Skylar Compliance SyncPack

Version 3.1.0

Table of Contents

Introduction to the Skylar Compliance SyncPack **4**

What Can I Do with this SyncPack? 5

Contents of the SyncPack 6

Skylar Automation Applications 7

Skylar Automation Applications (Internal) 8

Configuration Object 8

Steps 8

MCP Components 10

Installing the Skylar ComplianceSyncPack **12**

Prerequisites for this SyncPack 13

Installing the SyncPack 13

Downloading the SyncPack 13

Importing the SyncPack 14

Activating and Installing the SyncPack 14

Installing and Configuring the PowerPack 15

Installing the PowerPack 15

Configuring Applications for the Skylar Compliance SyncPack **17**

Workflow for Configuring Skylar One andSkylar Automation 18

Configuring Skylar One 18

Configuring Skylar Automation 18

Configuring Skylar One 18

Creating an SSH Credential for Discovering Devices 18

Align the "Restorepoint Connectivity" Dynamic Application with Skylar One Devices 19

Align the "Restorepoint Second Password" Dynamic Application with Skylar One Devices 20

Configuring Skylar Automation 21

Obtaining the API Token in Skylar Compliance 21

Creating a Configuration Object in Skylar Automation 21

Configuring the "Skylar Compliance: Sync Devices" Application 24

Configuring the "Skylar Compliance: Get the List of Logs from Skylar Compliance" Application 25

Configuring the "Skylar Compliance: Get list of credentials from Skylar One" Application 26

Configuring the "Skylar Compliance: Gather Compliance Logs from Skylar Compliance" Application 26

Configuring the "Skylar Compliance: Pre Check" Application 27

Configuring the "Skylar Compliance: Create or Update Custom Links" Application 27

Scheduling Skylar Automation Applications 28
Troubleshooting the Skylar Compliance SyncPack 30
Scaling Issues with the Grouping Device Count Configuration Option 30
Sync Failures Due to Dynamic Application Configuration Options 30
Troubleshooting Device Sync Errors 30

Chapter 1

Introduction to the Skylar Compliance SyncPack

Overview

This chapter describes how you can use the "Skylar Compliance" SyncPack to automatically add Skylar One devices to Skylar Compliance (formerly Restorepoint) when those devices are discovered in Skylar One and then sync data for those devices. This SyncPack also collects backup log data from Skylar Compliance.

The "Skylar Compliance" SyncPack uses the "Skylar Compliance" PowerPack.

This chapter covers the following topics:

What Can I Do with this SyncPack? *5*

Contents of the SyncPack *6*

What Can I Do with this SyncPack?

The "Skylar Compliance" SyncPack contains Skylar Automation (formerly PowerFlow) applications that can automatically add, or "onboard", Skylar One devices to Skylar Compliance when those devices are discovered in Skylar One. You can also use this SyncPack to collect backup log data from Skylar Compliance.

This SyncPack lets you configure the following integrations between Skylar Compliance and Skylar One:

- ***Onboard and Sync Devices***. The "Skylar Compliance: Sync Devices" application syncs existing Skylar One devices with Skylar Compliance devices. The application also adds new Skylar One devices and their associated elements to Skylar Compliance, including the domain and credential. The application gets details about how the device will be configured in Skylar Compliance, including the assigned agent and device type, from a mapping in the aligned configuration object.
- ***Get Logs from Skylar Compliance***. The "Skylar Compliance: Get the list of Logs from Skylar Compliance" application queries the Skylar Compliance API to collect backup success and failure logs from Skylar Compliance. These logs are also synced to Skylar One. You can use Skylar Automation to compare the logs to make sure the backups ran successfully in Skylar Compliance.
- ***Update credentials from Skylar One***. The "Skylar Compliance: Get list of credentials from Skylar One" application queries Skylar One for existing credentials and matches them against credentials in Skylar Compliance. If there is a change to the credential in Skylar One and the credential exists in Skylar Compliance, the credential is updated with the new information.
- ***Sync Compliance Logs to Skylar One as Events***. The "Skylar Compliance: Gather Compliance Logs from Skylar Compliance" application checks for compliance logs from Skylar Compliance and syncs them to Skylar One to create events for the compliance alerts in Skylar One.
- ***Verify correct configuration of Skylar One and Skylar Compliance systems***. The "Skylar Compliance: Pre Check Application" application allows you to verify that both the Skylar One and Skylar Compliance systems are correctly configured for device synchronization. It assesses the current onboarding capacity of the Skylar Compliance system, providing visibility into how many additional devices can be registered. Additionally, it performs a comprehensive permissions check on the Skylar One system, identifying any denied permissions that must be enabled to ensure smooth operation of the Skylar Compliance SyncPack.
- ***Create or update custom links***. The "Skylar Compliance: Create or Update Custom Links" application allows you to create and update custom links within the Skylar One platform. It enables the addition of direct navigation links to Skylar Compliance-onboarded devices from Skylar One device pages, streamlining access and improving operational efficiency. By integrating these links, users can quickly transition from Skylar One to the corresponding Skylar Compliance device, enhancing workflow and reducing navigation time.

For more information about configuring these integrations, see *Configuring Applications for the Skylar ComplianceSyncPack*.

Contents of the SyncPack

This section lists the contents of the "Skylar Compliance" SyncPack.

Skylar Automation Applications

Before you can use the integrations between Skylar Compliance and Skylar One, you will need to configure the following applications in the "Skylar Compliance" SyncPack:

- ***Skylar Compliance: Get list of credentials from Skylar One***. This application queries Skylar One for existing credentials and matches them against credentials in Skylar Compliance. If there is a change to the credential in Skylar One and the credential exists in Skylar Compliance, the credential is updated with the new information. For more information, see *Configuring the Skylar Compliance: Get list of credentials from Skylar One application*.
- ***Skylar Compliance: Get the List of Logs from Skylar Compliance***. This application queries the Skylar Compliance API to collect backup success and failure logs from Skylar Compliance. You can use Skylar Automation to compare the logs to make sure the backups ran successfully in Skylar Compliance. For more information, see *Configuring the Skylar Compliance: Get the List of Logs from Skylar Compliance Application*.
- ***Skylar Compliance: Sync Devices***. This application discovers newly registered Skylar One devices and then triggers the "Skylar Compliance: Onboard Device" application on the discovered device. The "Skylar Compliance: Onboard Device" application adds new devices and the associated elements to Skylar Compliance, and also creates Skylar Compliance custom attributes for the new devices in Skylar One. For more information, see *Configuring the Skylar Compliance: Sync Devices Application*.
- ***Skylar Compliance: Get a list of devices not present in Skylar One***. This application retrieves a list of devices that are not present in Skylar One but *are* present in Skylar Compliance.
- ***Skylar Compliance: Gather Compliance Logs from Skylar Compliance***. This application checks for compliance logs from Skylar Compliance and syncs them to Skylar One to create events for the compliance alerts in Skylar One. For more information, see *Configuring the Skylar Compliance: Gather Compliance Logs from Skylar Compliance Application*.
- ***Skylar Compliance: Pre Check Application***. This application verifies that both the Skylar One and Skylar Compliance systems are correctly configured for device synchronization. It assesses the current onboarding capacity of the Skylar Compliance system, providing visibility into how many additional devices can be registered. Additionally, it performs a comprehensive permissions check on the Skylar One system, identifying any denied permissions that must be enabled to ensure smooth operation of the Skylar Compliance SyncPack. For more information, see *Configuring the Skylar Compliance: Pre Check Application*.
- ***Skylar Compliance: Create or Update Custom Links***. This application allows you to create and update custom links within the Skylar One platform. It enables the addition of direct navigation links to Skylar Compliance-onboarded devices from Skylar One device pages, streamlining access and improving operational efficiency. By integrating these links, you can quickly transition from Skylar One to the corresponding Skylar Compliance device, enhancing workflow and reducing navigation time. For more information, see *Configuring the Skylar Compliance: Create or Update Custom Links*.

Skylar Automation Applications (Internal)

The following applications are "internal" applications that should not be run directly, but are automatically run by applications from the previous list. To view these internal Skylar Automation applications, click the Filter icon ( ) on the **Applications** page and select *Show Hidden Applications*. Internal applications are hidden by default.

- ***Skylar Compliance: Onboard Device***. This application adds new devices and the associated elements to Skylar Compliance, including the domain and credential. This application also creates Skylar Compliance custom attributes for the new devices in Skylar One. The application gets details about how the device will be configured in Skylar Compliance, including the assigned agent and device type, from a mapping in the aligned configuration object. This application is triggered by the "Skylar Compliance: Sync Devices" application.
- ***Skylar Compliance: Update Event info in Skylar One***. This application populates Skylar One events with log and backup information that is collected from Skylar Compliance. This application is triggered by the "Skylar Compliance: Get the List of Logs from Skylar Compliance" and the "Skylar Compliance: Gather Compliance Logs from Skylar Compliance" applications.

Configuration Object

- ***Skylar Compliance Base Config***. This configuration object can be used as a template after the SyncPack is installed on the Skylar Automation system. The configuration object includes the following:
    - Details for connecting to the Skylar One API, including the URL, username, and password.
    - Details for connecting to the Skylar Compliance API, including the URL, username, and password.
    - Details for connecting to the Skylar One database, including the URL, username, and password.
    - A mapping between Skylar One Device Class globally unique identifiers (GUIDs) and Skylar Compliance device types.
    - A default value for Skylar Compliance device types.
    - Mapping between Skylar One collector appliance IDs and Skylar Compliance agents.
    - A default backup schedule for all new devices added to Skylar Compliance.
    - An option to add a custom link configuration to Skylar One, a user access URL, a timestamp, and the option to allow device change detection.

Steps

The following steps are included in this SyncPack:

- Check Skylar One User Access
- Checking Skylar Compliance API Access and Device Availability

- Create and Update Skylar Compliance Credential
- Skylar Compliance: Create Device
- Create Skylar Compliance Domain
- Determine the change in Skylar Compliance Logs
- Skylar Compliance: Enrich Devices with Credentials data
- Fetch Device Limit from Skylar Compliance
- Fetch Skylar One Credential Data
- Filter devices from Skylar One
- Filter basic/snippet and ssh Skylar One credentials list
- Select devices from Skylar One
- Get backup data from Skylar Compliance
- Get list of Basic/Snippet credentials from Skylar One
- Get collector group details for list of Skylar One devices
- Get device class details for list of Skylar One devices
- Get Device Details from Skylar One
- Get device id from Skylar One
- Get device list from Skylar Compliance
- Get devices from Skylar One
- Retrieve Skylar Compliance Group Devices
- Get list of Skylar Compliance credentials
- Get Plugin Info
- Get Skylar Compliance Compliance Logs
- Get Logs from the Skylar Compliance and save in SA cache
- Get license details from Skylar Compliance
- Get list of SSH credentials from Skylar One
- Create or Update Custom Links
- Insert data in Skylar One database
- Optional QueryGQL Call Skylar Compliance
- Select Custom Link
- Select device id from Skylar One
- Update Device Event Info
- Add Skylar Compliance ID custom attribute to Skylar One device
- Create custom attribute

MCP Components

The following MCP tools and their filters work in conjunction with the MCP server introduced in version 3.4.0 of Skylar Automation. For more information, see the *Configuring the Skylar Automation MCP Server* chapter in the ***Skylar Automation*** manual.

IMPORTANT: All MCP tools listed below require a ***config_name*** that points to a Skylar Automation configuration object with the following fields:

- ***restorepoint_url***. The hostname or IP address, or full base URL of the Skylar Compliance instance.
- ***restorepoint_api_token***. The Skylar Compliance API key. This is used with the custom authorization scheme.

- ***list_devices***. Returns a paginated list of devices from Skylar Compliance.
  - ***limit***. Integer between 1 and 50. Defines results per page. The default value is 10.
  - ***offset***. Integer. The number of results to skip for pagination. The default value is zero.
- ***get_device_by_id***. Returns a single device.
  - ***device_id***. Integer. Required. Filters to a specific device.
- ***list_device_backups_by_type***. Returns the history of backups for a device, split by configuration type. Consecutive identical backups are collapsed.
  - ***device_id***. Integer. Required. Filters to a specific device.
  - ***limit***. Integer. Defines the number of backups to look through. The default value is 100.
- ***get_device_backup_by_id***. Returns the metadata for a single backup.
  - ***device_id***. Integer. Required. The ID of the device.
  - ***backup_id***. Integer. Required. The ID of the backup.
- ***get_device_backup***. Returns the actual config lines for a specific backup.
  - ***device_id***. Integer. Required. The ID of the device.
  - ***backup_id***. Integer. Required. The ID of the backup.
  - ***backup_type***. String. Required. The configuration type of the backup.
- ***compare_backup***. Returns a diff between two backups on two (possibly different) devices.
  - ***device1_id***. The ID of the first device.
  - ***backup1_id***. The ID of the first backup.
  - ***backup1_type***. The configuration type of the first backup.
  - ***device2_id***. The ID of the second device.
  - ***backup2_id***. The ID of the second backup.
  - ***backup2_type***. The configuration type of the second backup.

- ***list_agents***. Returns a paginated list of agents.
  - ***limit***. Integer between 1 and 50. Defines results per page. The default value is 10.
  - ***offset***. Integer. The number of results to skip for pagination. The default value is zero.
- ***list_jobs***. Returns a paginated list of currently running jobs.
  - ***limit***. Integer between 1 and 50. Defines results per page. The default value is 10.
  - ***offset***. Integer. The number of results to skip for pagination. The default value is zero.
- ***get_job_by_id***. Returns a single job.
  - ***job_id***. Integer. Required. The ID of the job.
- ***list_historic_jobs***. Returns a paginated list of historic (completed) jobs.
  - ***limit***. Integer between 1 and 50. Defines results per page. The default value is 10.
  - ***offset***. Integer. The number of results to skip for pagination. The default value is zero.
- ***list_logs***. Returns a paginated list of system logs.
  - ***limit***. Integer between 1 and 50. Defines results per page. The default value is 10.
  - ***offset***. Integer. The number of results to skip for pagination. The default value is zero.
- ***status***. Returns the combined system status (appliance, storage, memory, system, High Availability cluster). No additional parameters.
- ***get_device_compliance_results***. Returns the results of running compliance rules against a device.
  - ***device_id***. Integer. Required. The ID of the device.
- ***list_compliance_policies***. Returns a paginated list of compliance policies.
  - ***limit***. Integer between 1 and 50. Defines results per page. The default value is 10.
  - ***offset***. Integer. The number of results to skip for pagination. The default value is zero.
- ***get_compliance_policy_by_id***. Returns a single compliance policy.
  - ***policy_id***. Integer. Required. The ID of the policy.
- ***list_plugins***. Returns all plugins without pagination. No additional parameters.
- ***list_domains***. Returns a paginated list of domains.
  - ***limit***. Integer between 1 and 50. Defines results per page. The default value is 10.
  - ***offset***. Integer. The number of results to skip for pagination. The default value is zero.

TIP: Paginated tools are offset-based, rather than using cursors. Pass the next offset value to fetch the next page.

Chapter 2

Installing the Skylar ComplianceSyncPack

Overview

This manual describes how to install the "Skylar Compliance" SyncPack and the "Skylar Compliance" PowerPack.

This chapter covers the following topics:

Prerequisites for this SyncPack *13*

Installing the SyncPack *13*

Installing and Configuring the PowerPack *15*

Prerequisites for this SyncPack

The following table lists the port access required by Skylar Automation and this SyncPack:

Source IP	Skylar Automation Destination	Skylar Automation Source Port	Destination Port	Requirement
Skylar Automation	Skylar One API	Any	TCP 443	Skylar One API Access
Skylar Automation	Skylar Compliance API	Any	TCP 443	Skylar Compliance API Access
Skylar Automation	Skylar One Database	Any	TCP 7706	Skylar One Database Access

Installing the SyncPack

A SyncPack file has the **.whl** file extension type. You can download the SyncPack file from the ScienceLogic Support site.

WARNING: If you are *upgrading* to this version of the SyncPack from a previous version, make a note of any settings you made on the **Configuration** pane of the various integration applications in this SyncPack, as these settings are *not* retained when you upgrade.

Downloading the SyncPack

NOTE: If you are installing or upgrading to the latest version of this SyncPack in an offline deployment, see *Installing or Upgrading in an Offline Environment* to ensure you install any external dependencies.

To locate and download the SyncPack:

1. Go to the ScienceLogic Support Center at https://support.sciencelogic.com/s/.
2. Go to the **SyncPacks** page (Skylar Automation > SyncPacks).
3. In the ***Search*** field, search for the SyncPack and select it from the search results. The **Release Version** page appears.
4. On the **[Files]** tab, click the down arrow next to the SyncPack version that you want to install, and select *Show File Details*. The **Release File Details** page appears.
5. Click the **[Download File]** button to download the SyncPack.

After you download the SyncPack, you can import it to your Skylar Automation system using the Skylar Automation user interface.

Importing the SyncPack

To import a SyncPack in the Skylar Automation user interface:

1. On the **SyncPacks** page ( ) of the Skylar Automation user interface, click **[Import SyncPack]**. The **Import SyncPack** page appears.
2. Click **[Browse]** and select the **.whl** file for the SyncPack you want to install. You can also drag and drop a **.whl** file to the **Import SyncPack** page.
3. Click **[Import]**. Skylar Automation registers and uploads the SyncPack. The SyncPack is added to the **SyncPacks** page.
4. You will need to activate and install the SyncPack in Skylar Automation. For more information, see the following topic.

NOTE: You cannot edit the content package in a SyncPack published by ScienceLogic. You must make a copy of a ScienceLogic SyncPack and save your changes to the new SyncPack to prevent overwriting any information in the original SyncPack when upgrading.

Activating and Installing the SyncPack

To activate and install a SyncPack in the Skylar Automation user interface:

1. On the **SyncPacks** page of the Skylar Automation user interface, click the **[Actions]** button ( ) for the SyncPack you want to install and select *Activate & Install*. The **Activate & Install SyncPack** modal appears.

   NOTE: If you try to activate and install a SyncPack that is already activated and installed, you can choose to "force" installation across all the nodes in the Skylar Automation system.

   TIP: If you do not see the SyncPack that you want to install, click the Filter icon ( ) on the **SyncPacks** page and select *Toggle Inactive SyncPacks* to see a list of the imported PowerPacks.

2. Click **[Yes]** to confirm the activation and installation. When the SyncPack is activated, the **SyncPacks** page displays a green check mark icon ( ) for that SyncPack. If the activation or installation failed, then a red exclamation mark icon ( ) appears.
3. For more information about the activation and installation process, click the highlighted version in the **Installed SyncPack** column for that SyncPack. For a successful installation, the "Activate & Install SyncPack" application appears, and you can view the Step Log for the steps. For a failed installation, go to the hidden "activate & Install SyncPack" application on the **Applications** page and check the step logs.

4. If you have other versions of the same SyncPack on your Skylar Automation system, you can click the **[Actions]** button (⋮) for that SyncPack and select *Change active version* to activate a different version other than the version that is currently running.

Installing and Configuring the PowerPack

The following topics describe how to install and configure the "Skylar Compliance" PowerPack to work with the "Skylar Compliance" SyncPack.

Installing the PowerPack

The "Skylar Compliance" PowerPack includes the following tools, which you will use with the "Skylar Compliance" SyncPack:

- The "Restorepoint Connectivity" Dynamic Application, which tests SSH connectivity and indicates devices to be onboarded in Skylar Compliance.
- The "Restorepoint Second Password" Dynamic Application, which allows you to align a second credential to a device. For example, if you are a Cisco user, you can configure the privileged password for your device.
- Event policies for Restorepoint.
- A "Restorepoint" device class.
- A device group called "Restorepoint Devices", which includes a dynamic rule that matches devices with aligned Dynamic Applications, including the "Restorepoint Connectivity" Dynamic Application.
- The Skylar Compliance MIB is available in your Skylar Compliance system. The MIB must be loaded before you can use the PowerPack. For more information, see Downloading and Compiling the Skylar ComplianceMIB Files.

TIP: By default, installing a new version of a PowerPack overwrites all content from a previous version of that PowerPack that has already been installed on the target system. You can use the ***Enable Selective PowerPack Field Protection*** setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields.

To download and install the PowerPack:

1. Search for and download the PowerPack from the **PowerPacks** page at the ScienceLogic Support Center (Skylar One > PowerPacks, login required).
2. In Skylar One, go to the **PowerPacks** page (System > Manage > PowerPacks).
3. Click the **[Actions]** button and choose *Import PowerPack*. The **Import PowerPack** dialog box appears.
4. Click **[Browse]** and navigate to the PowerPack file from step 1.
5. Select the PowerPack file and click **[Import]**. The **PowerPack Installer** modal displays a list of the

PowerPack contents.

6. Click **[Install]**. The PowerPack is added to the **PowerPacks** page.

> **NOTE:** If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPacks** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Chapter 3

Configuring Applications for the Skylar Compliance SyncPack

Overview

This chapter describes how to configure Skylar One (formerly SL1) and Skylar Automation (formerly PowerFlow) so you can use the Skylar Automation applications in the "Skylar Compliance" SyncPack.

This chapter covers the following topics:

Workflow for Configuring Skylar One andSkylar Automation *18*

Configuring Skylar One *18*

Configuring Skylar Automation *21*

Troubleshooting the Skylar Compliance SyncPack *30*

Workflow for Configuring Skylar One andSkylar Automation

The following workflows describe how to configure Skylar One and Skylar Automation to work with the "Skylar Compliance" SyncPack:

Configuring Skylar One

1. *Create an SSH credential for discovering devices*
2. *Align the "Restorepoint Connectivity" Dynamic Application with the Skylar One devices you want to add to Skylar Compliance*
3. *Align the "Restorepoint Second Password" Dynamic Application with the Skylar One devices you want to add to Skylar Compliance*

Configuring Skylar Automation

1. *Obtain the API Token in Skylar Compliance*
2. *Use the "Skylar Compliance Base Config" file to create a configuration object*
3. *Configure the "Skylar Compliance: Sync Devices" application*
4. *Configure the "Skylar Compliance: Get the List of Logs from Skylar Compliance" application*
5. *Configure the "Skylar Compliance: Get list of credentials from Skylar One" application*
6. *Configure the "Skylar Compliance: Gather Compliance Logs from Skylar Compliance" application*
7. *Schedule Skylar Automation applications*

Configuring Skylar One

The following topics cover how to set up your Skylar One instance to work with the "Skylar Compliance" SyncPack.

Creating an SSH Credential for Discovering Devices

In Skylar One, you will need to create an SSH credential for the devices that you want to discover and add to Skylar Compliance. You will then need to use this credential to manually align the "Restorepoint Connectivity" Dynamic Application, which is used when you discover a device and add it to Skylar Compliance.

NOTE: If needed, create a new organization in Skylar One for the device you want to discover. For more information, see *Creating and Editing Organizations*.

To create an SSH/Key credential:

1. Go to the **Credentials** page (Manage > Credentials or System > Manage > Credentials in the classic user interface).
2. Click the **[Create New]** button and then select *Create SSH/Key Credential*. The **Edit Credential** modal page appears.
3. Complete the following fields:
    - ***Name***. Name of the credential. Can be any combination of alphanumeric characters.
    - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the ***What organization manages this service?*** field to align the credential with those specific organizations.
    - ***Timeout (ms)***. Time, in milliseconds, after which Skylar One will stop trying to communicate with the device from which you want to retrieve data. The default is 1500.
    - ***Hostname/IP***. Hostname or IP address of the device you want to discover.
        - You can include the variable **%D** in this field. Skylar One will replace the variable with the IP address of the current device (device that is currently using the credential).
        - You can include the variable **%N** in this field. Skylar One will replace the variable with hostname of the current device (device that is currently using the credential). If Skylar One cannot determine the hostname, Skylar One will replace the variable with the primary, management IP address for the current device.
    - ***Port***. Port number associated with the data you want to retrieve. The default TCP port for SSH servers is 22. The protocol attribute of your device in Skylar Compliance is set based on the port specified in this credential. If the port is 23, the attribute is set to telnet/tftp. For all other ports, the attribute is set to ssh/tftp.
    - ***Username***. Username for an SSH or user account on the device to be monitored. Make sure that this user has the permissions necessary to query the credentials from Skylar One.
    - ***Password***. Password for an SSH or user account on the device to be monitored.
    - ***Private Key (PEM Format)***. Leave this field blank.
4. Click **[Save]**. You will use this new credential in the following procedure, when you align the "Restorepoint Connectivity" Dynamic Application with the Skylar One device.

> **NOTE:** The Skylar One account that is being used by Skylar Automation to authenticate into Skylar One must have the secondary organization membership set to "(All Organizations)" to enable Skylar Automation to pull device lists from all organizations. For more information, see *Account Types*.

Align the "Restorepoint Connectivity" Dynamic Application with Skylar One Devices

You will use your new credential to manually align the "Restorepoint Connectivity" Dynamic Application to one or more Skylar One devices so you can add (or "onboard") those devices to Skylar Compliance.

To align the "Restorepoint Connectivity" Dynamic Application:

1. Go to the **Devices** page in Skylar One and select the device you want to add to Skylar Compliance. The **Device Investigator** page appears.
2. On the **[Collection]**s tab, click **[Edit]** and then click **[Align Dynamic Application]**. The **Align Dynamic Application** window appears.
3. Click *Choose Dynamic Application*. The **Choose Dynamic Application** window appears.
4. Search for the "Restorepoint Connectivity" Dynamic Application, select it, and click **[Select]**. The Dynamic Application now appears in the **Align Dynamic Application** window.
5. Clear the checkbox next to *Use Device SNMP Credential* and click *Choose Credential*. The **Choose Credential** window appears.
6. Select the credential for that device (from the previous procedure) and click **[Select]** . The name of the selected credential now appears in the **Align Dynamic Application** window.
7. Click **[Align Dynamic App]**. When the Dynamic Application is successfully aligned, it is added to the Collections tab, and a confirmation message appears at the bottom of the tab.
8. Repeat these steps for every device you want to add to Skylar Compliance.

The next time you discover a device in Skylar One and run the "Skylar Compliance: Sync Devices" application in Skylar Automation, any devices you discovered in Skylar One that are aligned with the "Restorepoint Connectivity" Dynamic Application get added to Skylar Compliance. Those devices are also part of the "Restorepoint Devices" Device Group.

Align the "Restorepoint Second Password" Dynamic Application with Skylar One Devices

To sync devices that have multiple sets of credentials with Skylar Compliance, you will need to align those devices to the "Restorepoint Second Password" Dynamic Application.

To align devices to the "Restorepoint Second Password" Dynamic Application:

1. Go to the **Devices** page in Skylar One and select the device with multiple sets of credentials that you want to add to Skylar Compliance. The **Device Investigator** page appears.
2. On the **[Collections]** tab, click **[Edit]** and then click **[Align Dynamic Application]**. The **Align Dynamic Application** window appears.
3. Click *Choose Dynamic Application*. The **Choose Dynamic Application** window appears.
4. Search for the "Restorepoint Second Password" Dynamic Application, select it, and click **[Select]**. The Dynamic Application now appears in the **Align Dynamic Application** window.
5. Clear the checkbox next to *Use Device SNMP Credential* and click *Choose Credential*. The **Choose Credential** window appears.
6. Select the additional credential for that device and click **[Select]** . The name of the selected credential now appears in the **Align Dynamic Application** window.
7. Click **[Align Dynamic App]**. When the Dynamic Application is successfully aligned, it is added to the Collections tab, and a confirmation message appears at the bottom of the tab.
8. Repeat these steps for every device with multiple credentials you want to add to Skylar Compliance.

Configuring Skylar Automation

The following topics cover how to set up your Skylar Automation instance to work with the "Skylar Compliance" SyncPack.

Obtaining the API Token in Skylar Compliance

The following procedure is relevant for Skylar Compliance 5.4.0 and later.

IMPORTANT: API tokens that are created by a Skylar Compliance user will be aligned with the account that was used to create it. For instance, if you are logged into Skylar Compliance as an admin when you create the API token, that token will have administrator-level privileges, and any actions performed using the token will be logged under the administrator user. As an alternative, you can create a new user named something like "SL1_API", and then you can create the token while logged in as that user.

To obtain your API token for the ***restorepoint_api_token*** Configuration Data field:

1. In Skylar Compliance, go to the **Users** page **(Administration > Users)** and click the **API Tokens** tab.
2. Click **Add Token** and give the token a new description.
3. Copy and paste the token into the ***restorepoint_api_token*** Configuration Data field for the Skylar Compliance configuration object.

Creating a Configuration Object in Skylar Automation

For this SyncPack, you can make a copy of the "Skylar Compliance Base Config" configuration object, which is the sample configuration file that was installed with the "Skylar Compliance" SyncPack.

TIP: The "Skylar Compliance Base Config" configuration object contains all of the required variables. Update the variables from that object to match your Skylar One and Skylar Compliance settings.

To create a configuration object based on the "Skylar Compliance Base Config" configuration object:

1. In the Skylar Automation user interface, go to the **Configurations** page (⚙).
2. Click the **[Actions]** button (⋮) for the "Skylar Compliance Base Config" configuration object and select *Edit*. The **Configuration** pane appears.

3. Click **[Copy as]**. The **Create Configuration** pane appears.
4. Complete the following fields:
    - ***Friendly Name***. Name of the configuration object that will display on the **Configurations** page.
    - ***Description***. A brief description of the configuration object.
    - ***Author***. User or organization that created the configuration object.
    - ***Version***. Version of the configuration object.

5. In the ***Configuration Data*** field, update the default variable definitions to match your Skylar Automation configuration:
    - ***sl1_url***. Type the URL for your associated Skylar One system.
    - ***sl1_user***. Type the username for your Skylar One system. Make sure this user has the permissions necessary to query the credentials from Skylar One.
    - ***sl1_password***. Type the password for your Skylar One system.
    - ***sl1_db_host***. Type the URL for your associated Skylar One database.
    - ***sl1_db_user***. Type the username for your Skylar One database.
    - ***sl1_db_password***.Type the password for your Skylar One database.
    - ***restorepoint_url***. Type the URL for your associated Skylar Compliance system.
    - ***restorepoint_api_token***. Type the API token for your Skylar Compliance system. See the *Obtaining the API Token in Skylar Compliance* section for steps on getting the token.
    - ***default_restorepoint_device_type***. Type the default device type for your Skylar Compliance system.
    - ***default_backup_interval***. Type the default time for the Backup Interval for your Skylar Compliance device. The value for the default_backup_interval field uses the following format: *second minute hour * * * * @0@@0@0*. The default value for version 2.1.0 is *0 15 * * * * *
    - ***create_custom_link***. Type a value to create an optional custom link from Skylar One to Skylar Compliance. If you are running Skylar One platform version 10.2.0 or later and have custom links enabled, you can set the value to *1* to automatically add the custom link definition for Skylar Compliance. The default value is *False/0*.
    - ***restorepoint_ui_url***. Type an optional user access URL that is different than the Skylar Compliance URL that is used to integrate with Skylar Automation.
    - ***timestamp***. The "Skylar Compliance: Get List of Credentials" application queries Skylar One for updated credentials and stores the last time that Skylar One was queried. Type a value that specifies the number of hours for the application to query Skylar One for updated credentials, if no previous timestamp is available (e.g. the first execution of the application). The application will update the credentials in Skylar Compliance that have been updated in Skylar One within the specified number of hours.
    - ***default_monitoring_monitor_device***. Type *True* or *False* to enable or disable device monitoring. The default value is *True*.
    - ***default_monitoring_fail_after***. Type how many failed attempts to onboard a device before Skylar Automation will stop attempting to discover the device.
    - ***default_monitoring_is_ping_type***. Type *True* or *False* to enable or disable ICMP ping rather than TCP connection. The default value is *True*.
    - ***default_monitoring_email_when_down***. Type *True* or *False* to enable or disable sending an email when the device is down. The default value is *False*.

- ***default_monitoring_email_when_up***. Type *True* or *False* to enable or disable sending an email when the device is back up. The default value is *True*.

6. The other optional values in the ***Configuration Data*** field require JSON code to edit their values. Click **[Toggle JSON Editor]** to show the JSON code.
7. In the ***Configuration Data*** field, be sure to include the required block of code to ensure that the applications aligned to this configuration object do not fail:

```
{
   "encrypted": false,
   "name": "<sl1_db_host>",
   "value": "${<IP address of Skylar One Host>}"
}
```

   For example:

```
{
   "encrypted": false,
   "name": "sl1_db_host",
   "value": "10.2.11.42"
}
```

8. To create a configuration variable, define the following keys:
   - ***encrypted***. Specifies whether the value will appear in plain text or encrypted in the JSON file. If you set this to "true", when the value is uploaded, Skylar Automation encrypts the value of the variable. The plain text value cannot be retrieved again by an end user. The encryption key is unique to each Skylar Automation system. The value is followed by a comma.
   - ***name***. Specifies the name of the configuration file, without the JSON suffix. This value appears in the user interface. The value is surrounded by double-quotes and followed by a comma.
   - ***value***. Specifies the value to assign to the variable. The value is surrounded by double-quotes and followed by a comma.
9. Click **[Save]**. You can now align this configuration object with one or more applications.

Configuring the "Skylar Compliance: Sync Devices" Application

The next time you discover a device in Skylar One and run the "Skylar Compliance: Sync Devices" application, any devices you discovered in Skylar One that are aligned with the “Restorepoint Connectivity" Dynamic Application are added to Skylar Compliance. Those devices are also part of the "Restorepoint Devices" device group.

If you include the SSH or Telnet credential you created earlier in a discovery session, the "Restorepoint Connectivity" Dynamic Application is automatically aligned. Optionally, you can manually align the Dynamic Application with your devices using the credential. Based on the Dynamic Application alignment,

the device is also automatically included in a Restorepoint device group. For more information about discovering a device in Skylar One, see the ***Discovery and Credentials*** manual .

To run the "Skylar Compliance: Sync Devices" application:

1. Go to the **Applications** page and select the "Skylar Compliance: Sync Devices" application.
2. Click the **[Configuration]** button. The **Configuration** pane appears.
3. In the ***Configuration*** drop-down, select *the configuration object you created earlier*.
4. In the ***restorepoint_config*** field, select *Enable* or *Disable* to allow device change detection. You should select the same value you entered in the selected configuration object.
5. Toggle on (blue) the ***generate_report*** configuration option to enable a report to be generated when devices are successfully synced or not.
6. Update the remaining fields as needed, and then click **[Save]**.
7. Click the **[Run]** button. The following actions occur:
    - If the Skylar One organization exists as a domain in Skylar Compliance, the device is added to that domain. Otherwise, a new domain is created in Skylar Compliance that maps to the Skylar One organization.
    - If needed, a new credential is created in Skylar Compliance that maps to the new Skylar One credential.
    - A new device is added in Skylar Compliance that maps to the new device in Skylar One :
        - The device is associated with the appropriate domain and credential.
        - The device is associated with an agent that maps to the Skylar One Data Collector monitoring that device, using a pre-defined mapping from the "Skylar Compliance Base Config" configuration object.
        - The device is configured with a plugin that maps to the Skylar One Device Class for that device, using a pre-defined mapping from the "Skylar Compliance Base Config" configuration object.

TIP: When a device is synced between Skylar One and Skylar Compliance, you can click the **[Tools]** button on the **Device Investigator** page in Skylar One for that synced device. Then you can click a custom "Skylar Compliance" link to navigate to the **Device Details** page for that device in Skylar Compliance. You can also view automation actions for an event on a synced device in Skylar One to view detailed logs about the event.

Configuring the "Skylar Compliance: Get the List of Logs from Skylar Compliance" Application

The "Skylar Compliance: Get the List of Logs from Skylar Compliance" application queries the Skylar Compliance API to collect backup success and failure logs from Skylar Compliance. These logs are also synced to Skylar One. You can use Skylar Automation to compare the logs to make sure the backups ran successfully in Skylar Compliance.

To run the "Skylar Compliance: Get the List of Logs from Skylar Compliance" application:

1. Go to the **Applications** page and select the "Skylar Compliance: Get the List of Logs from Skylar Compliance" application.
2. Click the **[Configuration]** button. The **Configuration** pane appears.
3. In the ***Configuration*** field, select *the configuration object you created earlier*.
4. In the ***restorepoint_config*** field, select *Enable* or *Disable* to allow device change detection. You should select the same value you entered in the selected configuration object.
5. Update the remaining fields as needed, and then click **[Save]**.
6. Click the **[Run]** button.

You should configure this application to run on a schedule, such as once a week or more if you frequently back up devices in Skylar Compliance. For more information, see *Scheduling Skylar Automation Applications*.

Configuring the "Skylar Compliance: Get list of credentials from Skylar One" Application

The "Skylar Compliance: Get list of credentials from Skylar One" application queries Skylar One for existing credentials and matches them against credentials in Skylar Compliance. If there is a change to the credential in Skylar One and the credential exists in Skylar Compliance, the credential is updated with the new information.

To run the "Skylar Compliance: Get list of credentials from Skylar One" application:

1. Go to the **Applications** page and select the "Skylar Compliance: Get list of credentials from Skylar One" application.
2. Click the **[Configuration]** button. The **Configuration** pane appears.
3. In the ***Configuration*** field, select *the configuration object you created earlier*.
4. Update the remaining fields as needed, and then click **[Save]**.
5. Click the **[Run]** button.

You should configure this application to run on a schedule, such as once a week. For more information, see *Scheduling Skylar Automation Applications*.

Configuring the "Skylar Compliance: Gather Compliance Logs from Skylar Compliance" Application

The "Skylar Compliance: Gather Compliance Logs from Skylar Compliance" application checks for compliance logs from Skylar Compliance and syncs them to Skylar One to create events for the compliance alerts in Skylar One.

To run the "Skylar Compliance: Gather Compliance Logs from Skylar Compliance" application:

1. Go to the **Applications** page and select the "Skylar Compliance: Gather Compliance Logs from Skylar Compliance" application.
2. Click the **[Configuration]** button. The **Configuration** pane appears.
3. In the ***Configuration*** field, select *the configuration object you created earlier*.

4. Update the remaining fields as needed, and then click **[Save]**.
5. Click the **[Run]** button.

You should configure this application to run on a schedule, such as once a week. For more information, see *Scheduling Skylar Automation Applications*.

Configuring the "Skylar Compliance: Pre Check" Application

The "Skylar Compliance: Pre Check" application verifies that both the Skylar One and Skylar Compliance systems are correctly configured for device synchronization. It assesses the current onboarding capacity of the Skylar Compliance system, providing visibility into how many additional devices can be registered. Additionally, it performs a comprehensive permissions check on the Skylar One system, identifying any denied permissions that must be enabled to ensure smooth operation of the Skylar Compliance SyncPack.

To run the "Skylar Compliance: Pre Check" application:

1. Go to the **Applications** page and select the "Skylar Compliance: Pre Check" application.
2. Click the **[Configuration]** button. The **Configuration** pane appears.
3. In the ***Configuration*** field, select *the configuration object you created earlier*.
4. Update the remaining fields as needed, and then click **[Save]**.
5. Click the **[Run]** button.

You should configure this application to run on a schedule, such as once a week. For more information, see *Scheduling Skylar Automation Applications*.

Configuring the "Skylar Compliance: Create or Update Custom Links" Application

The "Skylar Compliance: Create or Update Custom Links" Application" application allows you to create and update custom links within the Skylar One platform. It enables the addition of direct navigation links to Skylar Compliance-onboarded devices from Skylar One device pages, streamlining access and improving operational efficiency. By integrating these links, you can quickly transition from Skylar One to the corresponding Skylar Compliance device, enhancing workflow and reducing navigation time.

To run the "Skylar Compliance: Create or Update Custom Links" application:

1. Go to the **Applications** page and select the "Skylar Compliance: Create or Update Custom Links" application.
2. Click the **[Configuration]** button. The **Configuration** pane appears.
3. In the ***Configuration*** field, select *the configuration object you created earlier*.
4. Update the following fields as necessary:
    - ***update_existing_custom_link***. Enabled by default (blue). When enabled, it updates the custom link if it already exists; otherwise, it creates a new one. You can disable this toggle when setting up a new system to ensure only new links are created.
5. Click the **[Save]** button.
6. Click the **[Run]** button.

You should configure this application to run on a schedule, such as once a week. For more information, see *Scheduling Skylar Automation Applications*.

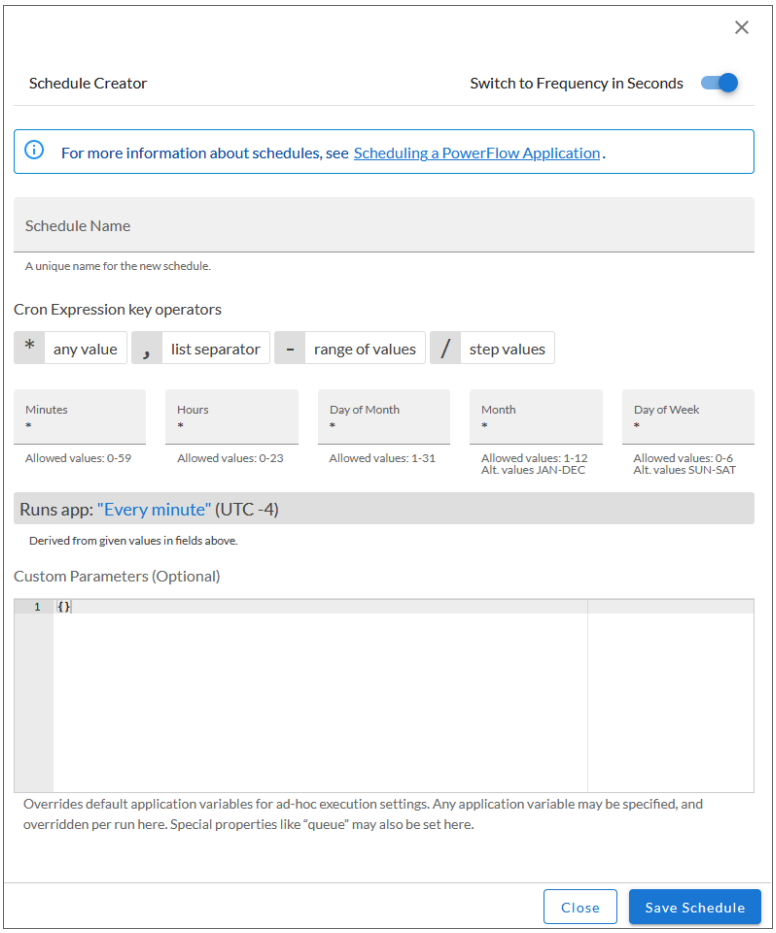
Scheduling Skylar Automation Applications

You can create one or more schedules for a single application in the Skylar Automation user interface. When creating each schedule, you can specify the queue and the configuration file for that application.

To schedule an application:

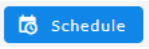
1. On the **Applications** page (), click the **[Schedule]** button for the application you want to schedule. The **Scheduler** window appears.
2. In the **Schedule List** pane, click the down arrow icon () next to an existing schedule to view the details for that schedule.
3. In the **Schedule Creator** pane, complete the following fields for the default ***Frequency*** setting:
   - ***Schedule Name***. Type a name for the schedule.
   - ***Frequency in seconds***. Type the number of seconds per interval that you want to run the application.
   - ***Custom Parameters***. Type any JSON parameters you want to use for this schedule, such as information about a configuration file or mappings.

4. To use a cron expression, click the ***Switch to Cron Expression*** toggle to turn it blue. If you select this option, you can create complicated schedules based on minutes, hours, the day of the month, the month, and the day of the week:



As you update the cron expression, the **Schedule** window displays the results of the expression in more readable language, such as *Runs app: "Every 0 and 30th minute past every hour on Sat"*, based on 0,30 in the ***Minutes*** field and 6 in the ***Day of Week*** field.

5. Click **[Save Schedule]**. The schedule is added to the **Schedule List** pane. Also, on the **Applications** page, the Schedule button now displays with a dark blue background:



NOTE: After you create a schedule, it continues to run until you delete it. Also, you cannot edit an existing schedule, but you can delete it and create a similar schedule if needed.

To view or delete an existing schedule:

1. On the **Applications** page, click the **[Schedule]** button for the application that contains a schedule you want to delete. The **Scheduler** window appears.

2. Click the down arrow icon ( ) to view the details of an existing schedule.
3. To delete the selected schedule, click the Actions icon ( ) and select **[Delete]**.

> **TIP:** On the **Scheduler** window for a Skylar Automation application, you can click the **[Copy as]** button from the **Schedule List** pane to make a copy of an existing schedule.

Troubleshooting the Skylar Compliance SyncPack

The following sections describe resolutions to some issues you might encounter when using the Skylar Compliance SyncPack.

Scaling Issues with the Grouping Device Count Configuration Option

The ***grouping_device_count*** configuration option in the "Skylar Compliance: Sync Devices" application allows you to define the number of devices to be onboarded per batch. By default, 500 devices will be onboarded per batch. Increasing the value in this field allows you to onboard a larger number of devices, but increases the load on Skylar Compliance due to the number of API requests. This can result in a read timeout error. To accommodate for the increased load, you can either lower the ***grouping_device_count*** value to decrease the number of devices in a batch, or increase the value in the ***read_timeout*** configuration option from the default of "30" to allow more time for Skylar Compliance to process the requests.

Sync Failures Due to Dynamic Application Configuration Options

If you experience issues with the "Skylar Compliance: Sync Devices" application, check that the globally unique identifier of the ***DA_Restorepoint_Connectivity*** configuration option matches the globally unique identifier (GUID) of the "Restorepoint Connectivity" Dynamic Application in Skylar One. If you have devices that use a second password, check to be sure that the globally unique identifier of the ***DA_Restorepoint_Second_Password*** configuration option matches the GUID of the "Restorepoint Second Password" Dynamic Application in Skylar One. If these configuration options have the incorrect GUID (or no value at all), you will experience errors when running the application.

Troubleshooting Device Sync Errors

If you receive an error that no new device was found to sync with the Skylar Compliance server, check the following:

- If you toggled on (blue) the ***generate_report*** configuration option on the "Skylar Compliance: Sync Devices" application, you can view a report of the failed sync, including what step failed, device details, and more. To view the report, go to the **Reports** page (), locate the "Skylar Compliance: Sync Devices" application, and look for the report that generated from the failed sync.
- Check to be sure you have added a credential to the device you want to sync. If you do not, you will see the device listed in the log of the "Get 'Dynamic Applications' aligned with Skylar One devices" application as a warning that the device does not contain a credential.
- Check to be sure that the credential associated with the device is an SSH credential. Otherwise you will see an error that the device is not attached to an SSH credential.
- Check to be sure that the "Skylar Compliance Connectivity" Dynamic Application is aligned to the device. If it is not, the device will not be added to the "Skylar Compliance Devices" group and you will see an error that no devices are found in Skylar One to sync to Skylar Compliance.

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010