Monitoring Cisco Email Security Appliance (ESA)

Cisco: ESA PowerPack Beta version 100

Table of Contents

Introduction 3

What is Cisco ESA? 3

What Does the Cisco: ESA PowerPack Monitor? 4

Installing the Cisco: ESA PowerPack 4

Configuration and Discovery 6

Prerequisites for Monitoring Cisco Email Security Appliances 6

Creating an SNMP Credential for Cisco ESA 6

Discovering a Cisco Email Security Appliance 8

Discovering a Cisco Email Security Appliance in the SL1 Classic User Interface 10

Dashboards 11

Device Dashboards 11

Cisco ESA Virtual 11

Chapter 1

Introduction

Overview

This manual describes how to monitor Cisco Email Security Appliances (ESA) in SL1 using the *Cisco: ESA* PowerPack.

The following sections provide an overview of Cisco ESA and the *Cisco: ESA* PowerPack:

This chapter covers the following topics:

What is Cisco ESA? 3

What Does the Cisco: ESA PowerPack Monitor? 4

Installing the Cisco: ESA PowerPack 4

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 Cisco ESA?

Cisco Email Security Appliance (ESA) is a virtual, all-in-one appliance that provides protection against spam, malware, viruses, and other inbound and outbound email threats and annoyances.

What Does the Cisco: ESA PowerPack Monitor?

To monitor Cisco Email Security Appliances devices using SL1, you must install the *Cisco: ESA* PowerPack. This PowerPack enables you to discover and collect data about Cisco Email Security Appliances.

The *Cisco: ESA* PowerPack includes:

- Dynamic Applications to discover and monitor performance and configuration data for Cisco ESA devices
- Device Classes for each of the Cisco ESA devices that SL1 monitors
- Event Policies that are triggered when Cisco ESA devices meet certain status criteria
- A device dashboard that displays performance data about Cisco ESA devices

Installing the Cisco: ESA PowerPack

Before completing the steps in this manual, you must import and install the latest version of the *Cisco: ESA* 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 ***System Administration*** manual.)

IMPORTANT: The minimum required MySQL version is 5.6.0.

To download and install the PowerPack:

1. Search for and download the PowerPack from the **PowerPacks** page (Product Downloads > PowerPacks & SyncPacks) at the ScienceLogic Support Site.
2. In SL1, 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 Cisco Email Security Appliances for monitoring by SL1 using the *Cisco: ESA* PowerPack:

This chapter covers the following topics:

Prerequisites for Monitoring Cisco Email Security Appliances 6

Creating an SNMP Credential for Cisco ESA 6

Discovering a Cisco Email Security Appliance 8

Prerequisites for Monitoring Cisco Email Security Appliances

To configure SL1 to monitor Cisco Email Security Appliances using the *Cisco: ESA* PowerPack, you must first have the following information about the appliance that you want to monitor:

- The appliance's IP address.
- The appliance's SNMP community string.

Creating an SNMP Credential for Cisco ESA

To configure SL1 to monitor Cisco Email Security Appliances, you must create an SNMP credential. This credential allows the Dynamic Applications in the *Cisco: ESA* PowerPack to connect with the Cisco ESA and collect data from it.

To create an SNMP credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).

2. Click the **[Actions]** button, and then select *Create SNMP Credential*. The **Create New SNMP Credential** modal 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*. This field is required.
    - ***Port***. The port SL1 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 SL1 will stop trying to communicate with the SNMP device. The default value is *1500*. This field is required.
    - ***Retries***. Number of times SL1 will try to authenticate and communicate with the external device. The default value is *1*. This field is required.

    SNMP V1/V2 Settings

    These fields appear if you selected *SNMP V1* or *SNMP V2* in the ***SNMP Version*** field. Otherwise, these fields are grayed out.

    - ***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. Otherwise, these fields are grayed out.

    - ***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. Choices are MD5 or SHA. The default value is *MD5*. This field is required.
    - ***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*.

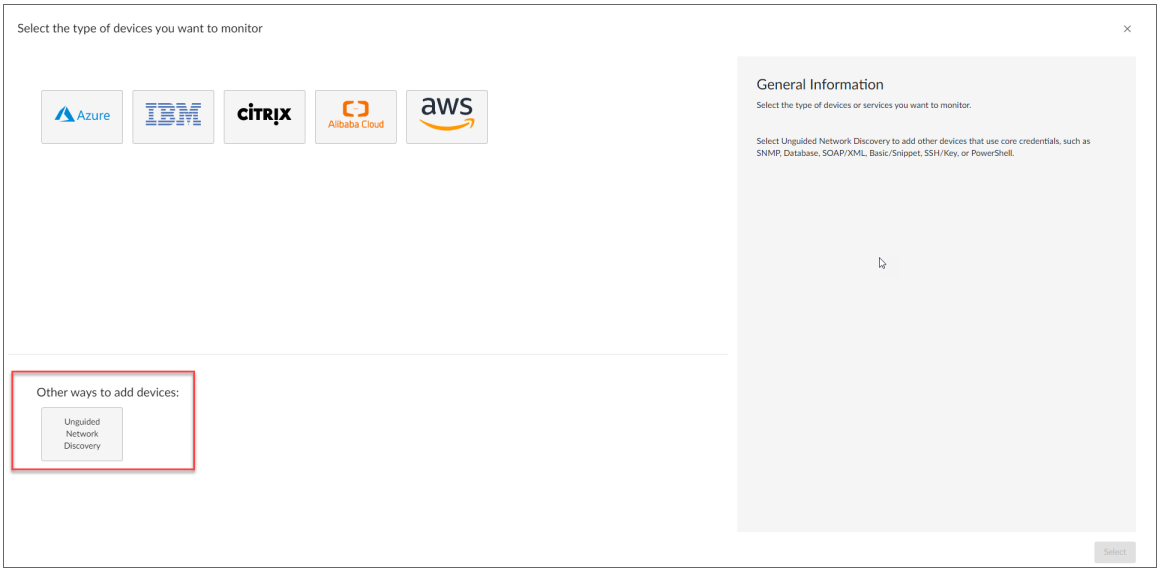
- ***SNMP v3 Engine ID***. The unique engine ID for the SNMP agent you want to communicate with. (SNMPv3 authentication and encryption keys are generated based on the associated passwords and the engine ID.) This field is optional.
- ***Context Name***. A context is a mechanism within SNMPv3 (and AgentX) 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. Choices are *DES* or *AES*. The default value is *DES*. This field is required.
- ***Privacy Protocol Passphrase***. Privacy password for the credential. This field is optional.

4. Click **[Save]**.

Discovering a Cisco Email Security Appliance

To discover the Cisco ESA that you want to monitor:

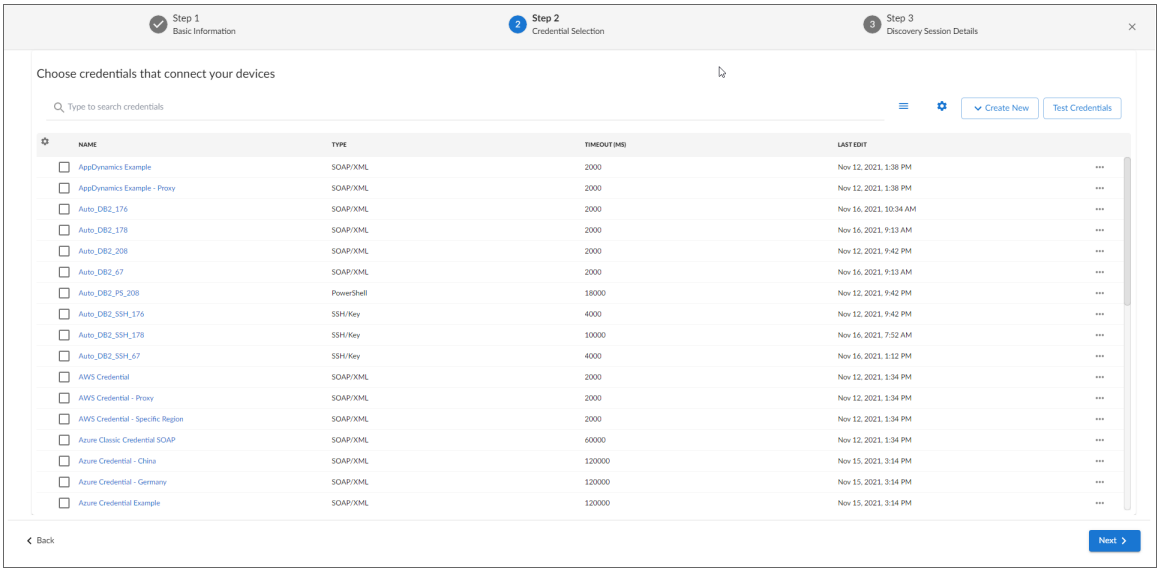
1. On the **Devices** page ( ) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears:



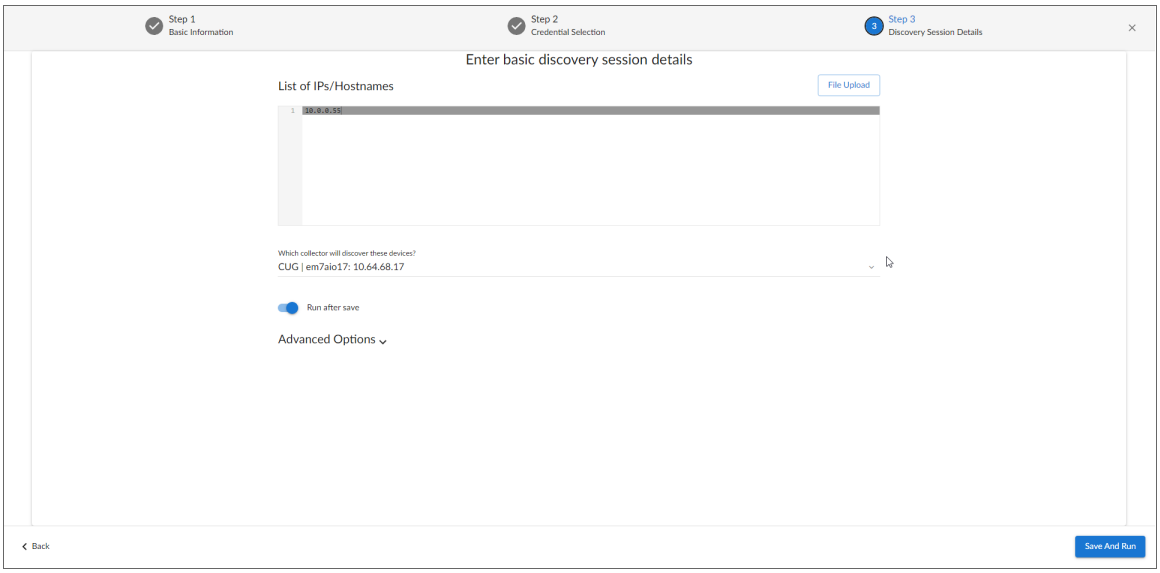
2. Click the **[Unguided Network Discovery]** button. Additional information about the requirements for discovery appears in the **General Information** pane to the right.
3. Click **[Select]**. The **Add Devices** page appears.
4. Complete the following fields:
    - ***Name***. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the **[Discovery Sessions]** tab.
    - ***Description***. Optional. 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.

- ***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 **Credentials** page of the **Add Devices** wizard appears:



6. On the **Credentials** page, select the SNMP credential you created for ESA.
7. Click **[Next]**. The **Discovery Session Details** page of the **Add Devices** wizard appears:



8. Complete the following fields:
   - ***List of IPs/Hostnames***. Type the IP address for the ESA device that you want to monitor.
   - ***Which collector will monitor these devices?***. Required. Select an existing collector to monitor the discovered devices.
   - ***Run after save***. Select this option to run this discovery session as soon as you save the session.

In the **Advanced options** section, click the down arrow icon ( ) to complete the following fields:

- ***Model Devices***. Enable this setting.

9. Click **[Save and Run]** if you enabled the Run after save setting, or **[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 a Cisco Email Security Appliance in the SL1 Classic User Interface

To discover the Cisco ESA that you want to monitor:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
2. Click the **[Create]** button. The **Discovery Session Editor** page appears.
3. On the **Discovery Session Editor** page, define values in the following fields:
   - ***Name***. Type a name for the discovery session.
   - ***IP Address/Hostname Discovery List***. Type the IP address for the ESA device that you want to monitor.
   - ***SNMP Credentials***. Select the SNMP credential you created for ESA.
   - ***Model Devices***. Select this checkbox.
4. Optionally, you can enter values in the other fields on this page. For more information about the other fields on this page, see the ***Discovery & Credentials*** manual.
5. Click **[Save]**, and then close the **Discovery Session Editor** window.
6. The discovery session you created appears at the top of the **Discovery Control Panel** page. Click its lightning-bolt icon ( ) to run the discovery session.
7. When the ESA is discovered, click its device icon ( ) to view its **Device Properties** page.

Chapter 3

Dashboards

Overview

The following sections describe the device dashboard that is included in the *Cisco: ESA* PowerPack:

This chapter covers the following topics:

Device Dashboards *11*

Device Dashboards

The *Cisco: ESA* PowerPack includes a device dashboard that provides summary information for Cisco Email Security Appliances. This device dashboard is aligned as the default device dashboard for the Cisco ESA devices.

Cisco ESA Virtual

The ***Cisco ESA Virtual*** device dashboard displays the following information:

- The basic information about the device
- Four instances of the Multi-series Performance Widget that display the following metrics trended over a specified period of time:
    - Memory, CPU, and Disk Input/Out Utilization
    - Open File Sockets
    - Top File System Utilization
    - Top Interfaces by Utilization

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com. For more information, see https://sciencelogic.com/company/legal.

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

International: +1-703-354-1010