Integrate Cisco Identity Services Engine

About Cisco ISE

The Cisco ISE Integration feature enables you to leverage the Cisco Identity Services Engine (ISE) for centralized authentication, authorization, and policy management in your Cisco SD-WAN Cloud environment. Gain greater visibility, control, and compliance while ensuring a secure and scalable network infrastructure.

Integrating Cisco ISE with Cisco SD-WAN Cloud allows for enhanced identity-based policies and visibility across your network fabric. This chapter provides step-by-step instructions for configuring the integration.

Note This feature is currently supported only on Early Adopter Cisco SD-WAN Cloud software releases.

Prerequisites for Cisco ISE integration

Before you begin the Cisco ISE integration, ensure you have these items and files ready:

- The reachable IP address of your Cisco ISE primary server node.
- A valid username and password with sufficient privileges on the Cisco ISE server.
- The VPN ID through which Cisco Catalyst SD-WAN Manager can communicate with the Cisco ISE server, typically VPN 0.
- The Root CA certificate files for the Cisco ISE Server and the pxGrid Server, in .cer format.

Configure Cisco ISE integration

Procedure

Step 1 Log in to your Cisco Catalyst SD-WAN Manager dashboard.

Step 2 On the navigation pane, select **Administration**.

Step 3 From the sub-menu, select **Integration Management**.

Step 4 In the main window, select the **Identity Services Engine** tab.

Step 5 Click **Add Connection**.

Step 6 In the **Add ISE Server** panel, complete these required fields:

- ISE Server IP Address - Enter the IP address of your Cisco ISE server.
- Username - Enter the administrative username for ISE.
- Password - Enter the corresponding password.
- VPN - Select the appropriate VPN from the drop-down menu to ensure the Manager can route traffic to the Cisco ISE server.

Step 7 Upload the trusted CA certificates to establish a secure connection:

a) Locate the **ISE Server CA** section.
b) Click **Choose a file** or drag and drop your Cisco ISE Server CA certificate file into the box.
c) Locate the **pxGrid Server CA** section.
d) Upload the pxGrid Server CA certificate file for pxGrid communication in the same manner.

Step 8 Review all entered information for accuracy and click **Submit**.

The system attempts to authenticate and establish a connection with the Cisco ISE server. Once successful, the server status should update to “Connected” or “Active” in the Integration Management list.

If you encounter any errors, check these conditions:

- Field Required Errors - Ensure all fields marked with a red asterisk (*) are filled.
- Certificate Errors - Ensure the certificates are in the correct .cer format and have not expired.
- Connectivity Issues - Verify that the selected VPN has a valid route to the Cisco ISE Server IP address and that firewall rules allow traffic on the necessary ports, such as HTTPS/443 and pxGrid ports.