Monitoring Fortinet: Fortigate

Fortinet: Fortigate PowerPack version 101

Table of Contents

Chapter 1

Introduction

Overview

This manual describes how to monitor Fortinet: Fortigate devices in Skylar One using the "Fortinet: Fortigate" PowerPack.

The following sections provide an overview of Fortinet: Fortigate and the "Fortinet: Fortigate" PowerPack:

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

What is Fortinet: Fortigate

Fortinet: Fortigate is a next-generation firewall that provides network security, threat identification and protection, and traffic management.

What Does the Fortinet: Fortigate PowerPack Monitor?

To monitor Fortinet: Fortigate devices using Skylar One, you must install the "Fortinet: Fortigate" PowerPack. This PowerPack enables you to discover, model, and collect data about Fortinet: Fortigate devices.

The "Fortinet: Fortigate" PowerPack includes:

- Dynamic Applications to discover, model, and monitor performance metrics and collect configuration data for Fortinet: Fortigate devices
- Event Policies and corresponding alerts that are triggered when Fortinet: Fortigate devices meet certain status criteria

Installing the Fortinet: Fortigate PowerPack

Before completing the steps in this manual, you must import and install the latest version of the "Fortinet: Fortigate" PowerPack.

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. For more information, see the section on *Global Settings*.

NOTE: For details on upgrading Skylar One, see the relevant *Skylar One Platform Release Notes*.

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 2

Configuration and Discovery

Overview

The following sections describe how to configure and discover Fortinet: Fortigate devices for monitoring by Skylar One using the "Fortinet: Fortigate" PowerPack:

This chapter covers the following topics:

Creating a Credential for Fortinet: Fortigate

To configure Skylar One to monitor Fortinet: Fortigate devices, you must first create an SNMP credential. This credential allows the Dynamic Applications in the "Fortinet: Fortigate" PowerPack to communicate with your Fortinet: Fortigate devices.

SNMP Credentials allow Skylar One to access SNMP data on a managed device. Skylar One uses SNMP credentials to perform discovery, run auto-discovery, and gather information from SNMP Dynamic Applications.

To create an SNMP credential in the classic user interface:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the **[Actions]** button and select *Create SNMP Credential*. The **Credential Editor** page appears.
3. Supply values in the following fields:
    - ***Profile Name***. Name of the credential. Can be any combination of alphanumeric characters. This field is required.

- ***SNMP Version***. SNMP version. Choices are *SNMP V1*, *SNMP V2*, and *SNMP V3*. The default value is *SNMP V2*.
- ***Port***. The port Skylar One will use to communicate with the external device or application. The default value is *161*. This field is required.
- ***Timeout (ms)***. Time, in milliseconds, after which Skylar One will stop trying to communicate with the SNMP device. The default value is *1500*.
- ***Retries***. Number of times Skylar One will try to authenticate and communicate with the external device. The default value is *1*.

SNMP V1/V2 Settings

These fields appear if you selected *SNMP V1* or *SNMP V2* in the ***SNMP Version*** field. The fields are inactive if you selected SNMP V3.

- ***SNMP Community (Read-Only)***. The SNMP community string (password) required for read-only access of SNMP data on the remote device or application. For SNMP V1 and SNMP V2 credentials, you must supply a community string, either in this field or in the ***SNMP Community (Read/Write)*** field.
- ***SNMP Community (Read/Write)***. The SNMP community string (password) required for read and write access of SNMP data on the remote device or application. For SNMP V1 and SNMP V2 credentials, you must supply a community string, either in this field or in the ***SNMP Community (Read Only)*** field.

SNMP V3 Settings

These fields appear if you selected *SNMP V3* in the ***SNMP Version*** field. These fields are inactive if you selected SNMP V1 or SNMP V2.

- ***Security Name***. Name for SNMP authentication. This field is required.
- ***Security Passphrase***. Password to authenticate the credential. This value must contain at least 8 characters. This value is required if you use a ***Security Level*** that includes authentication.
- ***Authentication Protocol***. Select an authentication algorithm for the credential. This field is required. Choices are:
    - *MD5*. This is the default value.
    - *SHA*
    - *SHA-224*
    - *SHA-256*
    - *SHA-384*
    - *SHA-512*

NOTE: The *SHA* option is SHA-128.

- ***Security Level***. Specifies the combination of security features for the credentials. This field is required. Choices are:
    - *No Authentication / No Encryption*.
    - *Authentication Only*. This is the default value.
    - *Authentication and Encryption*.
- ***SNMP v3 Engine ID***. The unique engine ID for the SNMP agent you want to communicate with. (SNMPv3 authentication and encryption keys are generated based on the associated passwords and the engine ID.) This field is optional.
- ***Context Name***. A context is a mechanism within SNMPv3 (and AgentX) that allows you to use parallel versions of the same MIB objects. For example, one version of a MIB might be associated with SNMP Version 2 and another version of the same MIB might be associated with SNMP Version 3. For SNMP Version 3, specify the context name in this field. This field is optional.
- ***Privacy Protocol***. The privacy service encryption and decryption algorithm. This field is required. Choices are:
    - *DES*. This is the default value.
    - *AES-128*
    - *AES-192*
    - *AES-256*
    - *AES-256-C*. This option is for discovering Cisco devices only.
- ***Privacy Protocol Passphrase***. Privacy password for the credential. This field is optional.

4. Click the **[Save]** button to save the new SNMP credential.
5. Repeat steps 1-4 for each SNMP-enabled device in your network that you want to monitor with Skylar One.

NOTE: When you define an SNMP Credential, Skylar One automatically aligns the credential with all organizations of which you are a member.

For more details on creating credentials, see the manual ***Discovery and Credentials***.

Discovering Fortinet: Fortigate Devices

To run an unguided discovery:

1. On the **Devices** page ( ) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears.
2. Click the **[Unguided Network Discovery Workflow]** button. Additional information about the requirements for discovery appears in the **General Information** pane to the right.
3. Click **[Select]**. The three-step discovery wizard appears, starting with the **Basic Information** page.
4. Complete the following fields:

- ***Discovery Session Name***. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the **[Discovery Sessions]** tab.
- ***Description***. Type a short description of the discovery session. You can use the text in this description to search for the discovery session on the **[Discovery Sessions]** tab. Optional.
- ***Select the organization to add discovered devices to***. Select the name of the organization to which you want to add the discovered devices.

5. Click **[Next]**. The **Credential Selection** page of the wizard appears.
6. On the **Credential Selection** page, you can optionally do one of the following:
    - If the credential you need is not in the list, click the **[Create New]** button and select the credential type you want to create to open the **Create Credential** window, where you can specify the name and organization for the credential, the third-party username and password, and other data such as Cloud Type and Proxy information. You can also test the credential before you save using the **Credential Tester** panel. Click **[Save & Close]** to save the credential and return to the **Credential Selection** page of the guided discovery session.
    - To edit a credential on the **Credential Selection** page, click the name of the credential you would like to edit from the ***Name*** column and edit that credential as needed. You can also test the credential before you save using the **Credential Tester** panel. Click the **[Save & Close]** button on the **Edit Credential** window to save your updates.
7. On the **Credential Selection** page of the **Add Devices** wizard, select one or more credentials to allow Skylar One to access a device's SNMP data and click **[Next]**. The **Discovery Session Details** page of the **Add Devices** wizard appears.
8. Complete the following fields:
    - ***List of IPs/Hostnames***. Provide a list of IP addresses, hostnames, or fully-qualified domain names for Skylar One to scan during discovery. This field is required. In this field, you can enter a combination of one or more of the following:
        - One or more *single IPv4 addresses* separated by commas and a new line. Each IP address must be in standard IP notation and cannot exceed 15 characters. For example, "10.20.30.1, 10.20.30.2, 10.20."
        - One or more *ranges of IPv4 addresses* with "-" (dash) characters between the beginning of the range and the end of the range. Separate each range with a comma. For example, "10.20.30.1 – 10.20.30.254".
        - One or more IP address ranges in *IPv4 CIDR notation*. Separate each item in the list with a comma. For example, "192.168.168.0/24".
        - One or more *ranges of IPv6 addresses* with "-" (dash) characters between the beginning of the range and the end of the range. Separate each range with a comma. For example, "2001:DB8:0:0:0:0:0:0-2001:DB8:0:0:0:0:0:0003".
        - One or more IP address ranges in *IPv6 CIDR notation*. Separate each item in the list with a comma. For example, "2001:DB8:0:0:0:0:0:0/117".
        - One or more hostnames (fully-qualified domain names). Separate each item in the list with a comma.

> **TIP:** You can also click the **[Upload File]** button to upload a comma-separated list of IPs.

- ***Which collector will discover these devices?***. Select an existing collector group to monitor the discovered devices. Required.

NOTE: When assigning devices to a collector group, Skylar One's multi-tenancy rules will validate that the collector group you select belongs to the organization you selected in the previous field. If you attempt to run a discovery session where the devices, collector group, and credentials do not all belong to the same organization, you will receive an error message and will not be able to save or execute the discovery session.

- ***Run after save***. Select this option to run this discovery session as soon as you click **[Save and Close]**.
- ***Advanced options***. Click the down arrow icon ( ) to access additional discovery options.

  In the **Advanced options** section, complete the following fields as needed:

  - ***Initial Scan Level***. For this discovery session only, specifies the data to be gathered during the initial discovery session. The options are:
  - *System Default (recommended)*. Use the value defined in the **Behavior Settings** page (System > Settings > Behavior) in the classic user interface of Skylar One.
  - *1. Model Device Only*. Discovery will discover if the device is up and running and if so, collect the make and model of the device. Skylar One will then generate a device ID for the device so it can be managed by Skylar One.
  - *2. Initial Population of Apps*. Discovery will search for Dynamic Applications to associate with the device. The discovery tool will attempt to collect data for the aligned Dynamic Applications. Discovery will later retrieve full sets of data from each Dynamic Application. Discovery will also perform *1. Model Device Only* discovery.
  - *3. Discover SSL Certificates*. Discovery will search for SSL certificates and retrieve SSL data. Discovery will also perform *2. Initial Population of Apps* and *1. Model Device Only*.
  - *4. Discover Open Ports*. Discovery will search for open ports. Discovery will also perform *3. Discover SSL Certificates*, *2. Initial Population of Apps*, and *1. Model Device Only*.

NOTE: If your system includes a firewall and you select *4. Discover Open Ports*, discovery might be blocked and/or might be taxing to your network.

  - *5. Advanced Port Discovery*. Discovery will search for open ports, using a faster TCP/IP connection method. Discovery will also perform *3. Discover SSL Certificates*, *2. Initial Population of Apps*, and *1. Model Device Only*.

NOTE: If your system includes a firewall and you select *5. Advanced Port Discovery*, some devices might remain in a pending state (purple icon) for some time after discovery. These devices will achieve a healthy status, but this might take several hours.

- *6. Deep Discovery*. Discovery will use nmap to retrieve the operating system name and version. Discovery will also scan for services running on each open port and can use this information to match devices to device classes. Discovery will search for open ports, using a faster TCP/IP connection method. Discovery will also perform *3. Discover SSL Certificates, 2. Initial Population of Apps*, and *1. Model Device Only*.

NOTE: For devices that don't support SNMP, option *6. Deep Discovery* allows you to discover devices that don't support SNMP and then align those devices with a device class other than "pingable". Note that option *6. Deep Discovery* is compute-intensive.

NOTE: If Skylar One cannot determine the appropriate Device Class, it will assign the device to the Generic SNMP Device Class.

- ***Scan Throttle***. Specifies the amount of time a discovery process should pause between each specified IP address (specified in the ***IP Address/Hostname Discovery List*** field). Pausing discovery processes between IP addresses spreads the amount of network traffic generated by discovery over a longer period of time. The choices are:
  - *System Default (recommended)*. Use the value defined in the **Behavior Settings** page (System > Settings > Behavior) in the classic user interface for Skylar One.
  - *Disabled*. Discovery processes will not pause.
  - *1000 Msec to 10000 Msec*. A discovery process will pause for a random amount of time between half the selected value and the selected value.
- ***Port Scan All IPs***. For the initial discovery session only, specifies whether Skylar One should scan all IP addresses on a device for open ports. The choices are:
  - *System Default (recommended)*. Use the value defined in the **Behavior Settings** page (System > Settings > Behavior) in the classic user interface for Skylar One.
  - *Enabled*. Skylar One will scan all discovered IP addresses for open ports.
  - *Disabled*. Skylar One will scan only the primary IP address (the one used to communicate with Skylar One) for open ports.
- ***Port Scan Timeout***. For the initial discovery session only, specifies the length of time, in milliseconds, after which Skylar One should stop trying to scan an IP address for open ports and begin scanning the next IP address (if applicable). Choices are:
  - *System Default (recommended)*. Use the value defined in the **Behavior Settings** page (System > Settings > Behavior).
  - Choices between 60 to 1,800 seconds.
- ***Scan Ports***. Specify a list of ports to scan, separated by colons (:). The default is *21:22:25:80:136*.

- ***Interface Inventory Timeout (ms)***. Specifies the maximum amount of time that the discovery processes will spend polling a device for the list of interfaces. After the specified time, Skylar One will stop polling the device, will not model the device, and will continue with discovery. The default value is 600,000 ms (10 minutes).
  - During the execution of this discovery session, Skylar One uses the value in this field first. If you delete the default values and do not specify another value in this field, Skylar One uses the value in the **Global Threshold Settings** page (System > Settings > Thresholds).
  - If you specify a value in this field and do not apply a device template to this discovery session, the ***Interface Inventory Timeout*** setting in the **Device Thresholds** page (Devices > Classic Devices > wrench icon > Thresholds, or Registry > Devices > Device Manager > wrench icon > Thresholds in the classic user interface) is set to this value for each discovered device. If there is no device template applied to the discovery session and no value is supplied in this field, Skylar One uses the value in the **Global Threshold Settings** page (System > Settings > Thresholds).
- ***Maximum Allowed Interfaces***. Specifies the maximum number of interfaces per devices. If a device exceeds this number of interfaces, Skylar One will stop scanning the device, will not model the device, and will continue with discovery. The default value is 10,000.
  - During the execution of this discovery session, Skylar One uses the value in this field first. If you delete the default values and do not specify another value in this field, Skylar One uses the value in the **Global Threshold Settings** page.
  - If you specify a value in this field and do not apply a device template to this discovery session, the ***Maximum Allowed Interfaces*** setting in the **Device Thresholds** page is set to this value for each discovered device. If there is no device template applied to the discovery session and no value is supplied in this field, Skylar One uses the value in the **Global Threshold Settings** page.
- ***Bypass Interface Inventory***. Specifies whether or not the discovery session should discover network interfaces.
  - *Selected*. Skylar One will not attempt to discover interfaces for each device in the discovery session. For each discovered device, the ***Bypass Interface Inventory*** checkbox on the **Device Investigator [Settings]** tab will be selected.
  - *Not Selected*. Skylar One will attempt to discover network interfaces, using the ***Interface Inventory Timeout*** value and ***Maximum Allowed Interfaces*** value.
- ***Discover non-SNMP***. Specifies whether or not Skylar One should discover devices that don't respond to SNMP requests.
  - *Selected*. Skylar One will discover devices that don't respond to the SNMP credentials selected in the ***SNMP Credentials*** field. These devices will be discovered as "pingable" devices.
  - *Not Selected*. Skylar One will not discover devices that don't respond to the SNMP credentials selected in the ***SNMP Credentials*** fields.

NOTE: You must either select a credential for the discovery session or select the ***Discover Non-SNMP*** option. Skylar One will prevent you from proceeding with discovery if you have not met those conditions.

- ***Model Devices***. Determines whether or not the devices that are discovered with this discovery session can be managed through Skylar One. Choices are:
  - *Selected*. When a device is modeled, Skylar One creates a device ID for the device; you can then access the device through the **Device Manager** page and manage the device in Skylar One.
  - *Not Selected*. If a device is not modeled, you cannot access the device through the **Device Manager** page, and you cannot manage the device in Skylar One. However, each discovered device will still appear in the Discovery Session logs. For each discovered device, the discovery logs will display the IP address and device class for the device. This option is useful when performing an initial discovery of your network, to determine which devices you want to monitor and manage with Skylar One. For the amount of time specified in the ***Device Model Cache TTL (h)*** field, a user can manually model the device from the **Discovery Session** window.
- ***Enable DHCP***. Specifies whether or not the specified range of IPs and hostnames use DHCP.
  - *Selected*. Skylar One will perform a DNS lookup for the device during discovery and each time Skylar One retrieves information from the device.
  - *Not Selected*. Skylar One will perform normal discovery.
- ***Device Model Cache TTL (h)***. Amount of time, in hours, that Skylar One stores information about devices that are discovered but not modeled, either because the ***Model Devices*** option is not enabled or because Skylar One cannot determine whether a duplicate device already exists. The cached data can be used to manually model the device from the **Discovery Session** window.
- ***Log All***. Specifies whether or not the discovery session should use verbose logging. When you select verbose logging, Skylar One logs details about each IP address or hostname specified in the ***IP Address/Hostname Discovery List*** field, even if the results are "No device found at this address."
  - *Selected*. This discovery session will use verbose logging.
  - *Not Selected*. This discovery session will not use verbose logging.
- ***Select Device Template***. As Skylar One discovers a device in the IP discovery list, that device is configured with the selected device template. You can select from a list of all device templates in Skylar One. For more information on device templates, see the manual on ***Device Groups and Device Templates***.

9. Click **[Save and Close]** to save the discovery session. The **Discovery Sessions** page (Devices > Discovery Sessions) displays the new discovery session.

10. If you selected the **Run after save** option on this page, the discovery session runs, and the **Discovery Logs** page displays any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page includes a link to the **Device Investigator** page for the discovered device.

Discovering Fortinet: Fortigate Devices in the Classic User Interface

To perform a discovery session for one IP address, multiple IP addresses, or a range of IP addresses on the **Classic Discovery** page:

> **NOTE:** To discover all the devices in your network, you must first know the range of IP addresses used in your network. If you need help, ask your network administrator.

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
2. In the **Discovery Control Panel**, click **[Create]**. The **Discovery Session Editor** page appears:
3. Supply values in the following fields:
    - ***Name***. Type a name for the discovery session. This name is displayed in the list of discovery sessions in the **Discovery Control Panel** page.
    - ***Description***. Optionally, type a description of the discovery session.
    - ***IP Address/Hostname Discovery List***. Provide a list of IP addresses or fully-qualified domain names for Skylar One to scan during discovery. In this field, you can enter a combination of one or more of the following:

> **NOTE:** Instead of manually entering a list of IP addresses and hostnames, you can upload a file that contains the list of IP addresses and hostnames. See the description of the ***Upload File*** field.

        - One or more *single IPv4 addresses* separated by commas. Each IP address must be in standard IP notation and cannot exceed 15 characters. For example, "10.20.30.1, 10.20.30.2, 10.20.30.3".
        - One or more *ranges of IPv4 addresses* with "-" (dash) characters between the beginning of the range and the end of the range. Separate each range with a comma. For example, "10.20.30.1 – 10.20.30.254".
        - One or more IP address ranges in *IPv4 CIDR notation*. Separate each item in the list with a comma. For example, "192.168.168.0/24".
        - One or more *ranges of IPv6 addresses* with "-" (dash) characters between the beginning of the range and the end of the range. Separate each range with a comma. For example, "2001:DB8:0:0:0:0:0:0-2001:DB8:0:0:0:0:0:0003".
        - One or more IP address ranges in *IPv6 CIDR notation*. Separate each item in the list with a comma. For example, "2001:DB8:0:0:0:0:0:0/117".

- One or more hostnames (fully-qualified domain names). Separate each item in the list with a comma.

CAUTION: If you enter both the hostname and IP address of the same devices, Skylar One will discover two duplicate devices.

NOTE: The following types of notation are **not supported**: IPv4 netmask with comma notation (e.g., 192.168.168.0,24); a list of single IPv6 addresses, separated by comma.

NOTE: Skylar One will display an error if your discovery session exceeds the maximum size for optimum performance. Skylar One will display a warning message if your discovery session includes 100 or more IP addresses. The warning message will tell you that discovery with more than 100 IP addresses might "take a long time to discover".

- ***Upload File***. Instead of manually entering a list of IP addresses and hostnames in the ***IP Address/Hostname Discovery List*** field, you can upload a file that contains a list of IP addresses and hostnames. The IP addresses and hostnames in the file must be in a format that is allowed for the ***IP Address/Hostname Discovery List*** field. Each address or range of addresses in the file must be separated by a newline character instead of a comma. You can browse to the file and then select it. After uploading the file, the ***IP Address/Hostname Discovery List*** field will display the IP addresses and hostnames from the file.
- ***SNMP Credentials***. A community string that allows Skylar One to access a device's SNMP data. SNMP credentials are defined in the **Credential Management** page (System > Manage > Credentials). If you want to retrieve SNMP data from one or more devices, you must select one or more working SNMP credentials in this field. You can select multiple credentials from this field. Skylar One will try each selected credential when discovering devices and retrieving device data.
- ***Other Credentials***. A username and password pair (among other fields) that allows Skylar One to access a device's database data, SOAP data, XML data, WMI data, WBEM data, or data that is monitored with a Snippet Dynamic Application. These credentials are defined in the **Credential Management** page (System > Manage > Credentials). You can select multiple credentials from this field. Skylar One will try each selected credential when searching for Dynamic Applications to align with each discovered device.

NOTE: You can use the field at the top of the ***SNMP Credentials*** field and the ***Other Credentials*** field to filter the list of credentials. If you enter an alpha-numeric string in the field, the ***SNMP Credentials*** field or the ***Other Credentials*** field will include only credentials that match the string.

NOTE: Your organization membership(s) might affect the list of credentials you can see in the ***SNMP Credentials*** field and the ***Other Credentials*** field.

- ***Initial Scan Level***. For this discovery session only, specifies the data to be gathered during the initial discovery session. The options are:
    - *System Default (recommended)*. Use the value defined in the **Behavior Settings** page (System > Settings > Behavior).
    - *0. Model Device Only*. Discovery will discover if the device is up and running and if so, collect the make and model of the device. Skylar One will then generate a device ID for the device so it can be managed by Skylar One.
    - *1. Initial Population of Apps*. Discovery will search for Dynamic Applications to associate with the device. The discovery tool will attempt to collect data for the aligned Dynamic Applications. Discovery will later retrieve full sets of data from each Dynamic Application. Discovery will also perform *0. Model Device Only* discovery.
    - *2. Discover SSL Certificates*. Discovery will search for SSL certificates and retrieve SSL data. Discovery will also perform *1. Initial Population of Apps* and *0. Model Device Only*.
    - *3. Discover Open Ports*. Discovery will search for open ports. Discovery will also perform *2. Discover SSL Certificates*, *1. Initial Population of Apps*, and *0. Model Device Only*.

NOTE: If your system includes a firewall and you select *3. Discover Open Ports*, discovery might be blocked and/or might be taxing to your network.

    - *4. Advanced Port Discovery*. Discovery will search for open ports, using a faster TCP/IP connection method. Discovery will also perform *2. Discover SSL Certificates*, *1. Initial Population of Apps*, and *0. Model Device Only*.

NOTE: If your system includes a firewall and you select *4. Advanced Port Discovery*, some devices might remain in a pending state (purple icon) for some time after discovery. These devices will achieve a healthy status, but this might take several hours.

    - *5. Deep Discovery*. Discovery will use nmap to retrieve the operating system name and version. Discovery will also scan for services running on each open port and can use this information to match devices to device classes. Discovery will search for open ports, using a faster TCP/IP connection method. Discovery will also perform *2. Discover SSL Certificates, 1. Initial Population of Apps*, and *0. Model Device Only*.

NOTE: For devices that don't support SNMP, option *5. Deep Discovery* allows you to discover devices that don't support SNMP and then align those devices with a device class other than "pingable". Note that option *5. Deep Discovery* is compute-intensive.

NOTE: If Skylar One cannot determine the appropriate Device Class, it will assign the device to the Generic SNMP Device Class.

- ***Scan Throttle***. Specifies the amount of time a discovery process should pause between each specified IP address (specified in the ***IP Address/Hostname Discovery List*** field). Pausing discovery processes between IP addresses spreads the amount of network traffic generated by discovery over a longer period of time. The choices are:
    - *System Default (recommended)*. Use the value defined in the **Behavior Settings** page (System > Settings > Behavior).
    - *Disabled*. Discovery processes will not pause.
    - *1000 Msec to 10000 Msec*. A discovery process will pause for a random amount of time between half the selected value and the selected value.
- ***Port Scan All IPs***. For the initial discovery session only, specifies whether Skylar One should scan all IP addresses on a device for open ports. The choices are:
    - *System Default (recommended)*. Use the value defined in the **Behavior Settings** page (System > Settings > Behavior).
    - *0. Disabled*. Skylar One will scan only the primary IP address (the one used to communicate with Skylar One) for open ports.
    - *1. Enabled*. Skylar One will scan all discovered IP addresses for open ports.
- ***Port Scan Timeout***. For the initial discovery session only, specifies the length of time, in milliseconds, after which Skylar One should stop trying to scan an IP address for open ports and begin scanning the next IP address (if applicable). Choices are:
    - *System Default (recommended)*. Use the value defined in the **Behavior Settings** page (System > Settings > Behavior).
    - Choices between 60,000 to 1,800,000 milliseconds.
- ***Detection Method & Port***. During discovery, Skylar One will scan the list of ports selected in this field to determine if the range of devices is up and running and which ports are open on each discovered device. If a device does not respond to SNMP or ICMP, Skylar One uses an open port to collect availability data for that device. If you are not sure which ports are used by the range of devices, select the entry *Default Method*. Skylar One will check ICMP (ping), FTP, SSH, Telnet, SMTP, and HTTP ports.

NOTE: You can use the field at the top of the ***Detection Method & Port*** field to filter the list of ports. If you enter an alpha-numeric string in the field, the ***Detection Method & Port*** field will include only ports that match the string.

- ***Interface Inventory Timeout (ms)***. Specifies the maximum amount of time that the discovery processes will spend polling a device for the list of interfaces. After the specified time, Skylar One will stop polling the device, will not model the device, and will continue with discovery. The default value is 600,000 ms (10 minutes).
    - During the execution of this discovery session, Skylar One uses the value in this field first. If you delete the default values and do not specify another value in this field, Skylar One uses the value in the **Global Threshold Settings** page (System > Settings > Thresholds).
    - If you specify a value in this field and do not apply a device template to this discovery session, the ***Interface Inventory Timeout*** setting in the **Device Thresholds** page (Devices > Classic Devices > wrench icon > Thresholds, or Registry > Devices > Device Manager > wrench icon > Thresholds in the classic user interface) is set to this value for each discovered device. If there is no device template applied to the discovery session and no value is supplied in this field, Skylar One uses the value in the **Global Threshold Settings** page (System > Settings > Thresholds).
- ***Maximum Allowed Interfaces***. Specifies the maximum number of interfaces per devices. If a device exceeds this number of interfaces, Skylar One will stop scanning the device, will not model the device, and will continue with discovery. The default value is 10,000.
    - During the execution of this discovery session, Skylar One uses the value in this field first. If you delete the default values and do not specify another value in this field, Skylar One uses the value in the **Global Threshold Settings** page.
    - If you specify a value in this field and do not apply a device template to this discovery session, the ***Maximum Allowed Interfaces*** setting in the **Device Thresholds** page is set to this value for each discovered device. If there is no device template applied to the discovery session and no value is supplied in this field, Skylar One uses the value in the **Global Threshold Settings** page.
- ***Bypass Interface Inventory***. Specifies whether or not the discovery session should discover network interfaces.
    - *Selected*. Skylar One will not attempt to discover interfaces for each device in the discovery session. For each discovered device, the ***Bypass Interface Inventory*** checkbox in the **Device Properties** page will be selected.
    - *Not Selected*. Skylar One will attempt to discover network interfaces, using the ***Interface Inventory Timeout*** value and ***Maximum Allowed Interfaces*** value.

NOTE: If a device has already been discovered and then is rediscovered through the **Discovery Session Editor** page, the ***Bypass Interface Inventory.*** checkbox in the **Device Properties** page will retain its previous value, regardless of what is selected in the **Discovery Session Editor** page.

- ***Discover Non-SNMP Devices***. Specifies whether or not Skylar One should discover devices that don't respond to SNMP requests.
    - *Selected*. Skylar One will discover devices that don't respond to the SNMP credentials selected in the ***SNMP Credentials*** field. These devices will be discovered as "pingable" devices.
    - *Not Selected*. Skylar One will not discover devices that don't respond to the SNMP credentials selected in the ***SNMP Credentials*** fields.
- ***Model Devices***. Determines whether or not the devices that are discovered with this discovery session can be managed through Skylar One. Choices are:
    - *Enabled*. When a device is modeled, Skylar One creates a device ID for the device; you can then access the device through the **Device Manager** page and manage the device in Skylar One.
    - *Disabled*. If a device is not modeled, you cannot access the device through the **Device Manager** page, and you cannot manage the device in Skylar One. However, each discovered device will still appear in the Discovery Session logs. For each discovered device, the discovery logs will display the IP address and device class for the device. This option is useful when performing an initial discovery of your network, to determine which devices you want to monitor and manage with Skylar One. For the amount of time specified in the ***Device Model Cache TTL (h)*** field, a user can manually model the device from the **Discovery Session** window.
- ***DHCP***. Specifies whether or not the specified range of IPs and hostnames use DHCP.
    - *Selected*. Skylar One will perform a DNS lookup for the device during discovery and each time Skylar One retrieves information from the device.
    - *Not Selected*. Skylar One will perform normal discovery.
- ***Device Model Cache TTL (h)***. Amount of time, in hours, that Skylar One stores information about devices that are discovered but not modeled, either because the ***Model Devices*** option is not enabled or because Skylar One cannot determine whether a duplicate device already exists. The cached data can be used to manually model the device from the **Discovery Session** window.
- ***Collection Server PID***. This field contains a list of all Data Collectors on the network. Select the Data Collector that is local or closet to the devices to be discovered.
    - For Skylar One appliances, only the name of the appliance will appear in this field.

NOTE: After initial discovery, each device will use the collector group that contains this Data Collector for collection and rediscovery.

- ***Organization***. This field contains a list of all organizations defined in Skylar One. Devices discovered during the discovery session will be assigned to the selected organization.

NOTE: Make sure you have the desired organization created and selected before running the discovery process. This field assigns all devices and networks in the specified IP range to a single organization. However, you can later assign individual devices and networks to different organizations.

- ***Add Devices to Device Group(s)***. When Skylar One discovers a device in the IP discovery list, that device is added to each selected device group. You can select one or more device groups from a list of device groups in Skylar One that have "Discovery" selected in the ***Visibility*** field. For more information on device groups, see the manual on ***Device Groups and Device Templates***.

NOTE: You can use the field at the top of the ***Add Devices to Device Group(s)*** field to filter the list of device groups. If you enter an alpha-numeric string in the field, the ***Add Devices to Device Group(s)*** field will include only device groups that match the string.

- ***Apply Device Template***. As Skylar One discovers a device in the IP discovery list, that device is configured with the selected device template. You can select from a list of all device templates in Skylar One. For more information on device templates, see the manual on ***Device Groups and Device Templates***.
- ***Log All***. Specifies whether or not the discovery session should use verbose logging. When you select verbose logging, Skylar One logs details about each IP address or hostname specified in the ***IP Address/Hostname Discovery List*** field, even if the results are "No device found at this address."
    - *Selected*. This discovery session will use verbose logging.
    - *Not Selected*. This discovery session will not use verbose logging.

4. Click the **[Save]** button **to save the discovery session**. Close the **Discovery Session Editor** page.
5. In the **Discovery Control Panel** page, click the **[Reset]** button. The new discovery session will appear in the **Session Register** pane.
6. To launch the new discovery session, click its ***Queue this Session*** icon ( ).
7. If no other discovery sessions are currently running, the session will be executed immediately. If another discovery session is currently running, your discovery session will be queued for execution.

Viewing Fortinet: Fortigate Component Devices

In addition to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface), you can view the Fortinet: Fortigate system and all associated component devices in the following places in the user interface:

- The **Device View** modal page (click the bar-graph icon [] for a device, then click the **Topology** tab) displays a map of a particular device and all of the devices with which it has parent-child relationships. Double-clicking any of the devices listed reloads the page to make the selected device the primary device.
- The **Device Components** page (Devices > Device Components) displays a list of all root devices and component devices discovered by Skylar One in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with an Fortinet: Fortigate system, find the Fortinet: Fortigate device and click its plus icon (**+**).
- The **Component Map** page (Classic Maps > Device Maps > Components) allows you to view devices by root node and view the relationships between root nodes, parent components, and child components in a map. This makes it easy to visualize and manage root nodes and their components. Skylar One automatically updates the **Component Map** as new component devices are discovered. The platform also updates each map with the latest status and event information. To view the map for a Fortinet: Fortigate system, go to the **Component Map** page and select the map from the list in the left NavBar. To learn more about the **Component Map** page, see the ***Views*** manual.

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

International: +1-703-354-1010