also need to enter the Group DN string: `cn=users,ou=Groups,dc=mycompany,dc=com`.

Chapter 21

Storage

Overview

This chapter describes how to use file storage in Skylar Compliance. You can use the **Storage** page (Administration > Storage) to save file storage configurations in Skylar Compliance. These can be used in the **Archive** or **Logs** page, or for automated configuration export from Skylar Compliance. Archives also include the trusted CA certificates.

This chapter covers the following topics:

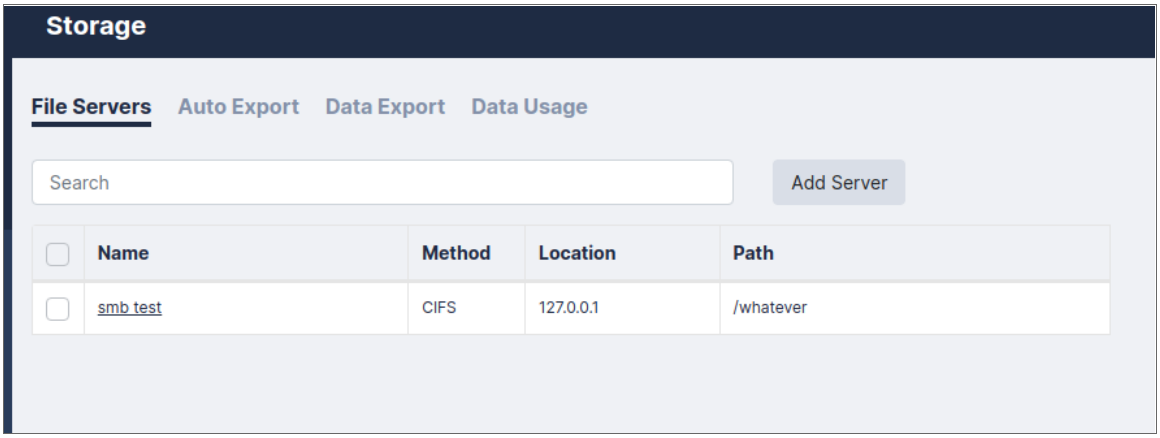
File Servers *213*

Auto Export *213*

Data Export *214*

Data Usage *214*

File Servers



For each file server, you can define the following fields:

- ***Name***. Type a name for the file server.
- ***Protocol***. Select CIFS (Windows Server), FTP, SCP or SFTP from the drop down menu.
- ***Server IP***. The IP address and port of the remote server.
- ***Path***. The full path on the remote server. For example, */home/user1* (FTP) or *share1directory2subdirectory3* (CIFS).
- ***Username***. The username. This will be an FTP user, or a valid windows user if using CIFS.
- ***Password***. The password for the associated username.
- ***Use NTLMv2 (CIFS Only)***. If you are using CIFS with the NTLMv2 authentication protocol, you can select this checkbox.

Auto Export

For each policy, you can define the following fields:

- ***Server***. The fileserver to store the exported configurations. You can also define a new server by using the *[New Server]* option. For more information on details on the configuration, see *File Servers*.
- ***Policy***. When to automatically export configurations to your external server. **Always Export** will export when the backup is complete, **Only Export new Versions** will export when the backup is complete and the version number of the backup has changed, and **Export before automatic deletion** will export only the backups that are due to be removed from the Skylar Compliance appliance.

There are additional options you can apply to your new policy:

- ***Use GPG***. Users must enter a **passphrase** to securely encrypt the exported configurations before transfer to your external server.

- ***Include Domain/Device***. The filename / path on the remote server will contain the domain name/device name. For example, */home/user1* (FTP) or *share1directory2subdirectory3* (CIFS).
- ***Disabled***. If this checkbox is selected, the policy will not run. This options allows you to temporarily disable an auto-export policy.

Data Export

You can use this page to export device configurations on-demand.

- ***Configurations***. **No configs**, only the **Most Recent** version of the config, or **All Configs**.
- ***Data***. Includes the device's **Logs**, and/or the **Device Data** in your export.
- ***For***. The devices or domains to export.
- ***As***. The format to export the configurations. They can be exported as *TGZ* or *ZIP* archives, or directly export the individual config files.
- ***Chunk size***. If you've selected an archive format, you can choose the size to create the archive files.
- ***To***. The server to store the exported configurations. For more information, see *File Servers*. Alternately, you can choose to export device configurations directly to your workstation, via the browser.

Data Usage

The Data Usage page displays statistics on the storage disk of your Skylar Compliance appliance.

- ***Total Disk Size***. The size of the encrypted volume that Skylar Compliance uses to store device configurations and settings.
- ***Total Used***. The total amount of that volume's space that has been used.
- ***Backup Size***. Space used by device configurations.
- ***Index Size***. Space used by Skylar Compliance's search index (used primarily for the *Global Search* function).
- ***Cache Size***. Space used by the Skylar Compliance cache. This is usually device configurations that needed to be extracted for viewing or comparisons. Skylar Compliance will automatically remove this cache, if needed. You can also manually clear the cache and click **[Clear Cache]** to clear the cache.
- ***Debug Size***. Space used by Skylar Compliance debugging logs, such as Appliance Debug Logs. Appliance Debug Logs are cleared if a new Debug Log is started. You can manually clear the Appliance Debug Logs and click **[Clear Debug]**.

Chapter 22

Getting Help

Overview

Click **Help** to access a link to the Skylar Compliance product documentation for your current page.

You can also click **Help > Help Index** to access the HTML user guide, download a PDF copy of the user guide, or access the Plugin Guide (**Help > Plugin Guide**).

This chapter covers the following topics:

Error Messages 216

Using the System Shell 218

Factory Reset 219

Skylar Compliance Plugins 220

Frequently Asked Questions 221

Contacting ScienceLogic Support 221

Error Messages

If you experience an error, review the descriptions and solutions below.

Errors During Backup Operations

Error	Description	Solution
Connection timeout (Cause 1)	Skylar Compliance can't connect to the device using the specified protocol.	Check that the protocol is correct and that there is connectivity to the device (e.g., no firewall is blocking the required ports). If the device uses back-connections, also check that this is not blocked, and/or NAT is correctly configured on Skylar Compliance. Check **Help > Plugin Guide** to verify the connectivity requirements for this particular device.
Connection timeout (Cause 2)	The device is not sending the expected output to Skylar Compliance within the allocated time.	Check that you have selected the correct plugin and that the device firmware/operating system is supported by Skylar Compliance.
Connection failed: Device SSH key has changed	Skylar Compliance has detected that device's SSH key has changed	This error typically occurs because the device has been replaced. If the device has been replaced, edit the device and click **[Clear Cache]**
Timeout waiting for username prompt	Skylar Compliance can connect to the device but did not receive a username prompt.	Check that you are using the correct plug-in. If the device is not configured to prompt a username, leave the Username field empty in the device definition.
Timeout waiting for password prompt	Skylar Compliance can connect to the device but did not receive a password prompt.	Check that you are using the correct plug-in and that the device username and password are correct.
Timeout waiting for device prompt	Skylar Compliance can connect to the device but did not receive the device CLI prompt.	Check that you are using the correct plug-in and that the device username and password are correct.
Error creating backup	Skylar Compliance can connect to the device but is not able to	Connect to the device manually from your PC or from the Skylar

Error	Description	Solution
	create a backup on the device. This can be caused by a number of circumstances, usually a lack of available disk space.	Compliance system shell and attempt to create a backup to determine the cause of the error.
Error transferring backup	Skylar Compliance can connect to the device and create a backup on the device but is not able to transfer it back. This is usually due to a firewall blocking a required port (e.g., TFTP) between Skylar Compliance and the device. If your device has a large backup file (several Mbytes) and you are backing up over a WAN, this error message can be caused by a timeout during file transfer.	Check the **Plugin Guide** (Help > Plugin Guide) and ensure that the TCP or UDP ports required by your device are not blocked by any firewalls.
Incorrect checksum after transfer	Wherever possible, Skylar Compliance calculates an MD5 checksum of the backup file before and after transfer to ensure the integrity of the file. If the checksum changes, this indicates that the file got corrupted in transit.	Retry the backup. An isolated error of this type may indicate a problem on the network (e.g., faulty switches or cables). A reoccurring error may be caused by a large backup file and/or a slow network, where only part of the file is transferred. Try and reduce the size of the backup if possible; use SCP or FTP instead of TFTP wherever possible.
Wrong parameter found at .^. position		Check that you have specified the correct unit when backing up a 3Com 5500 switch.
Error backing up the device/Could not hold conversation with device	Although a failure will normally generate a specific error message, you may occasionally encounter a generic error.	Check that the device credentials are correct, that you are using the correct device plug-in, and that the required TCP/UDP traffic is allowed between Skylar Compliance and the device. If you are still unsuccessful, contact Technical Support.

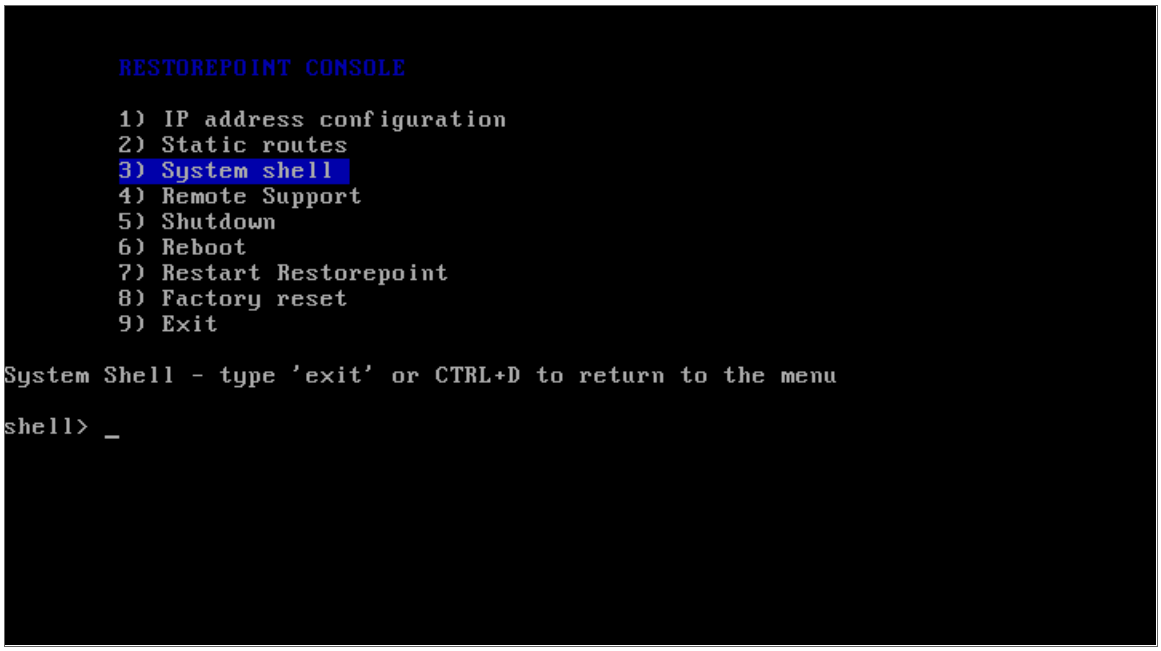
Other Messages

It is possible to experience messages that are not included above. The following errors message may also result:

Error	Description	Solution
Cryptfs not mounted	The encrypted storage was not mounted correctly after a reboot. This may happen if the appliance is powered off without a clean shutdown.	Login with your username, password, and encryption password. Skylar Compliance will attempt to check and mount the encrypted storage. If you keep receiving this message every few minutes, contact Technical Support.
Couldn't connect to update server	Skylar Compliance needs to communicate to the update server (`support.restorepoint.com`) to check whether new software or device plug-ins are available.	Check the following: 1. Check that the DNS servers configured in the **System** page are correct and are working properly. 2. Check that a firewall is not blocking HTTPS traffic from Skylar Compliance to `support.restorepoint.com`. 3. If Skylar Compliance uses a proxy to access the internet, check that the correct proxy username and password are being used and that the password for the proxy user account has not expired. 4. If Skylar Compliance is located on a network without internet access, disable automatic updates by selecting **This appliance is not connected to the Internet** in the **System** page.
Connection failed: Device SSH key has changed	Skylar Compliance has detected that device's SSH key has changed	This error typically occurs because the device has been replaced. If the device has been replaced, edit the device and click **[Clear Cache]**
License expired	You've either received a license has expired message or can't obtain software updates.	Contact ScienceLogic Support.

Using the System Shell

The system shell provides some useful command line network tools that can be used to troubleshoot connectivity problems. To start the system shell, log in to the Skylar Compliance console using an *admin* account and select **System Shell**.



Ensure that you are familiar with these tools before using the system shell. The available commands are:

- ***help***. Lists the available commands.
- ***ping***. Sends an ICMP Echo Request packet to a network host.
- ***traceroute***. Displays the route packets take to a network host.
- ***nslookup***. Query a DNS name server.
- ***telnet***. Connect to a host using the TELNET protocol.
- ***ssh***. Connect to a host using the SSH protocol.
- ***tcpdump***. Displays the network traffic.
- ***exit***. Returns you to the main menu.

Factory Reset

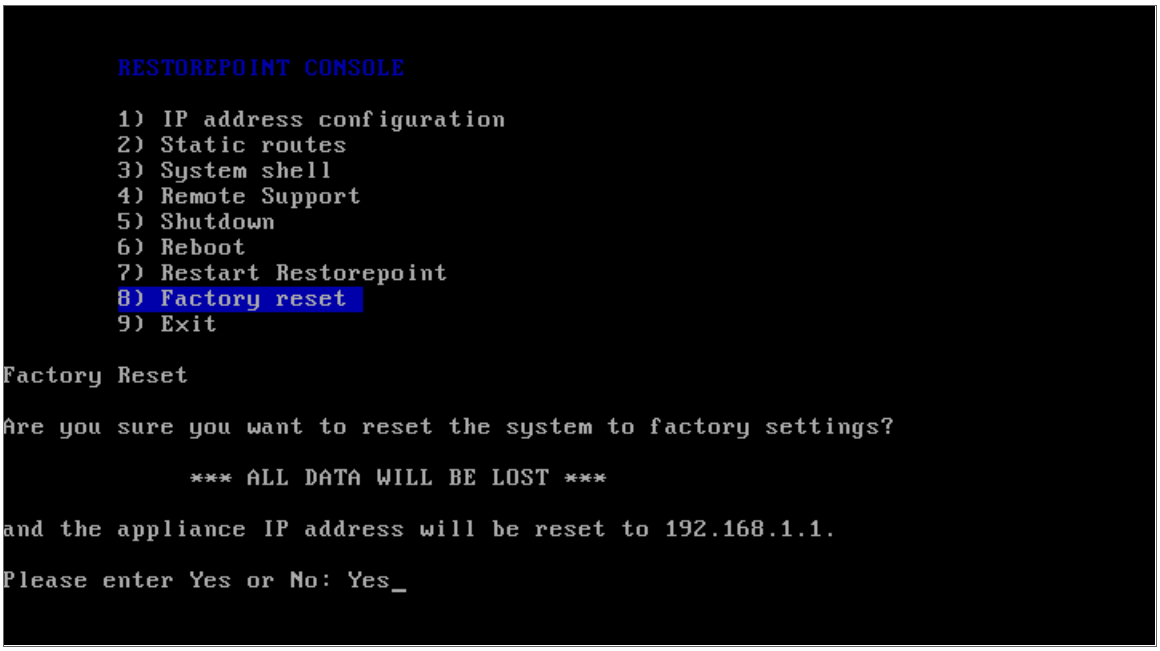
If you need to reset your Skylar Compliance appliance to factory settings, you can follow the factory reset procedure. Note that the factory reset will permanently erase **ALL** of the information stored on the appliance, not just the system settings. In particular:

- The encryption key will be deleted.
- All the device data (configuration and backups) will be erased.
- All the administrators (except *admin*) will be deleted.
- All plugins will be deleted.
- System settings will be reset to their default values.
- The password for the *admin* user will be reset to `admin`.

Note : To reset the appliance, you must have the admin password. If you need to reset Skylar Compliance and you do not know the admin password, contact ScienceLogic Support.

To start the factory reset procedure:

1. Log in as *admin* on the Skylar Compliance console.
2. Choose the ***Factory reset*** option.
3. Confirm that you understand and accept that your data will be lost and enter *Yes*, otherwise enter *No* to abort.



The system will then erase the database and reset the system settings to their default values. This can take some time, depending on how much data is stored on the appliance. Do not shut down or power off the system before the reset has completed or you may damage the appliance. Skylar Compliance will automatically shut down at the end of the procedure.

Skylar Compliance Plugins

All Skylar Compliance Plugins that are currently supported can be found on the ScienceLogic Support Plugins page. For more information on Plugins to enable your Skylar Compliance appliance, see *Skylar Compliance Plugins*.

For additional information, see the Knowledge Base article https://support.sciencelogic.com/s/article/14984 .

Frequently Asked Questions

Error	Solution
I have forgotten my encryption password.	See *Connecting to Skylar Compliance after a reboot* and *Password Reset* for more information.
I cannot connect to the web interface.	Check that you have network connectivity. The power and network LEDs on the front panel of your Skylar Compliance appliance should be lit. If you are in an environment using a proxy server, check that you are connecting to the device on port 443, or that your browser is set to bypass connection to the device.
I cannot add a device.	Check that the model and firmware version of the device you are adding is on the list of supported devices. The list of supported devices can be found in the **Plugin Guide** (Help > Plugin Guide).
I do not get notifications.	Check that the task is not paused in the **Info > Schedule** page.
Scheduled tasks are not running.	Check that the task is not paused in the **Info > Schedule** page.
I have a device that is not supported but would like to see support for it.	Contact Technical Support and let us know the vendor, product, model, and version of the device. Wherever possible, Skylar Compliance will endeavor to add support for your device.
I still need assistance and require remote support.	If you are having problems and need a support engineer from Skylar Compliance to help troubleshoot the issue, click the **Remote Support** option on the Skylar Compliance appliance to create an SSH tunnel to our support server which allows a support engineer to assist you. Alternatively, our support team can set up a web session with you (WebEx, join.me, GoToMeeting, or similar).

Contacting ScienceLogic Support

Skylar Compliance Technical Support is now linked to ScienceLogic Support. If you need support, contact the *ScienceLogic Support Center*. From there, you can search knowledge base articles and other resources, or open a case with ScienceLogic Support. Access to the portal requires registration and a valid software license.

© 2003 - 2026, ScienceLogic, Inc.

All rights reserved.

ScienceLogic™, the ScienceLogic logo, and ScienceLogic's product and service names are trademarks or service marks of ScienceLogic, Inc. and its affiliates. Use of ScienceLogic's trademarks or service marks without permission is prohibited.

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information herein, the information provided in this document may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described herein at any time without notice.



800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010