Delinea

Cisco Enable Launching in Secret Server

The end goal in this process is to allow administrators to launch into Cisco IOS device consoles via SSH and have Secret Server populate the enable password into their session on their behalf, without them having to know the credential itself. The process requires two separate Secrets – one that stores the "connecting" user credentials (with privilege to connect to the target Cisco device) and one that stores the enable credential. Both Secrets will need to use differing templates, as their behavior in use ends up being slightly different.

This guide is designed to assist users in preparing their environment for using Cisco Enable account launching.

Contents

Stage 1 – Initial Template Configuration

1. Head to Admin -> Secret Templates. Select the **Cisco Account (SSH)** template and enter it.
2. Duplicate the **Cisco Account (SSH)** template (ID: 6010) and name the duplicate "Cisco Account (SSH) Enable Template" or an indicative name of your choosing.
3. Return to the **Cisco Account (SSH)** template**.** Under the Mapping tab select **Add Mapping**. Scroll to the bottom of the list and under **Extended Types** select **Username and Password**.
4. Map the username field to the username field and likewise for the password field.
5. Now head to the **Cisco Account (SSH) Enable Template** created in Step 2 and enter its configuration panel.
6. Under **Mapping -> Password Changing** click the **Edit** button and change the **Password Type to Use** to "Cisco Enable Secret Custom". Map the Machine Name field to the Host field and the Password field to the Password field. Click **Save.**
7. On the same page, under the Launchers panel, click the **Edit** button to the right of the PuTTY launcher. Scroll to the bottom and edit the **Connect As Commands**. Set the Connect As Command to "enable", the Connect As Command Response to "Password:$PASSWORD" and the Line Ending to "Carriage Return (/r). Click **Save**.
8. The template creation is now complete for both Secret types.

Stage 2 – Secret Onboarding – Connecting Account

The Connecting account onboard is straightforward. The Secret simply needs to be created, either via the UI or via the Secrets API endpoint (https://docs.delinea.com/ss/11.0.0/api-scripting/rest-api-powershell-examples/index.md#creating_a_secret) against the **Cisco Account (SSH)** template. The Secret Name, Host, Username and Password fields should be populated with the appropriate data for the intended host.

Stage 3 – Secret Onboarding – Enable Account

1. The enable account Secret should be created against the **Cisco Account (SSH) Enable Template** and its details – Secret Name, Host, Username and Password – should be filled out in accordance with the enable Secret. It is worth noting that the **Username** field must exist, however its contents will be ignored and hence it can be left blank.
2. Ensure that the **SSH Proxy** is set to **Yes** under the Security tab for the Secret. More details on configuring the SSH Proxy can be found here: https://docs.delinea.com/ss/11.0.0/networking/ssh-proxy-configuration/index.md
3. Under the **Remote Password Changing** tab, **Edit** the Associated Secrets. Click **Add Secret** and select the Secret that was created in Stage 2 – Secret Onboarding – Connecting Account. Once selected, click Save.
4. Head to the **Settings** tab and under **SSH Launcher**, press **Edit**. Under “Connect Using”, select “Credentials on another Secret” and select the connecting account created in Stage 2 from the dialog that appears. Once selected, click Save.
5. You should now be able to click the **Launch** button on the Enable Secret, PuTTY will open and you will end up with an enable shell on the target Cisco host.