



Configuring Telemetry

- [Telemetry Collection, page 1](#)
- [Configuring the Proxy, page 3](#)

Telemetry Collection

The Cisco APIC-EM uses telemetry to collect information about the user experience with the controller. This information is collected for the following reasons:

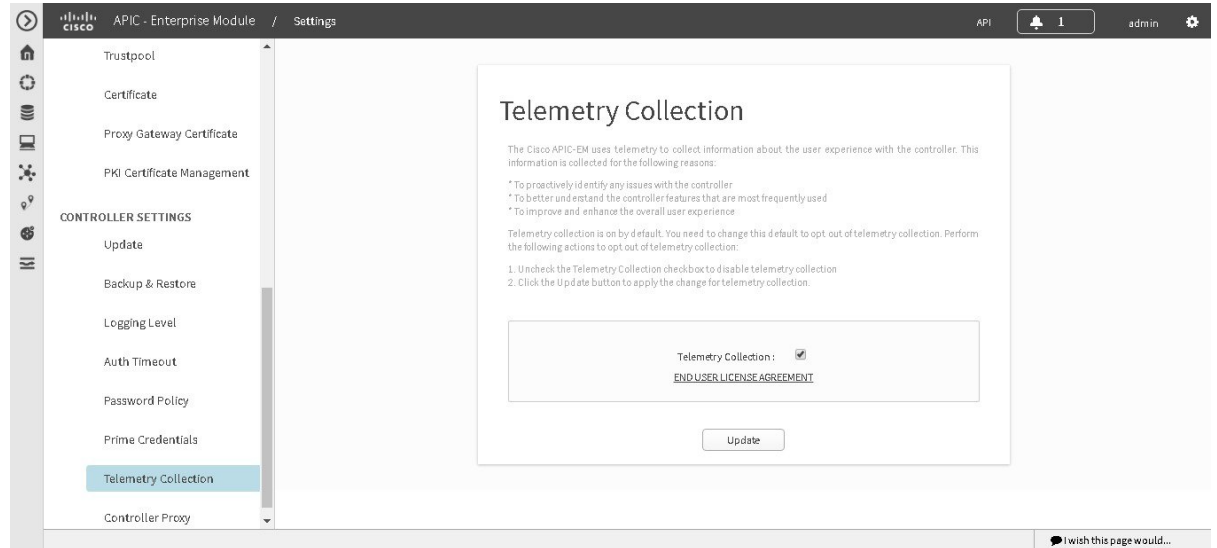
- To proactively identify any issues with the controller
- To better understand the controller features that are most frequently used
- To improve and enhance the overall user experience

You are able to view some of the collected telemetry data by viewing the logs using the Cisco APIC-EM GUI. For information about this method, see *Searching the Services Logs* in Chapter 6, *Configuring the Cisco APIC-EM Settings*.

Telemetry is enabled with a telemetry service that collects data from the many other controller services. The telemetry service supports Data Access Service (DAS). The telemetry service uploads data to the Cisco Clean Access Agent (CAA) infrastructure on the Cisco cloud using HTTPS.

Telemetry collection is on by default. If you wish to opt out of telemetry collection, then perform the steps in the following procedure.

Figure 1: Telemetry Collection Window



Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see "User Settings" in the chapter, "Configuring the Cisco APIC-EM Settings".

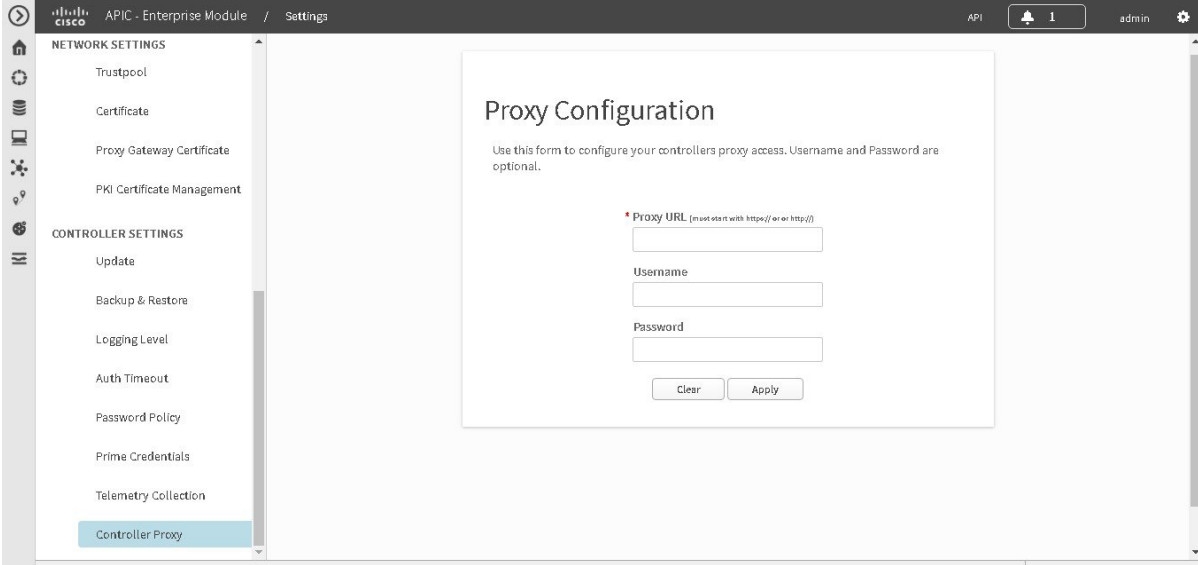
-
- Step 1** In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.
- Step 2** Click the **Settings** link from the drop-down menu.
- Step 3** In the **Settings** navigation pane, click **Telemetry Collection** to view the **Telemetry Collection** window. When accessing the **Telemetry Collection** window for the first time, the GUI displays a blue box with a check that indicates that telemetry collection is enabled.
- Step 4** (Optional) Click the **End User License Agreement** to review the agreement for telemetry collection.
- Step 5** (Optional) Uncheck the **Telemetry Collection** blue box to disable telemetry collection.
- Step 6** (Optional) Click the **Update** button to apply the change for telemetry collection.
-

Configuring the Proxy

If the Cisco APIC-EM is unable to communicate directly with the telemetry server in the Cisco cloud, then a message will appear in the controller GUI (for an admin user) requesting that you configure access to the proxy. This message will contain a direct link to the **Proxy Configuration** window where you can configure this access. To configure access, enter the appropriate settings for the proxy server that exists between the controller and the telemetry server.

You configure these settings using the **Proxy Configuration** window in the Cisco APIC-EM GUI.

Figure 2: Proxy Configuration Window



The screenshot shows the Cisco APIC-EM GUI. The top navigation bar includes the Cisco logo, 'APIC - Enterprise Module / Settings', and user information 'API 1 admin'. A left sidebar lists settings categories: NETWORK SETTINGS (Trustpool, Certificate, Proxy Gateway Certificate, PKI Certificate Management) and CONTROLLER SETTINGS (Update, Backup & Restore, Logging Level, Auth Timeout, Password Policy, Prime Credentials, Telemetry Collection, and Controller Proxy). The main content area is titled 'Proxy Configuration' and contains the following text: 'Use this form to configure your controllers proxy access. Username and Password are optional.' Below this text are three input fields: 'Proxy URL (must start with https:// or http://)', 'Username', and 'Password'. At the bottom of the form are 'Clear' and 'Apply' buttons. A feedback link 'I wish this page would...' is visible in the bottom right corner.

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see "User Settings" in the chapter, "Configuring the Cisco APIC-EM Settings".

-
- Step 1** In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.
 - Step 2** Click the **Settings** link from the drop-down menu.
 - Step 3** In the **Settings** navigation pane, click **Controller Proxy** to view the **Proxy Configuration** window.
 - Step 4** Enter the proxy server's URL address.
 - Step 5** (Optional) If the proxy server requires authentication, then enter the username for access to the proxy server.
 - Step 6** (Optional) If the proxy server requires authentication, then enter the password that is required for access to the proxy server.
 - Step 7** Click the **Apply** button to apply your proxy configuration settings to the controller.
-