Setting Up the User Interface

- (Optional) Requirements and Limitations for Dual-Stack Mode (IPv6 Support), on page 1
- Set Up the User Interface, on page 2

(Optional) Requirements and Limitations for Dual-Stack Mode (IPv6 Support)

Secure Workload clusters running on physical hardware can be configured to use IPv6 in addition to IPv4 for certain communications to and from the cluster.

Note You can use the Dual-Stack Mode (IPv6 support) feature when installing or upgrading to 3.6.1.5 and 3.7.1.5 releases, however, the feature is not available when you are installing or upgrading to patch releases.

Limitations

If you are considering enabling dual stack mode, note the following:

- You can enable IPv6 connectivity only during initial deployment or upgrade to a major release (you cannot enable this feature during patch upgrades.)
- Dual-stack mode is supported only on physical hardware/bare-metal clusters.
- There is no support for an IPv6-only mode.
- You cannot revert to IPv4-only mode after dual stack mode is enabled for the cluster.
- Data Backup and Restore (DBR) is not supported if dual-stack connectivity is enabled.
- Do not enable dual-stack mode for clusters configured with Federation.
- The following features always and only use IPv4 (note that IPv4 is always enabled even if IPv6 is enabled):
  - (Applicable for release 3.7.1.5 and 3.6.x) Enforcement on AIX agents
  - (Applicable for release 3.6.x) Hardware agent communication with the cluster
  - (Applicable for release 3.6.x) Connectors for flow ingestion, inventory enrichment, or alert notifications

Requirements

- You must configure both A and AAAA DNS records for FQDN. You must configure this before you enable dual stack mode for your cluster.
- External services such as NTP, SMTP, and DNS should be available over both IPv4 and IPv6, for redundancy purposes.
- In order to configure dual stack mode for a cluster:
  - The two cluster leaf switches will each need to be allocated routable IPv6 addresses on two different networks, for redundancy, and default gateways will need to be provided for each network.
  - For 39RU clusters, a site routable IPv6 network with space for at least 29 host addresses is required.
  - For 8RU clusters, a site routable IPv6 network with space for at least 20 host addresses is required.
  - The first three host addresses of the site routable IPv6 network are reserved for the Cisco Secure Workload cluster HSRP configuration and must not be used by any other devices.

Additional Information

Agents communicate with the cluster using IPv4 unless you configure them to use IPv6. For instructions, see the User Guide available from the Secure Workload portal.

Set Up the User Interface

Before you begin

- To complete this configuration, you need a device such as a laptop computer with an Ethernet port and access to the internet.
- You need an Ethernet cable to connect the device to the highest server in the Tetration (Secure Workload) cluster.
- Google Chrome is the only supported browser for the Setup portal, which is required for part of this process.
- (Optional) Beginning with version 3.6 and later, you can configure your cluster in dual-stack mode, which allows both IPv4 and IPv6 to be used for communication between certain Secure Workload components and between Secure Workload and network services such as NTP and DNS. (Secure Workload already handles IPv6 traffic, whether or not you enable dual-stack mode.) You can enable this support only during deploy or upgrade.

  If you are considering enabling support for IPv6, see (Optional) Requirements and Limitations for Dual-Stack Mode (IPv6 Support), on page 1.

Important Enter IPv4 addresses in all fields in the procedure below unless the field name explicitly states IPv6.

Procedure

Step 1 Configure the internet device with an IP address of 2.2.2.1/30 (255.255.255.252).

Step 2 Use an Ethernet cable to connect the Ethernet port on the internet device to the ETH1 port on the highest server in the top of the Tetration (Secure Workload) cluster.

Step 3 On the internet device, open the Chrome browser and go to http://2.2.2.2:9000.

Note The Chrome browser is the only browser tested with this process.

The Tetration (Secure Workload) Setup Diagnostics page opens.

Step 4 If there are errors in the Diagnostics page, check the cabling connections between cluster devices for broken connections or cables routed incorrectly (use the cabling tables in the appendix to verify all cabling) before continuing with this procedure. When done, return to Step 2.

Step 5 Click **Continue**.

The RPM Upload page opens.

Note If the Site Config page opens instead, enter the following URL to open the RPM Upload page:

http://2.2.2.2:9000 /upload

Step 6 Upload RPM objects to the Tetration (Secure Workload) cloud as follows:

a. Click **Choose File**.

b. Browse to find the adhoc and mother files.

c. Click **Upload**.

The Site Config page opens.

Step 7 Use the Site Config page to set up the new site as follows:

- **General** form
  a. In the **Site Name** field, enter the unique cluster name.
  b. In the **SSH Public Key** field, paste in the authentication key.
  Note Generate your own SSH key pair, which can be used for cluster SSH access.
  c. Click **Next**.
- **Email** form
  a. Fill in the required email addresses.
  b. Click **Next**.
- **L3** form

  Enter each of the requested addresses. All fields with * are required fields. Enter all addresses as IPv4 unless the field name specifies IPv6.

(Optional) If you are installing software version 3.6 or later: To enable dual-stack mode (support for both IPv4 and IPv6):

a. Check the IPv6 checkbox.

b. Enter the IPv6 address in CIDR notation for both Leaf 1 and Leaf 2 switches.

c. Enter the Leaf 1 and Leaf 2 IPv6 Default Gateway.

d. Click **Next**.

- **Network** form

  Enter all addresses as IPv4 unless the field name specifies IPv6.

  a. In the **Internal network IP address** field, paste in the address from the orchestrator deployment output.

  b. In the **External network IP address** field, paste in the address from the orchestrator deployment output.

  c. In the **External gateway IP address** field, paste in the address from the orchestrator deployment output.

  d. In the **DNS resolver IP address** field, paste in the address from the orchestrator deployment output.

  e. In the **DNS domain** field, enter your DNS domain (for example, "cisco.com").

  f. (Software version 3.6 or later) If you enabled IPv6 on the L3 page, **IPv6** is automatically selected.

  If IPv6 is selected, you must specify IPv6 addresses reserved for Secure Workload use:

  - Enter the **External IPv6 Network**.

    The first 3 IPv6 addresses in the IPv6 External Network field are always reserved for the switches of the Secure Workload cluster and should not be used for any other purpose.

  - If you want to use IPv6 only for certain addresses, enter those addresses in the **External IPv6 IPs** field.

  Note
  - For a 39 RU cluster, ensure that at least 29 IPv6 addresses are available in the IPv6 External Network or the External IPv6 IPs list.
  - For an 8 RU cluster, ensure that at least 20 IPv6 addresses are available in the IPv6 External Network or the External IPv6 IPs list.

  g. Click **Next**.

- **Service** form

  a. In the **NTP Servers** field, enter the space-separated list of NTP server names or IP addresses from the Orchestrator deployment output.

  b. In the **SMTP Server** field, enter the name or IP address of an SMTP server that can be used by Tetration (Secure Workload) for sending email messages (this server must be accessible by Tetration (Secure Workload)).

c. In the **SMTP Port** field, enter the port number of the SMTP server. AWS restricts the use of ports 25 and 465. You must configure your account correctly or use port 587.

d. (Optional) In the **SMTP Username** field, enter the user name for SMTP authentication.

e. (Optional) In the **SMTP Password** field, enter the password for SMTP authentication.

f. (Optional) In the **HTTP Proxy Server** field, enter the name or IP address of an HTTP proxy server that will be used by Tetration (Secure Workload) to access external services on the internet.

g. (Optional) In the **HTTP Proxy Port** field, enter the port number for the HTTP proxy server.

h. (Optional) In the **HTTPs Proxy Server** field, enter the name or IP address of an HTTPs proxy server that will be used by Tetration (Secure Workload) to access external services on the internet.

i. (Optional) In the **HTTPs Proxy Port** field, enter the port number for the HTTPs proxy server.

j. (Optional) In the **Syslog Server** field, enter the name or IP address of an syslog server that can be used by Tetration (Secure Workload) to send alerts.

k. (Optional) In the **Syslog Port** field, enter the port number of the syslog server.

l. (Optional) In the **Syslog Severity** field, enter severity level for the syslog messages. The possible values include informational, notice, warning, error, critical, alert, and emergency.

m. Click **Next**.

- **UI** form

  a. In the **UI VRRP VRID** field, enter "77" unless you need a unique VRID.

  b. In the **UI FQDN** field, enter the fully qualified domain name where you will access the cluster.

  c. In the **UI Airbrake Key** field, leave blank.

  d. Click **Next**.

     Tetration (Secure Workload) validates your configuration settings and displays the status for the settings.

- **Advanced** form

  a. In the **External IPs** field, enter IPv4 addresses.

  b. Click **Continue**.

Step 8 If there are any failures, click **Back** and edit the configuration (see Step 7).

Note You cannot modify these settings in the setup GUI after leaving this page. However, you can modify the settings later from the company page in the GUI.

Step 9 If there are no failures noted for your configuration and you do not need to make any changes, click **Continue**.

Tetration (Secure Workload) is configured according to the settings that you specified. This process can take one to two hours without any interaction on your part.

What to do next

If you deployed software version 3.6 or later and you enabled IPv6 connectivity:

- You can access the Cisco Secure Workload web portal using either IPv4 or IPv6.
- By default, software agents communicate with the Secure Workload cluster using IPv4 even if the cluster is enabled to support IPv6. If you want supported agents to use IPv6 for this purpose, you must configure the **Sensor VIP FQDN** field on the **Platform > Cluster Configuration** page in the Secure Workload web portal. For important instructions, see the user guide, available as online help from the Secure Workload web portal or from https://www.cisco.com/c/en/us/support/security/tetration/products-installation-and-configuration-guides-list.html.