Remote Troubleshooter Application

This guide provides the following topics:

Prerequisites

Before using the Remote Troubleshooter application, perform the following tasks:

- Review the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide* for assistance in resolving any issues you may encounter with the Cisco APIC-EM controller.
- Contact Cisco support and work with a Cisco support engineer to resolve your issue and/or have a Cisco Technical Assistance Center (TAC) case open.
- Ensure that you have internet connectivity with at least one of the following ports enabled for outgoing SSH connections for the Remote Troubleshooter application: 22, 25, 53, 80, 443, or 4766.

Remote Troubleshooter Overview

Cisco APIC-EM supports the Remote Troubleshooter application. This application creates a technical support tunnel that enables a Cisco support engineer to connect to a Cisco APIC-EM cluster and troubleshoot issues. The application uses outbound SSH to create a secure connection with the cluster through this support tunnel.

As an administrator, you can use the Remote Troubleshooter application to control when a Cisco support engineer has access to a particular cluster and for how long (since a Cisco support engineer cannot establish a secure support tunnel on their own). The application will indicate whenever a Cisco support engineer establishes a remote access session, and you can end a session at any time by disabling the support tunnel they are using.

By default, the support tunnel remains open for 24 hours, but you can extend its duration beyond 24 hours (if necessary). However, we recommend for security reasons that you or the Cisco support engineer close the support tunnel as soon as all of the troubleshooting work is complete.

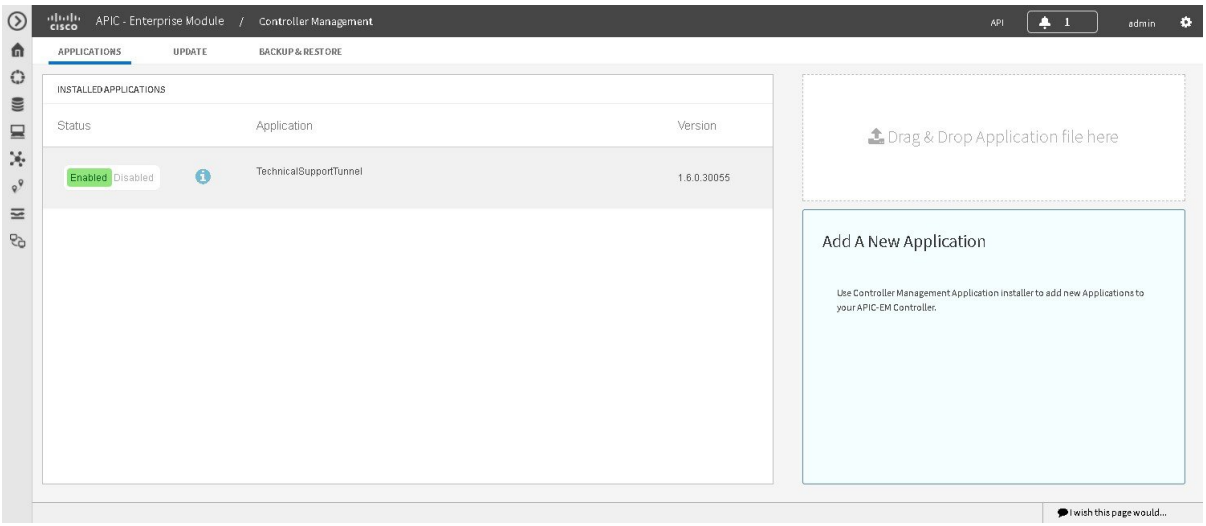
Configuring Remote Troubleshooter

The following procedure describes how to enable and configure the Remote Troubleshooter application. Once the application is enabled and configured, you can then use it to manage access to a Cisco APIC-EM cluster for remote troubleshooting.

Step 1 From the global toolbar, click either **admin** or the **Settings** icon (gear) at the top right corner of the controller screen.

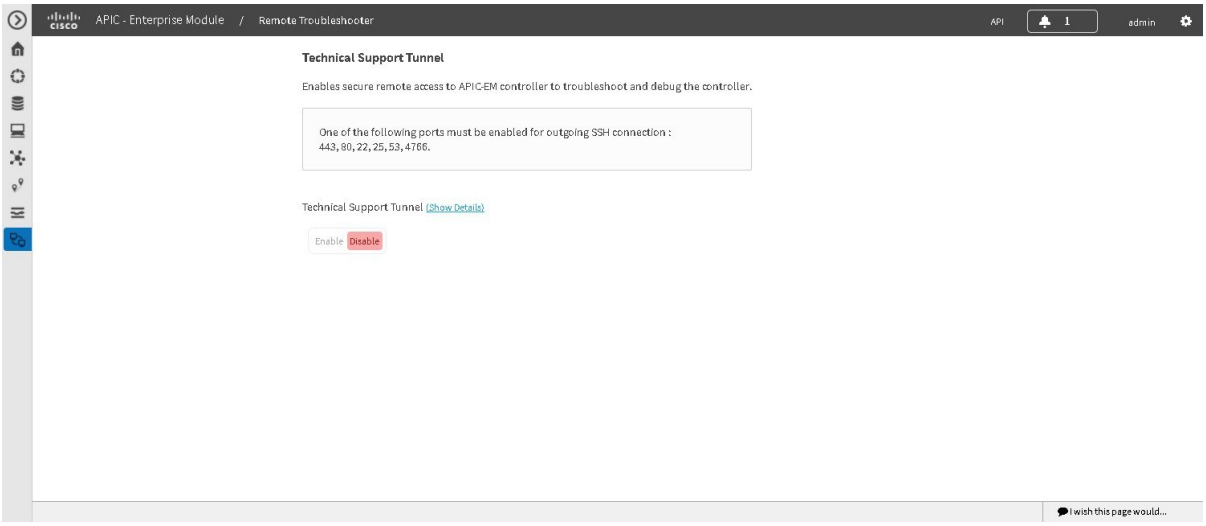
Step 2 Click the **App Management** link from the drop-down menu.
The **Controller Management** page opens with the **Applications** tab selected by default.

Step 3 In the **Installed Applications** table, locate the **Technical Support Tunnel** application icon and click **Enabled** from the **Status** column.
The Remote Troubleshooter application then becomes enabled and its icon displays in the navigation pane.

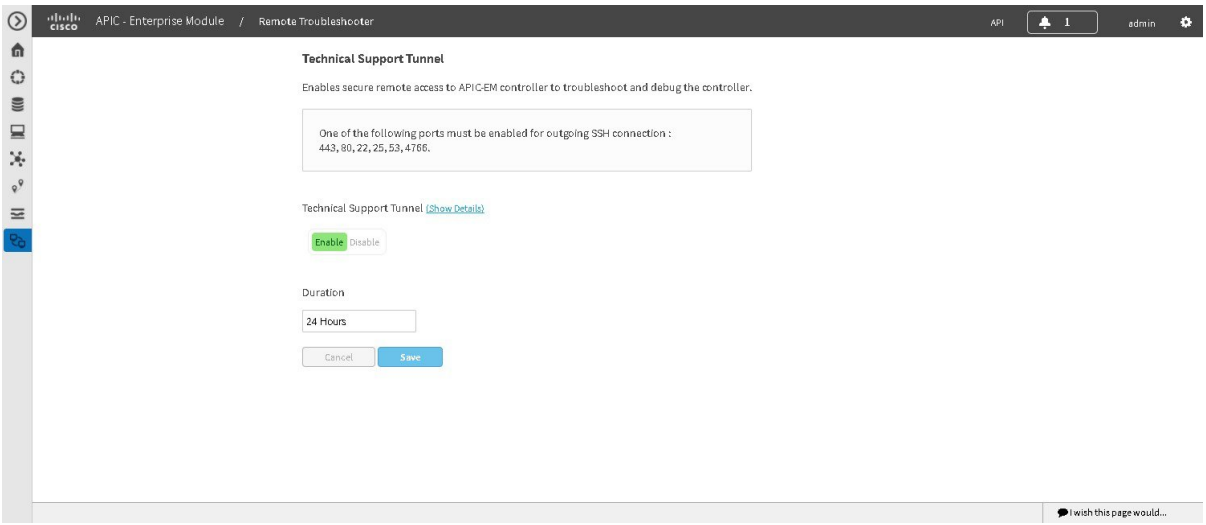


Proceed to create a support tunnel that a Cisco support engineer will use to securely access the Cisco APIC-EM cluster that needs to be evaluated.

Step 4 From the navigation pane, click the Remote Troubleshooter application.
The **Technical Support Tunnel** window appears.

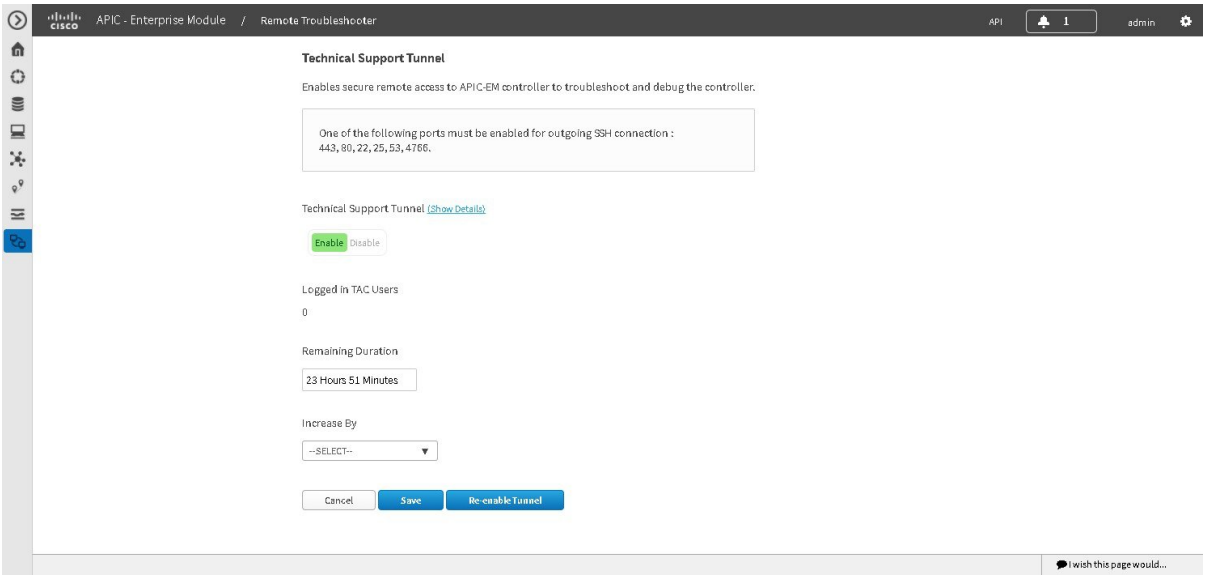


Step 5 Click **Enable** for the **Technical Support Tunnel** toggle.
The **Duration** field appears with `24 Hours` (the default value) set.



Step 6 Click **Save**.
The **Remote Troubleshooter** page updates, indicating one of the following:

- A secure support tunnel has been established.
- Authentication failed.
- The support tunnel server is currently unreachable.



Note If the authentication fails, then the Cisco APIC-EM will continue to attempt authentication every 5 minutes for the next 30 minutes. If authentication fails after those attempts, the support tunnel that you are trying to create is disabled automatically.

After a support tunnel has been successfully created, the **Remote Troubleshooter** page updates, indicating the number of support engineers that currently have remote access sessions open with the Cisco APIC-EM cluster in question and the time remaining until the support tunnel will be disabled.

Step 7 Click the **Show Details** link to open a dialog box that provides the following information for the support tunnel you just created:

Controller ID	The identification number of the controller that the support tunnel is connected with.
Password	The support tunnel's password.
SSH Key	This dialog box also lists the SSH key generated for the support tunnel. Cisco APIC-EM maintains a copy of every SSH key it has generated. If you reenable a particular support tunnel at a later point in time, you can reuse the SSH key that was generated for it previously, generate a new key, or reset the key by assigning it with a new value.

Note You will need to share this information (preferably via secure means) with the appropriate Cisco support engineer.

Step 8 (Optional) Extend the duration of a support tunnel session by choosing the desired value (in hours) from the **Increase By** drop-down list and then clicking **Save**.

Step 9 (Optional) To end a support tunnel session before the time allotted to it has expired, click the **Technical Support Tunnel** toggle (ensuring that **Disable** is selected) and then click **Save**.

When you disable the support tunnel session, any support engineers currently connected to the Cisco APIC-EM cluster will lose access.

What to Do Next

After a support tunnel has been successfully created and the Cisco support engineers have remote access to the Cisco APIC-EM cluster, proceed to work with them to resolve your troubleshooting issue.

Important Close the support tunnel session when finished working with the Cisco support engineers on your troubleshooting issue.