Cisco Enablement Services Portal – User Guide for Distributed Customer

Document Name: Cisco Enablement Services Portal – User Guide for Distributed Customer
Revision: 5.0
Creation Date: 10th Jan 2017

1 Document Control

Change Record

| Date	Version	Change Summary
01/10/2017	1.0	Initial draft
03/09/2017	1.1	Review Comments Implemented
09/18/2018	1.2	Updated as per latest release changes
07/30/2019	2.0	CDA URL Change
07/21/2020	2.1	Operational Support details updated
08/12/2022	3.0	Enhancements to MAC Address Management UI

Contents

2 Overview

This document provides the information on how to use Cisco Enablement Services Portal. The document further goes into details for various tabs and the functionalities therein. It has screenshots for major steps which will help user to navigate through every functionality.

The web application is a platform for users to align the Cisco devices with the correct configuration profile and the profile eventually activates the device. The application also provides reports and activation history of the uploaded devices, and this document will guide the users through all the necessary steps in the device activation process.

3 Cisco Enablement Services Portal

3.1   Login

- Login to Cisco Enablement Services Portal by entering the below link in the browser.
 https://software.cisco.com/software/cda/home#
- The below site will open.
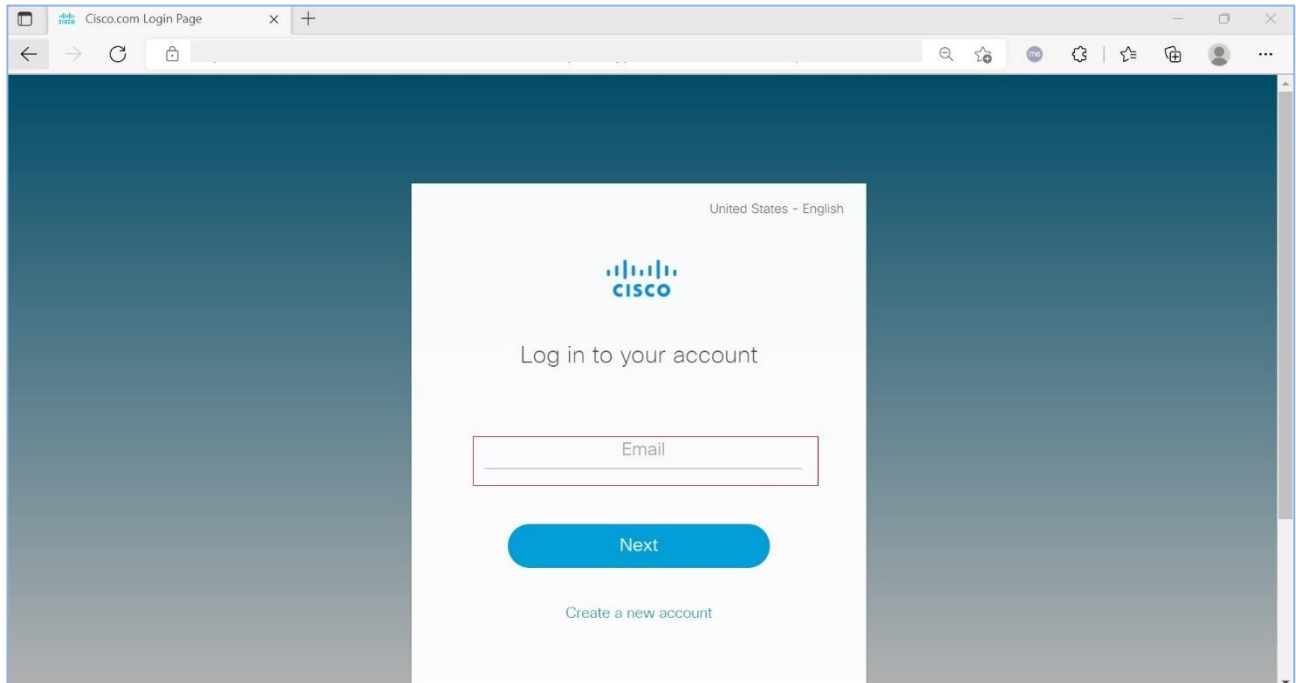
- Enter the Email ID of Cisco and click on next.
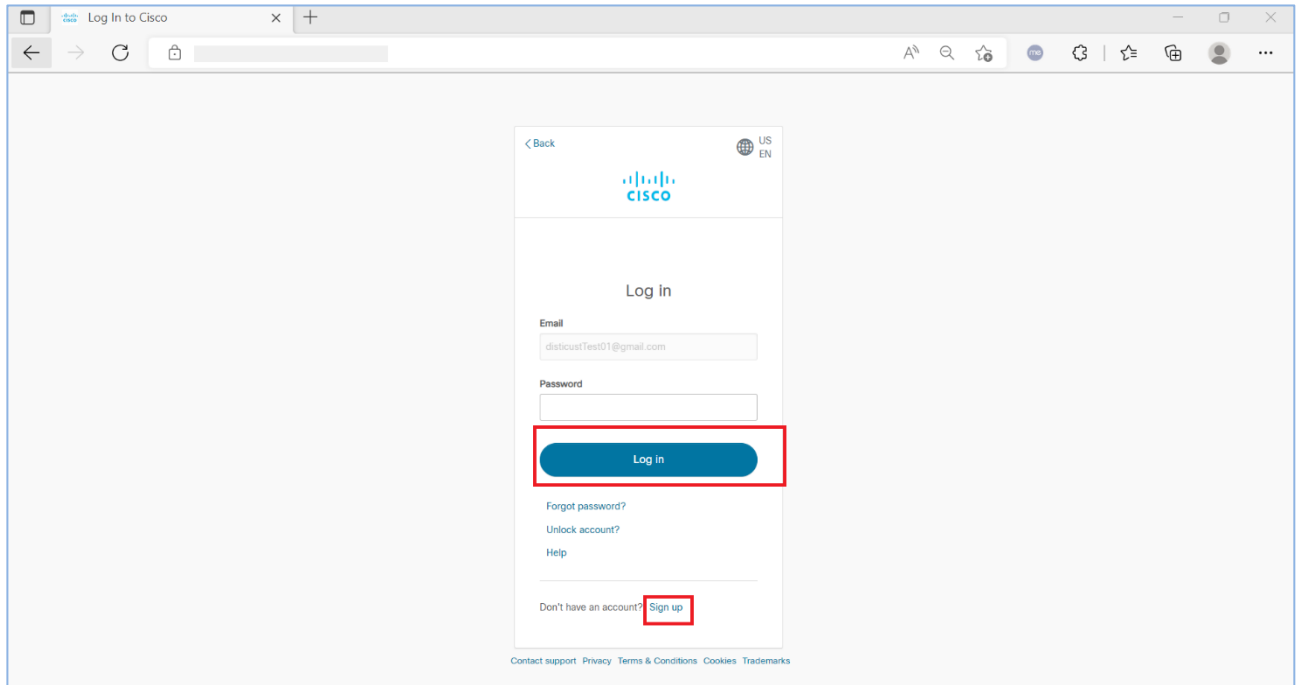
- Enter the Password and click on Login.
- If you do not have valid user id, you can register by providing your details using the Sign-**Up** Link.
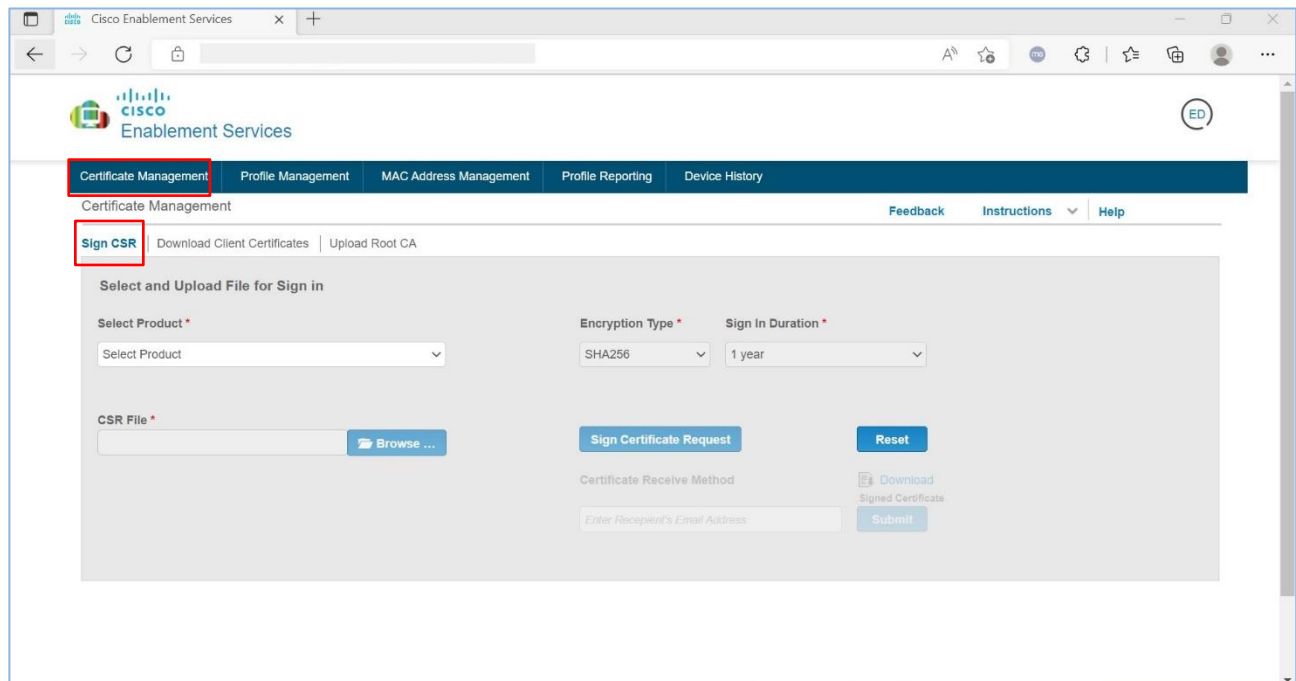
3.2   Certificate Management

Users can use Certificate Management page to get the certificate signed by Cisco which is used by the device to communicate to the Service Provider's server. Users can download the signed Certificate or can have the signed certificate sent to a specific email address.

- Click on 'Certificate Management' Tab.

3.2.1   Sign CSR

- Click on 'Sign CSR' Tab.

- Select a product from the 'Select Product' drop down.
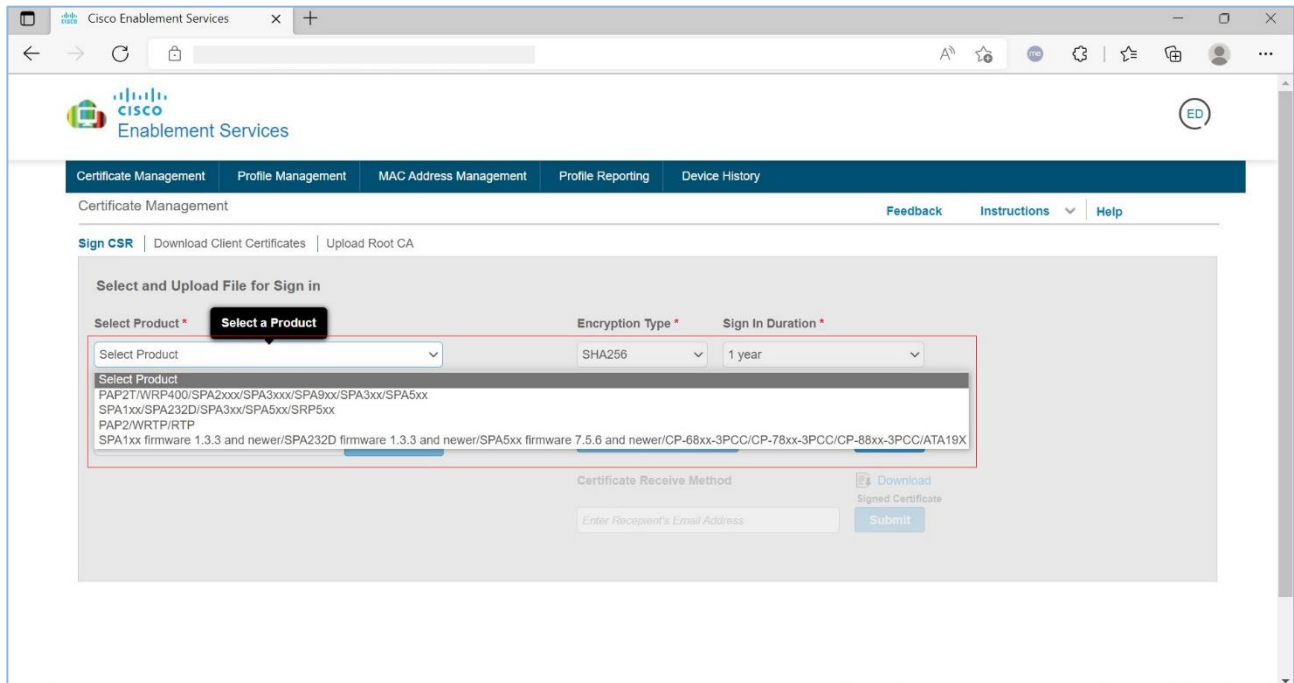
- 'Encryption Type', 'Sign in Duration' and the 'CSR File' attributes will be enabled only upon selecting the Product.
- Select the type of encryption from the under the 'Encryption Type' drop down (SHA1/SHA256). By default, the value selected is SHA256 Duration is 1 Year.
- Select the duration for the certificate from the 'Sign-In Duration' drop down (1 year /180 days).
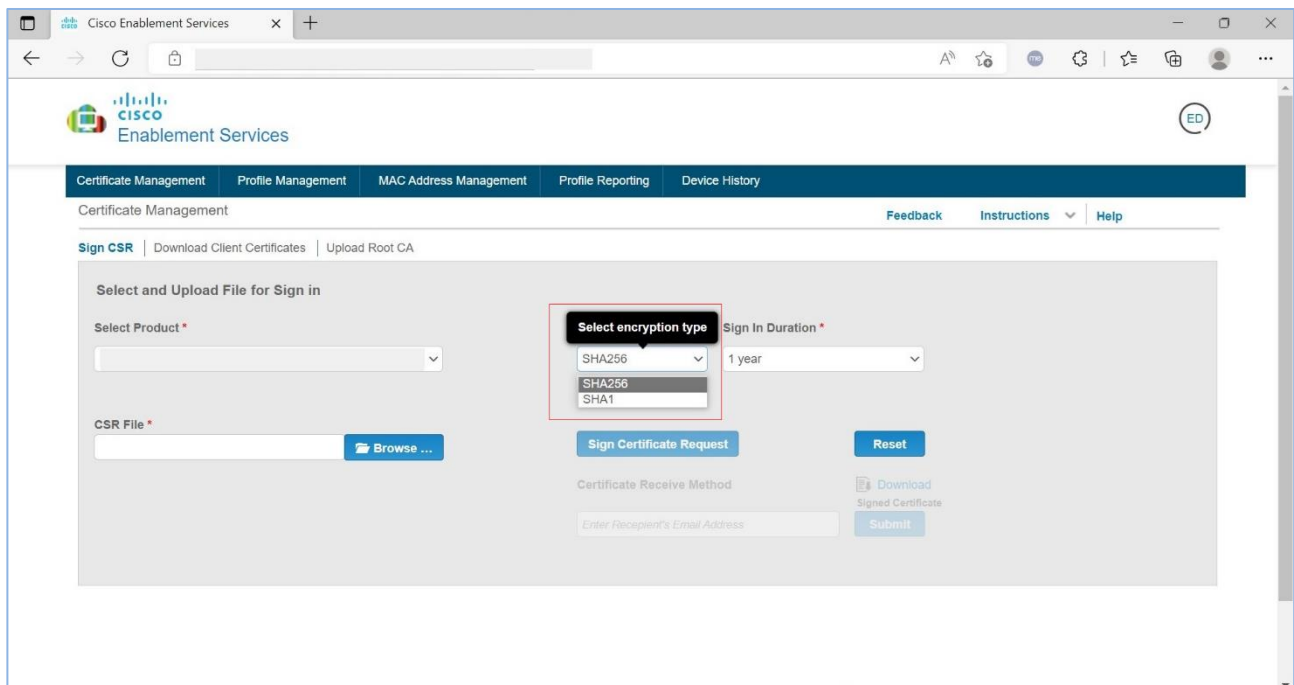
- The 'Sign in Duration' for the SHA1 encryption is defaulted to 180 days and SHA256 encryption is defaulted to 1 Year and limited to 1 year for both encryptions.

1. **SHA1 Encryption**:

2. **SHA256 Encryption:**

- *Note:*
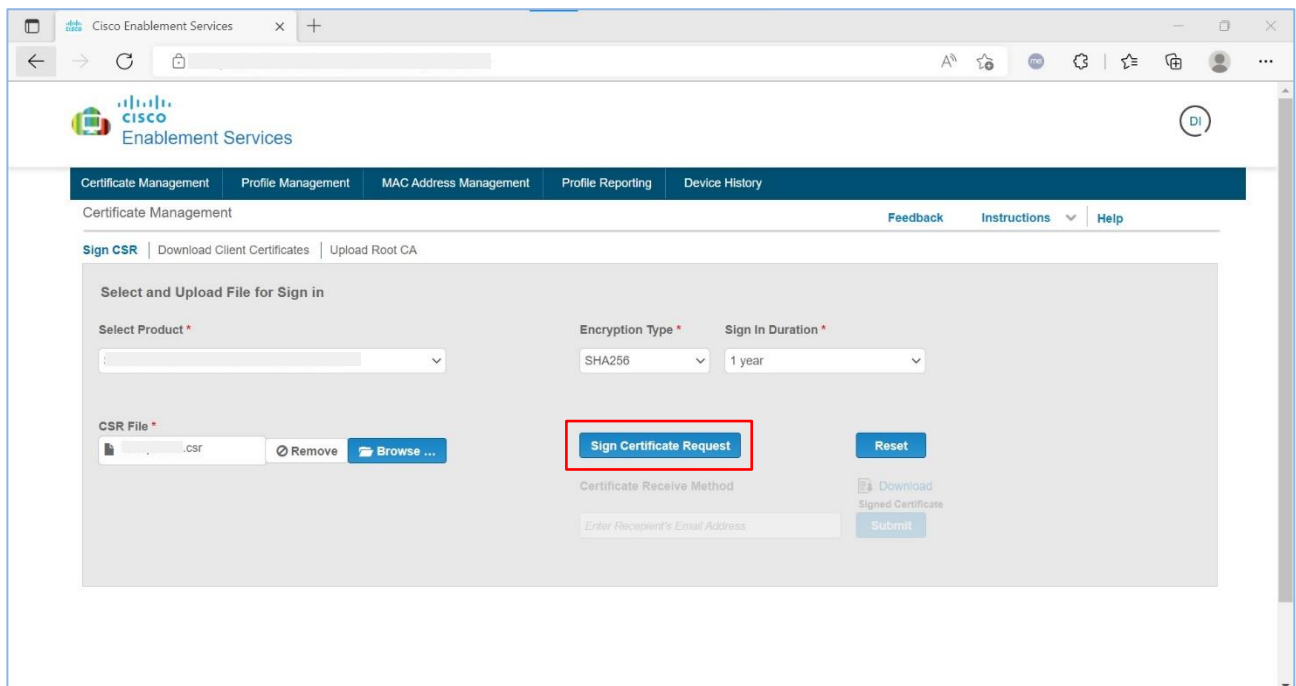 - When SHA1 encryption is selected below warning message will pop up to confirm the encryption selection.
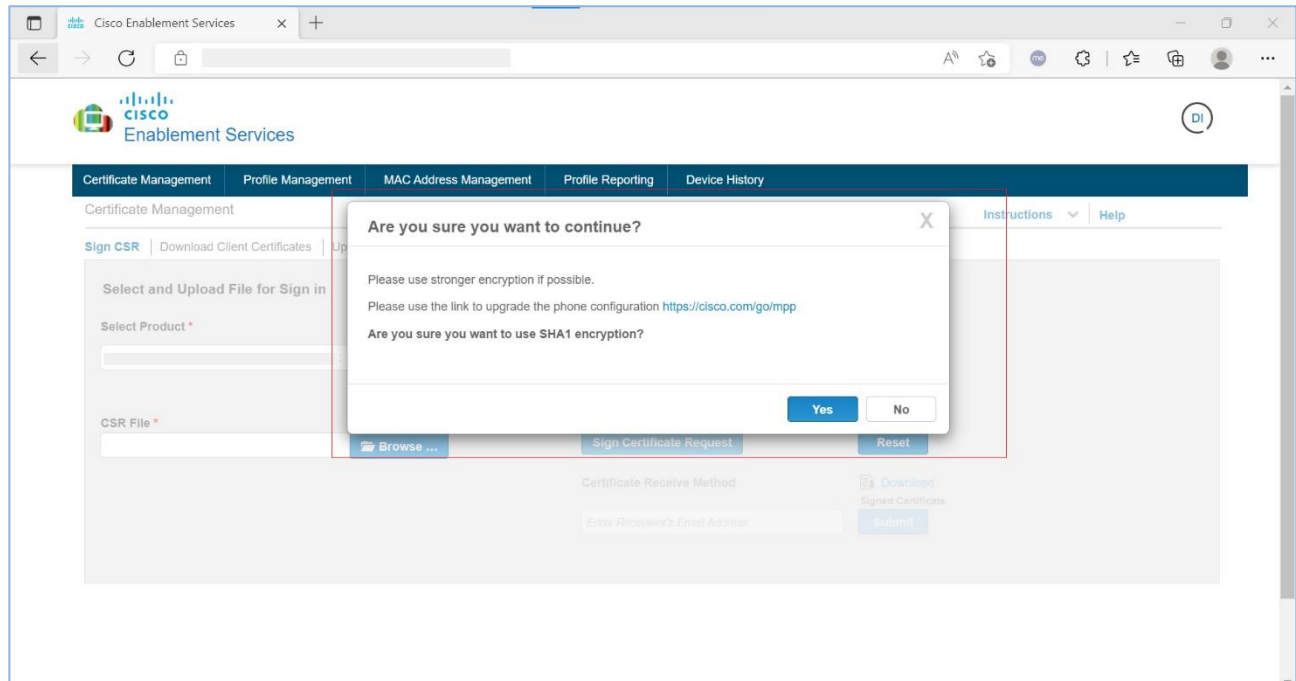
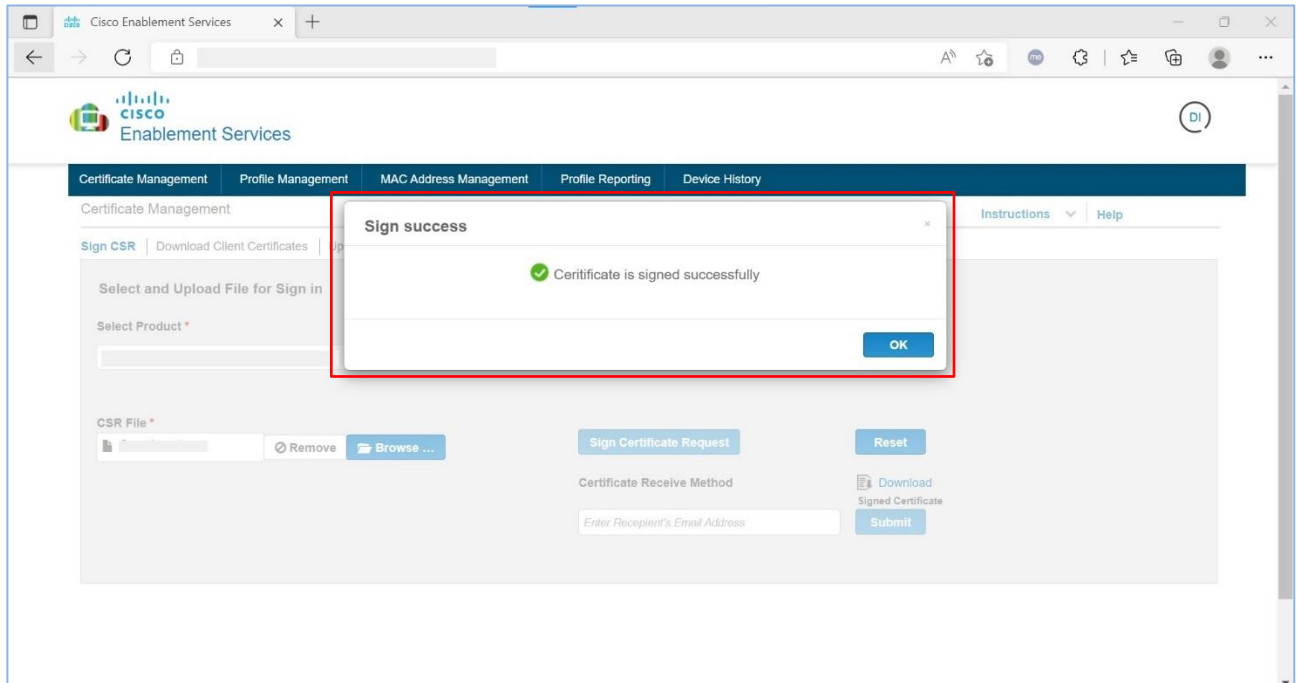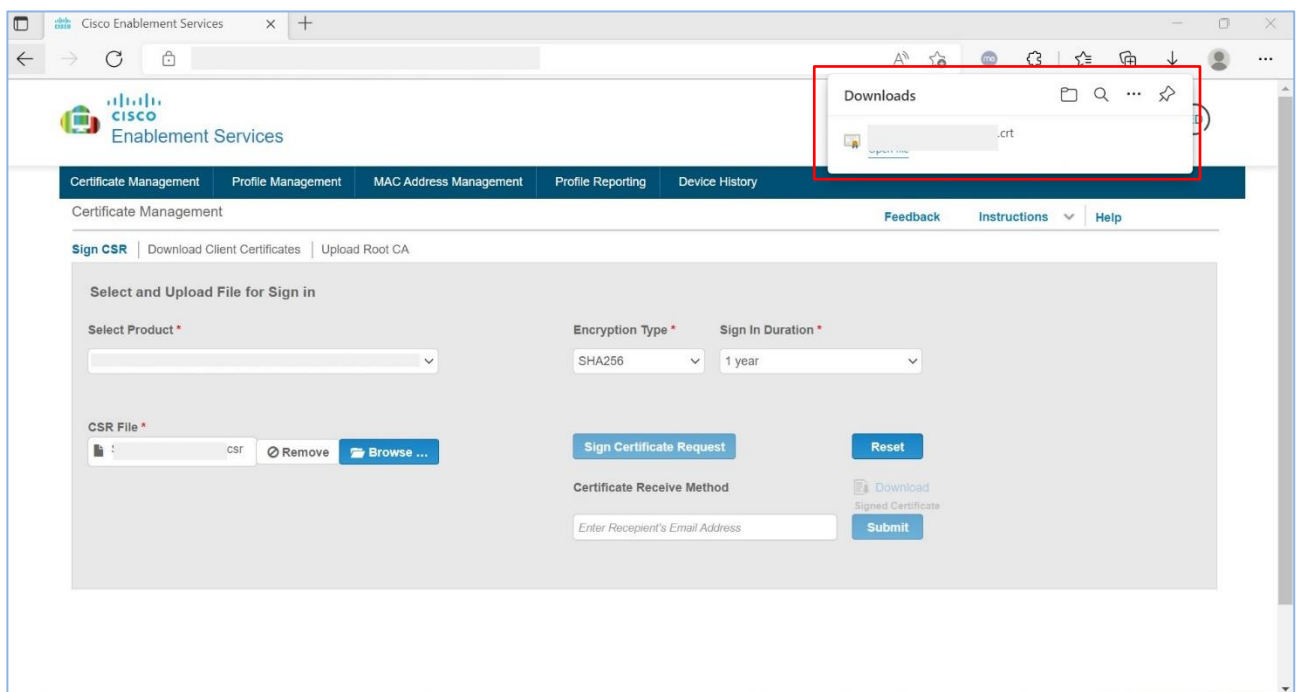

- Upload the CSR file in the CSR File field.
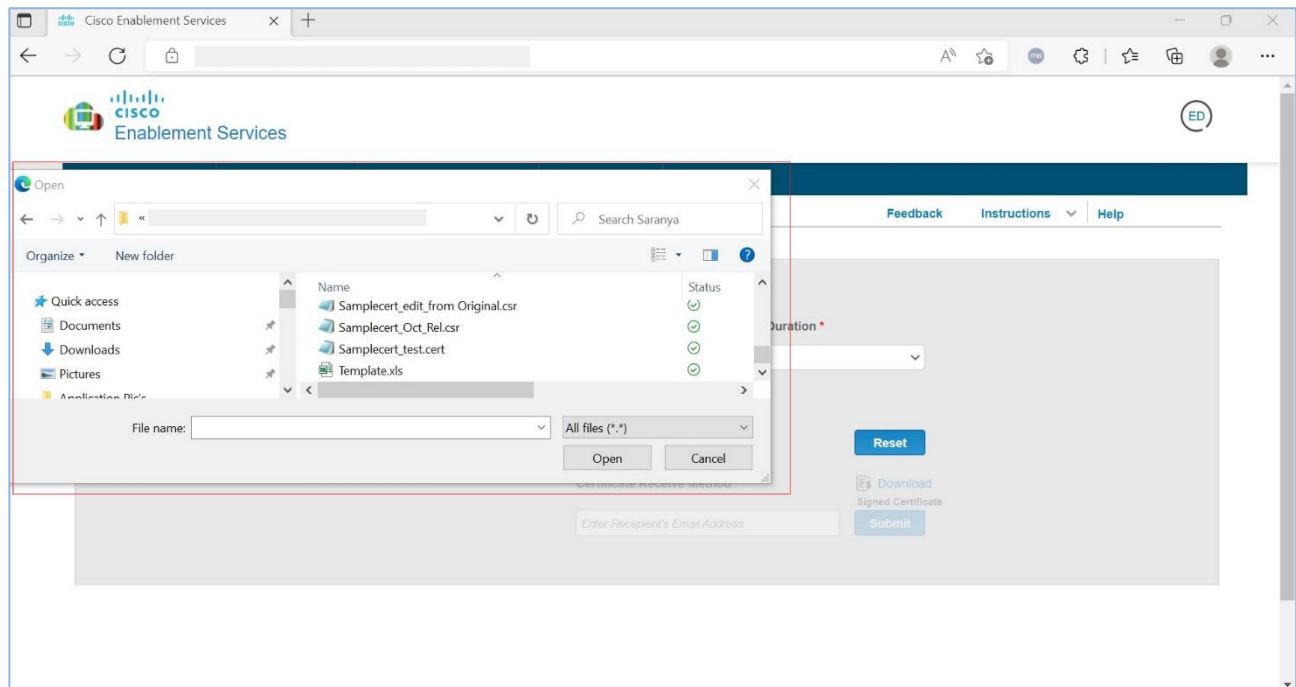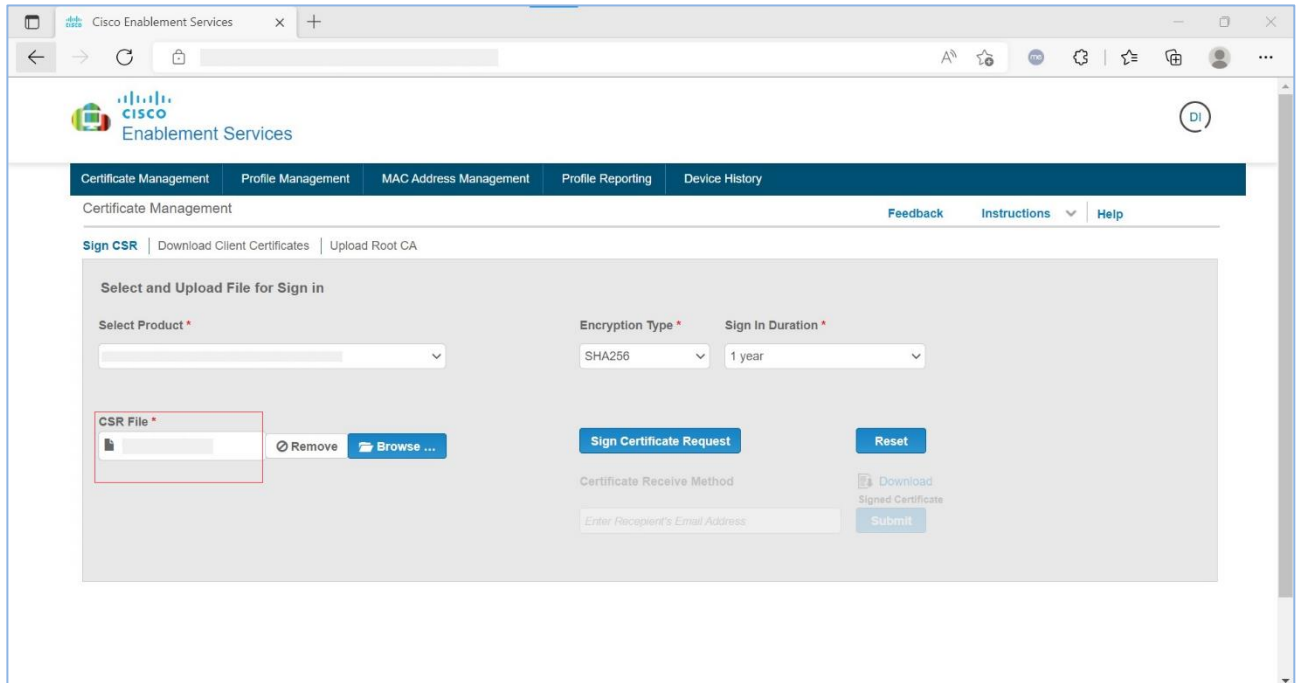
- Click on 'Sign Certificate Request' to sign the certificate file that was uploaded. File will now be signed.

- Once the certificate is signed successfully the message, 'Certificate is signed successfully' will appear on the screen as shown below.
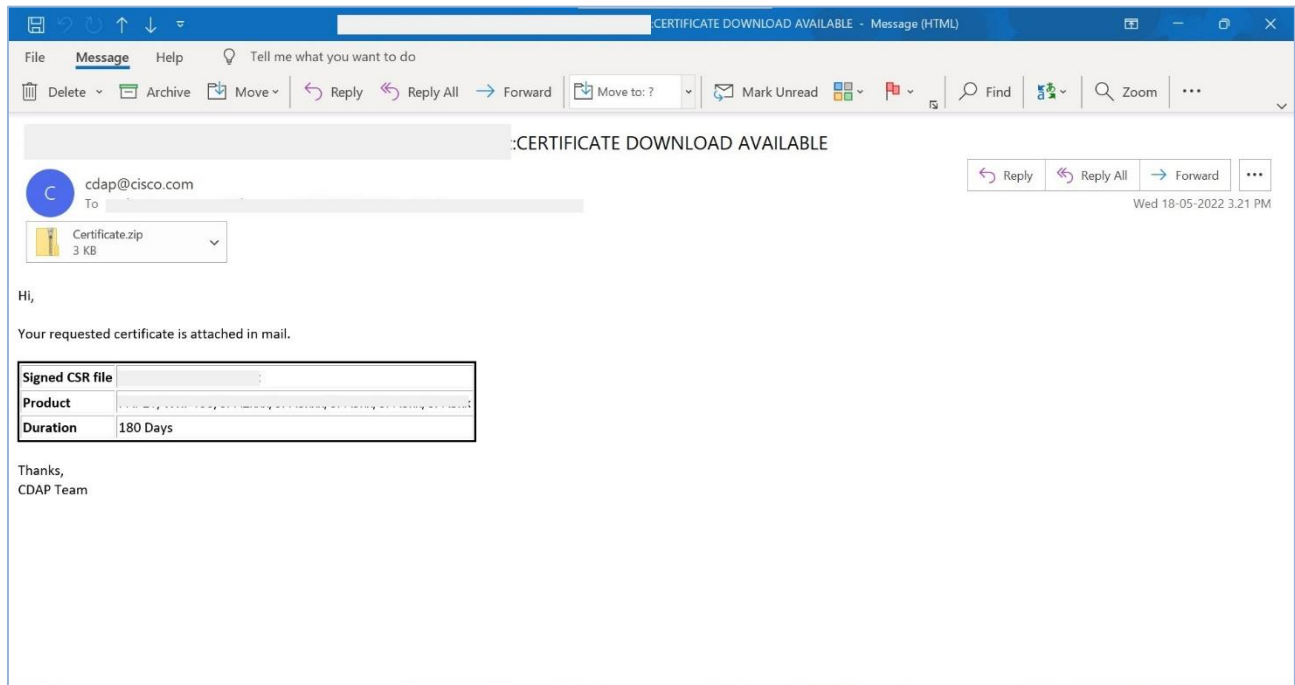
- Click OK.

- Click on 'Download' to download the signed certificate.

- Under 'Certificate Receive Method' - Enter an email address in the email address field to send the signed certificate to an email address.

- Click on 'Submit' button to send the signed certificate to email address entered. You will get a confirmation message stating that the file has been sent to the email address. The file uploaded to be signed and the file sent through email has the same name.
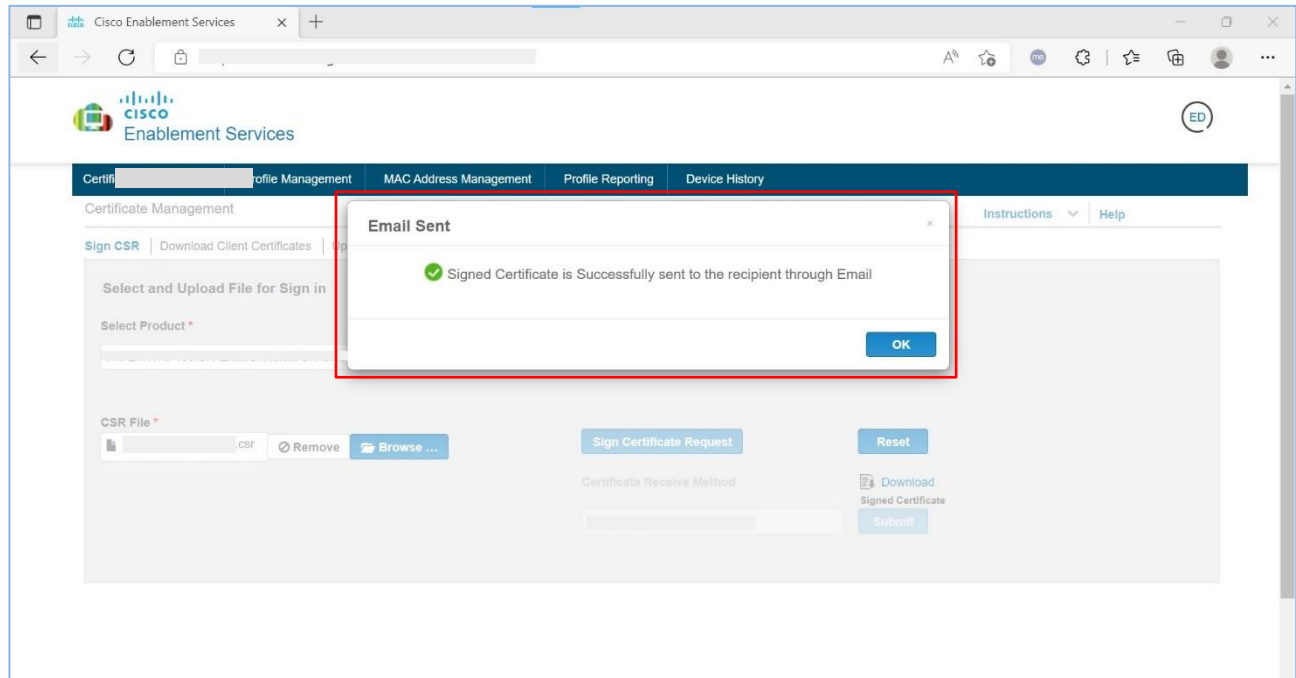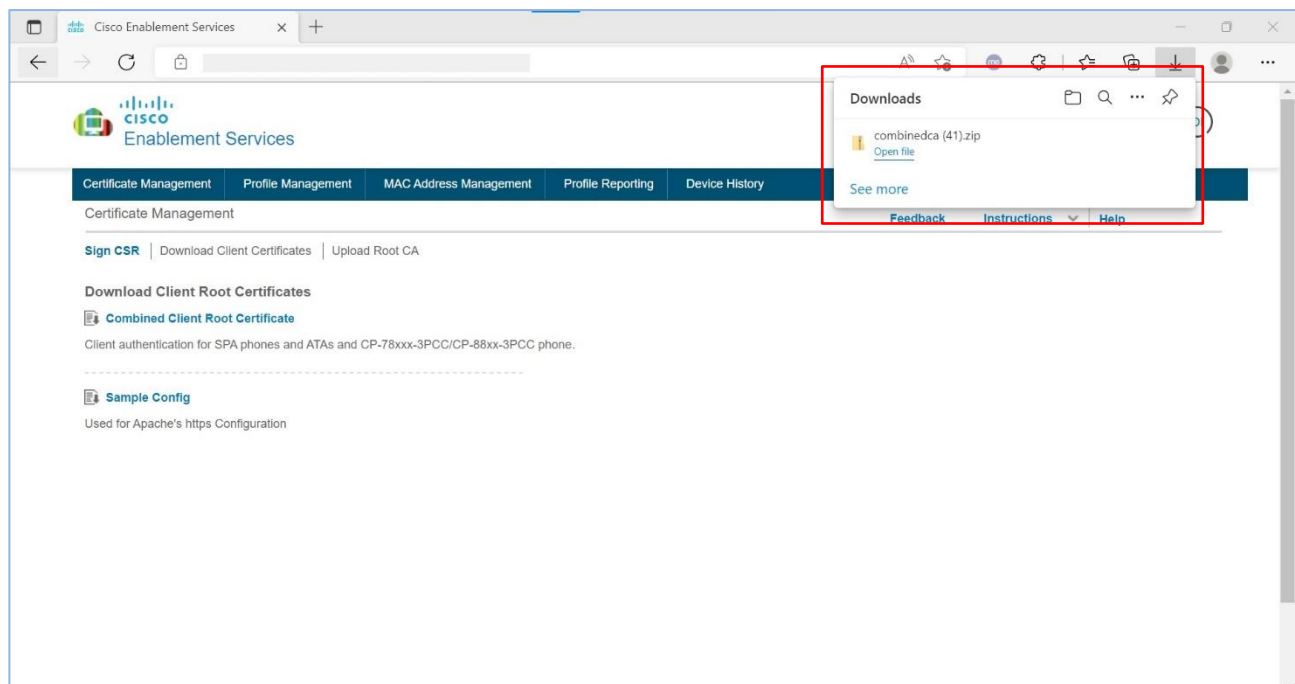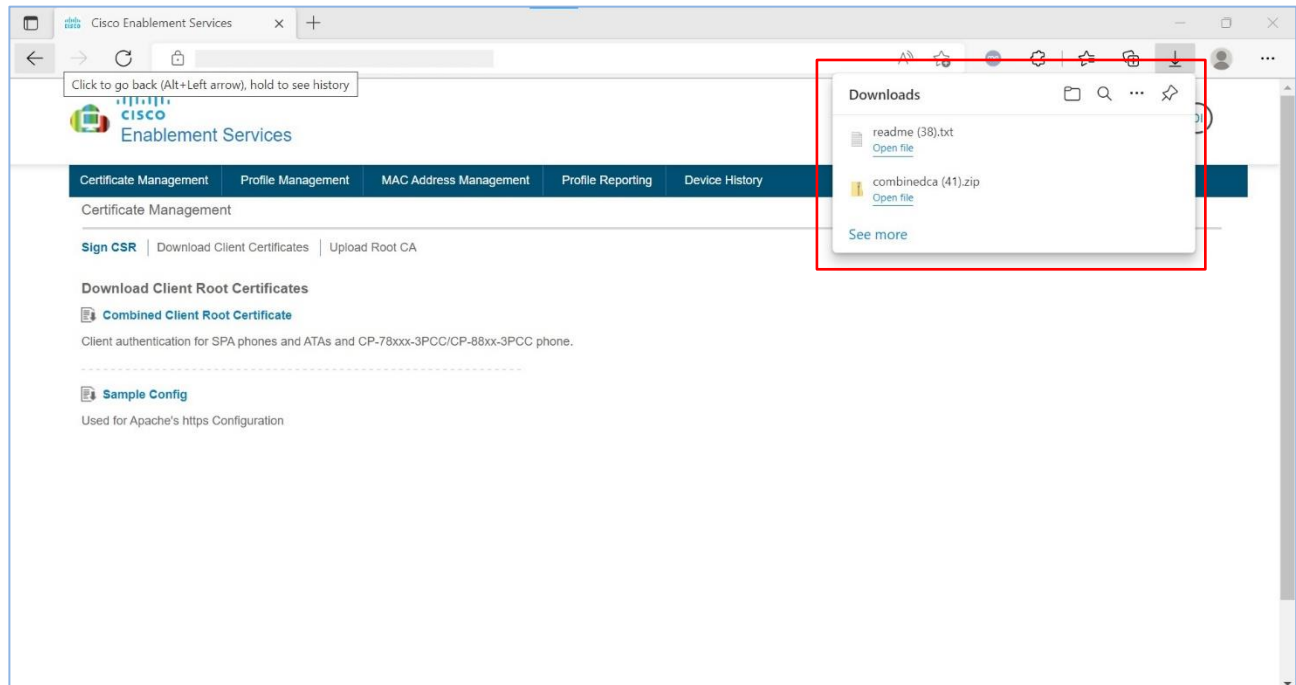
- Email received in the inbox.

3.2.2 Download Client Certificates

- Click on 'Download Client Certificates' tab to download client certificates from the portal.
- Click on 'Combined Client Root Certificate' link to download certificate used for SPA phones and ATAs.

- Click on 'Sample Config' link to download the configuration file used for Apache Configuration.


3.2.3 Upload Root CA

This is a capability to allow Service Provider/Reseller to upload Root CA to CDA web portal and provide CDA web server hosted URL that can be used for their profile configuration. CDA web portal can host the Root CA file that the Customer will upload and provide URL back that will be used for profile configuration.

- Click on 'Upload Root CA' tab.
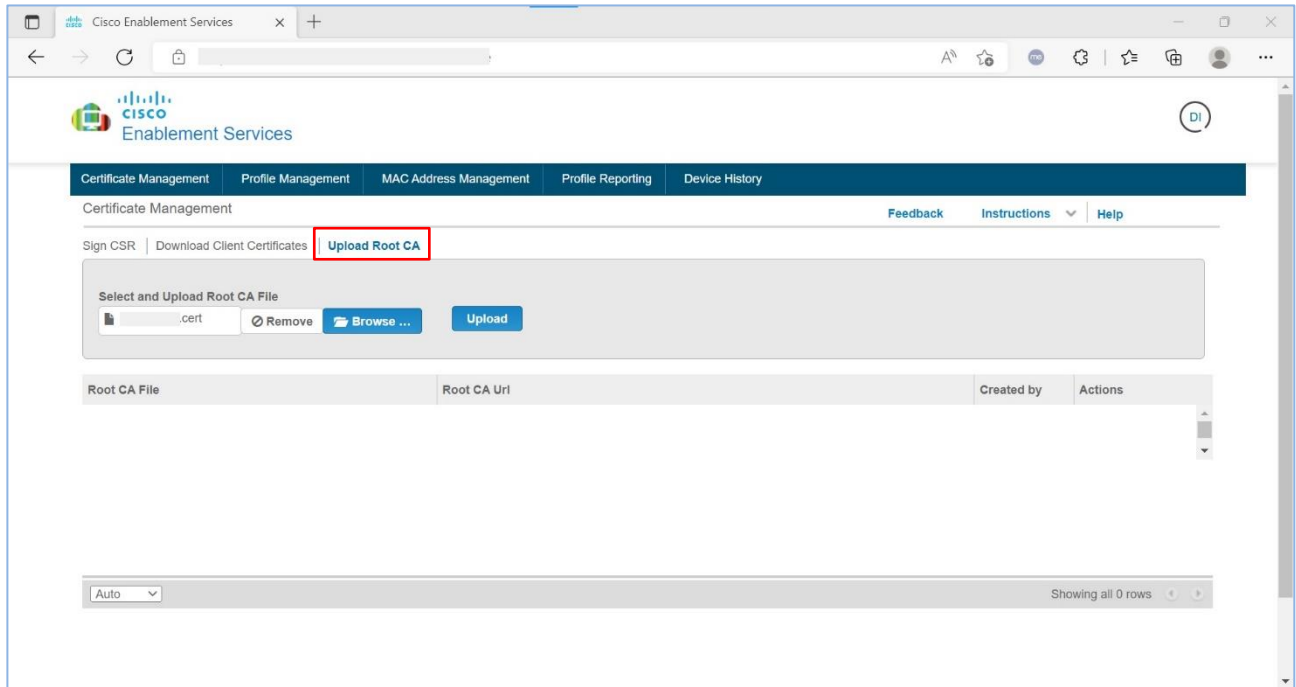
- Click on 'Browse button' select the file. Portal will accept only these formats:
  - **.pem, .cer, .crt, and .cert.**
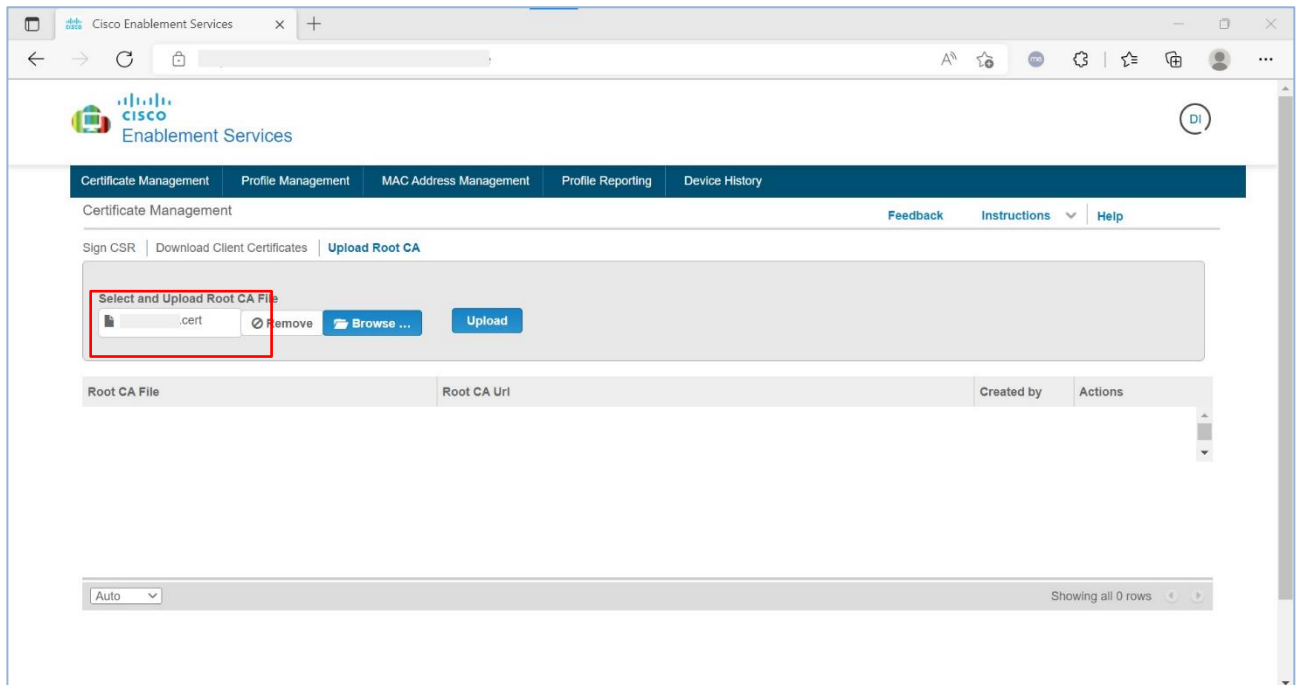
- <u>Note</u>:
  - The Root CA file should be < = 20 KB in size.
  - Portal allows up to 100 files to be uploaded.
  - After the maximum limit, user is expected to delete at least one file to upload one file.
 - Only a valid PEM format cert file can be uploaded.

- Click on 'Upload' button to upload the file.
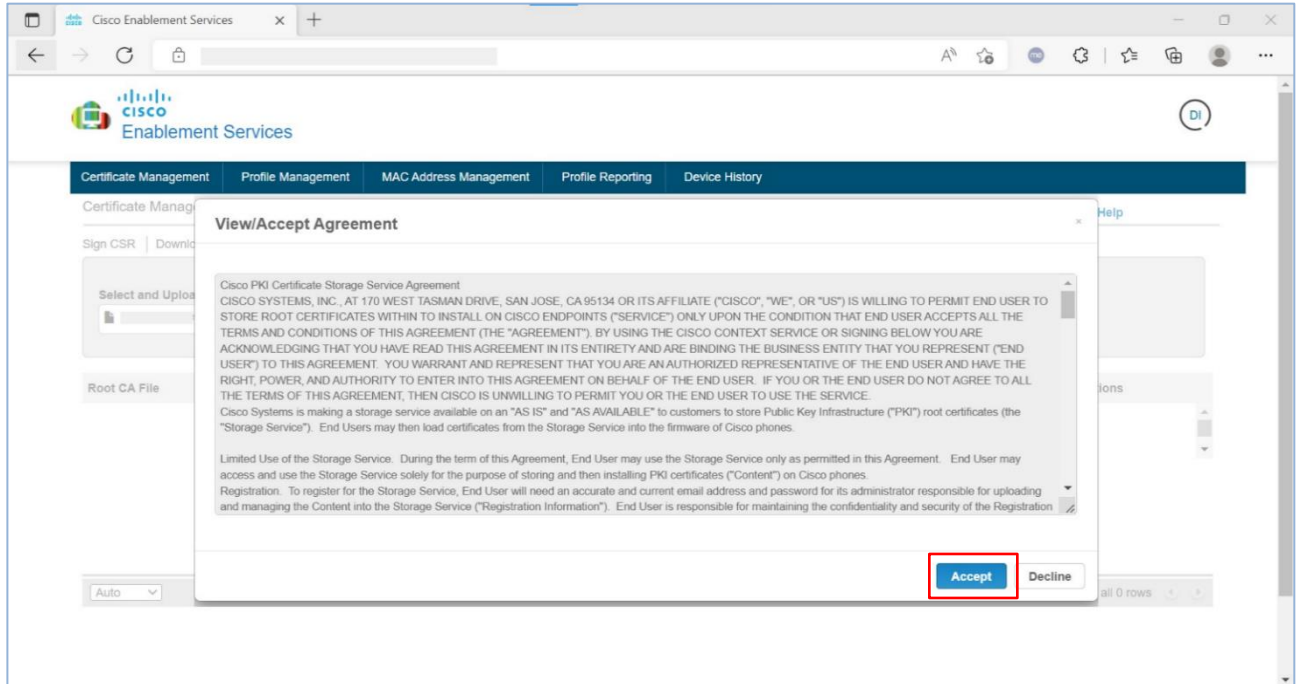
- Once you click on upload, the View/accept agreement screen will appear. Click on "Accept" to upload the file. If you click on "Decline" file will not upload.
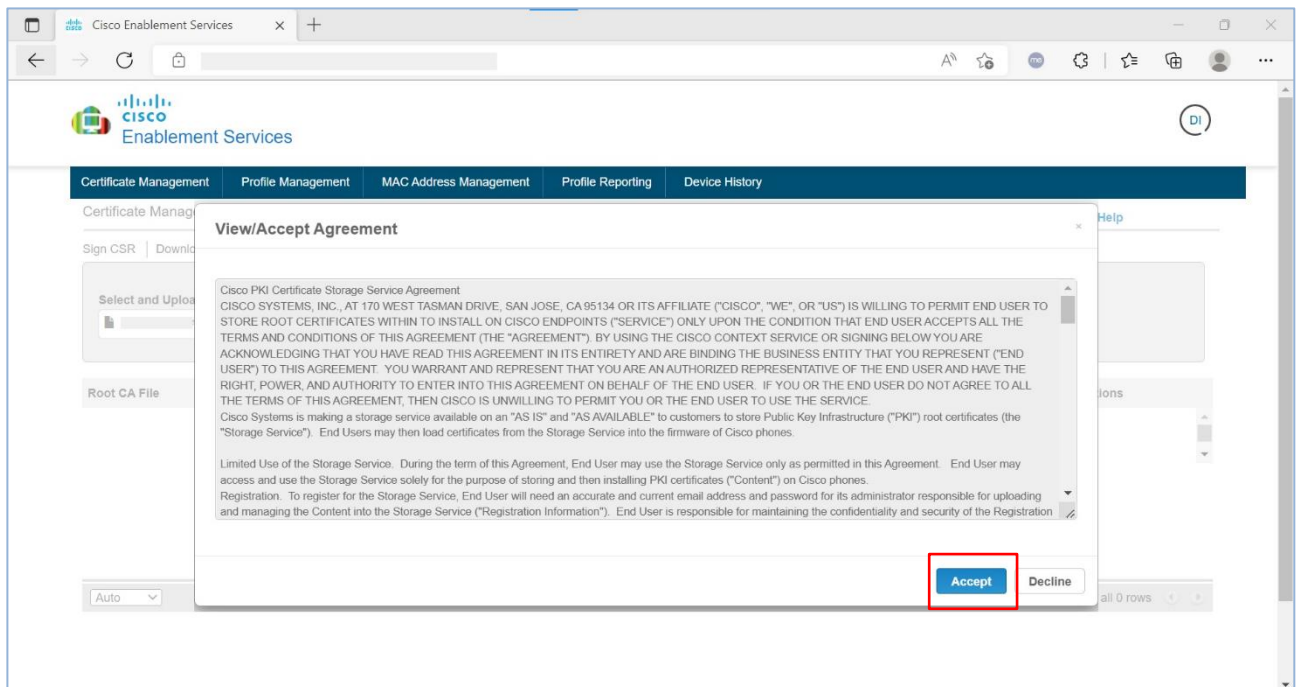
- Now the file is uploaded. You can Edit /Delete and copy the file URL option to modify file.
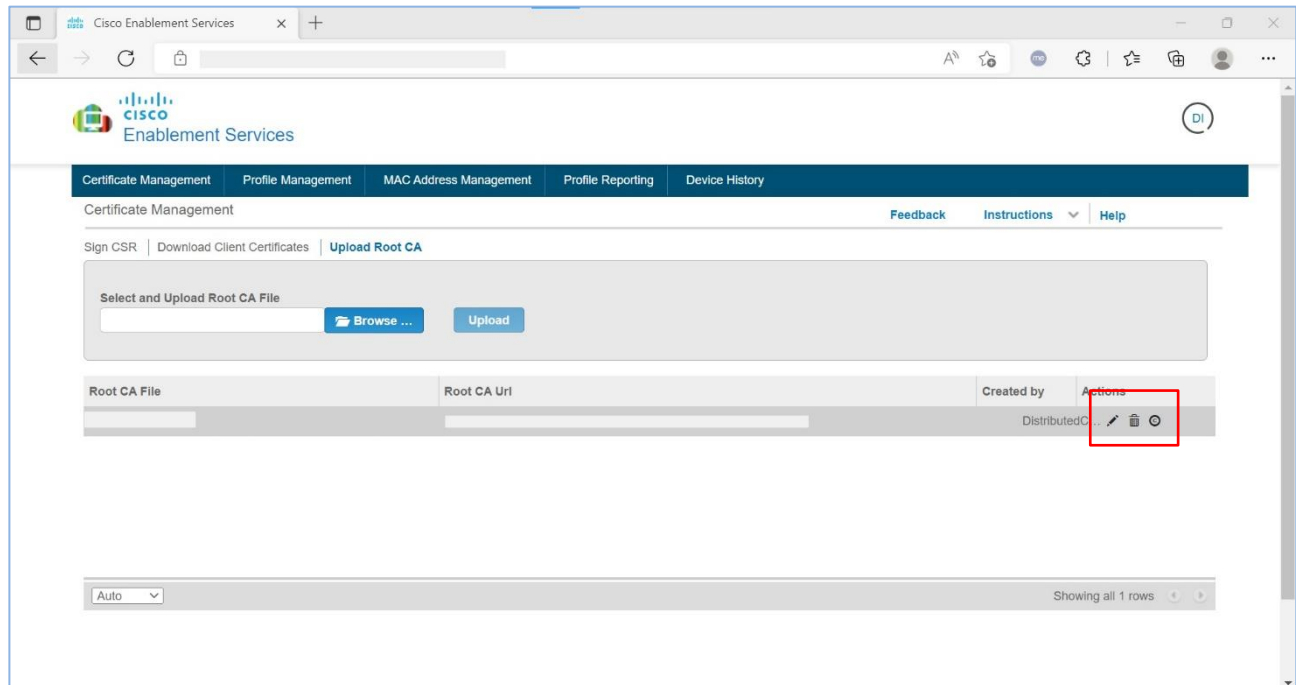
- To Edit, click on ✏
- To Delete, click on 🗑
- To Copy the file URL, click on ⊝
- Note:
    - User can only edit / delete a single file.
    - Edit the file and click on 'Save'.
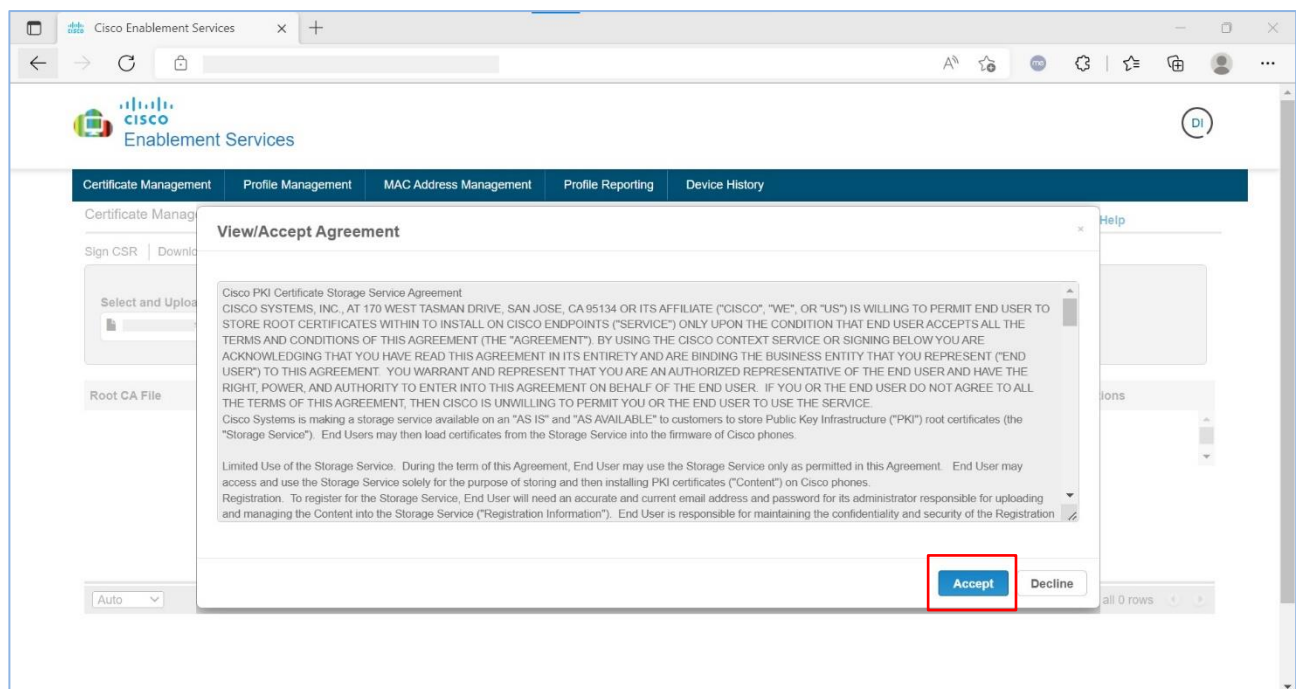
3.3 Profile Management

Profile Management page can be used to add new profiles, edit profiles, and delete profiles. Users can add profiles for the company they belong to.
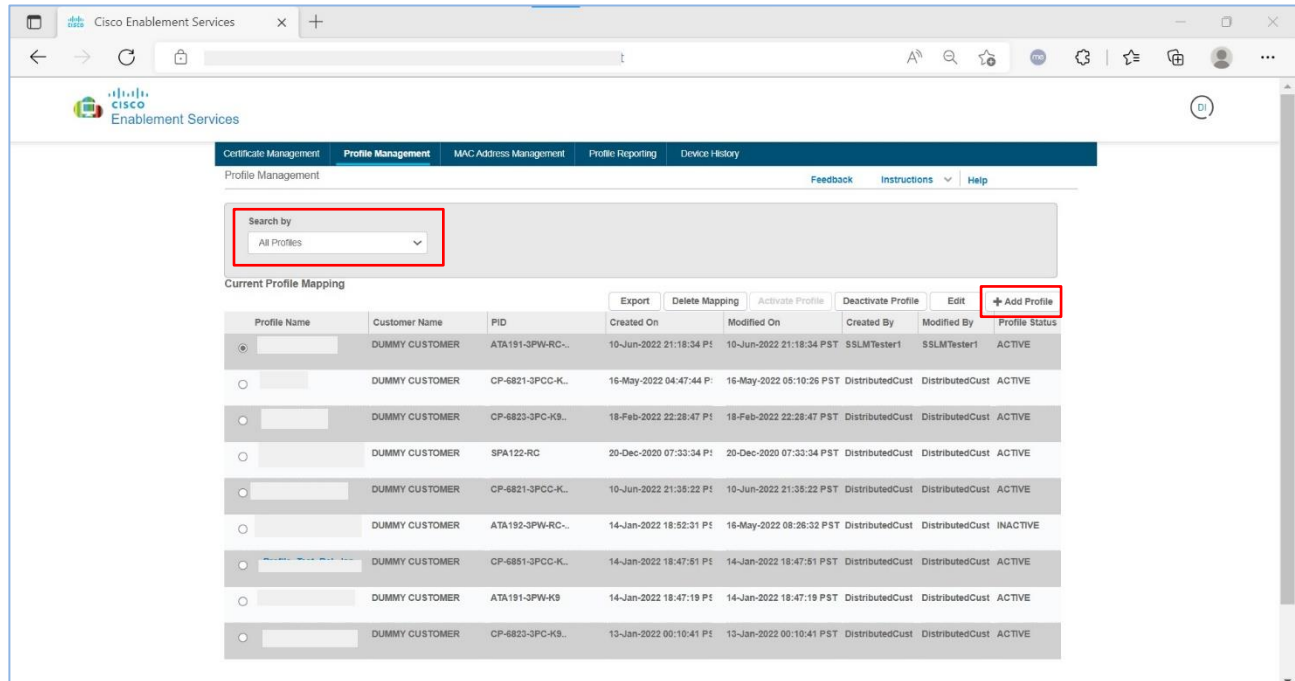
- Click on "Profile Management" tab.
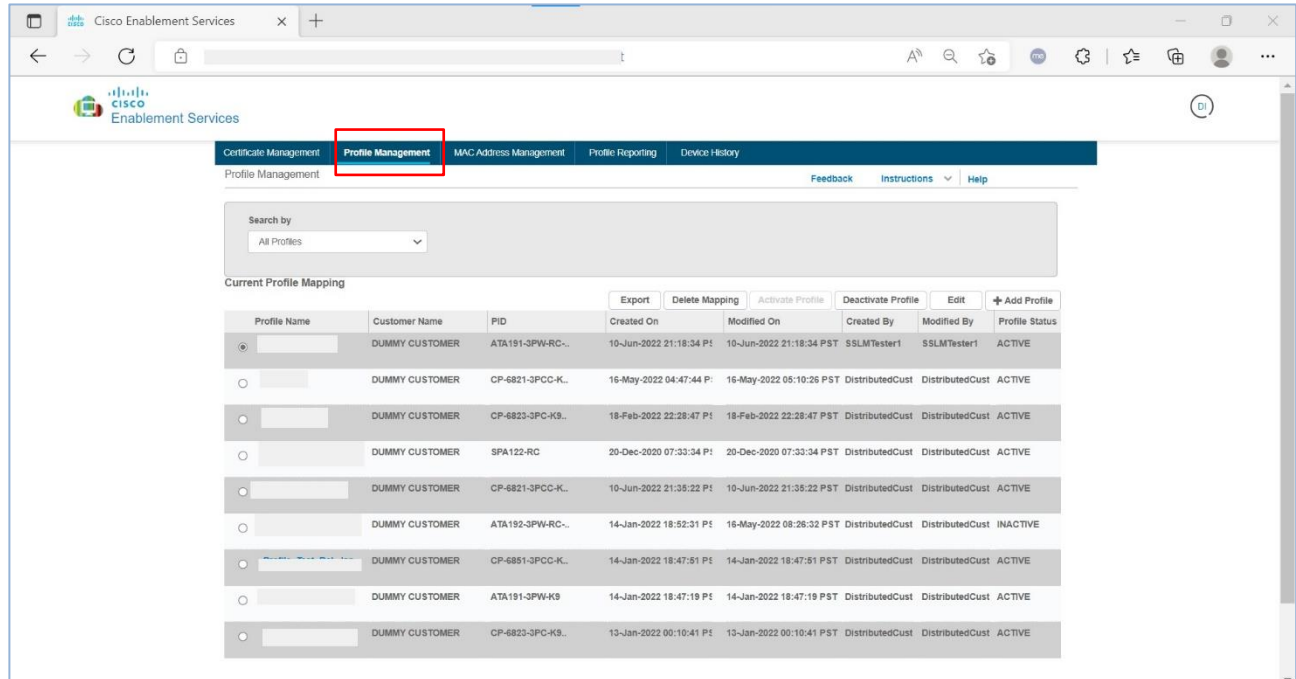
- Select an option from the dropdown to proceed with the search.
- Click on profile name to view the contents of the profile.

1. Add/Create Profile

- Click on Add Profile button to add profiles.

- Note:

  o The Profile name should be unique. Duplicate Profile name is not allowed in the system. However, for Distributed Customer/Customer Admin/ Customer User roles, same name can be used for two Profiles with different PIDs selected.
  o **Distributed Customer:**
    - While user is creating a new profile by using the same profile name that already is available to him/her, the system will map the existing profile of the PID by creating a new line available on the screen. But if a different user is trying to create the profile, then the user is prompted to use a different profile name.

High Level Flow - Profile Management

User A can be a Distributed Customer / Customer Admin

User A creates Profile

Profile exists with that name?

Is the Profile created by the User A or by users from the Org he belong to?

Yes

No

No

Yes

Return Error message to User to enter unique Profile name

Create the profile

Add to the existing mapping without updating the config file
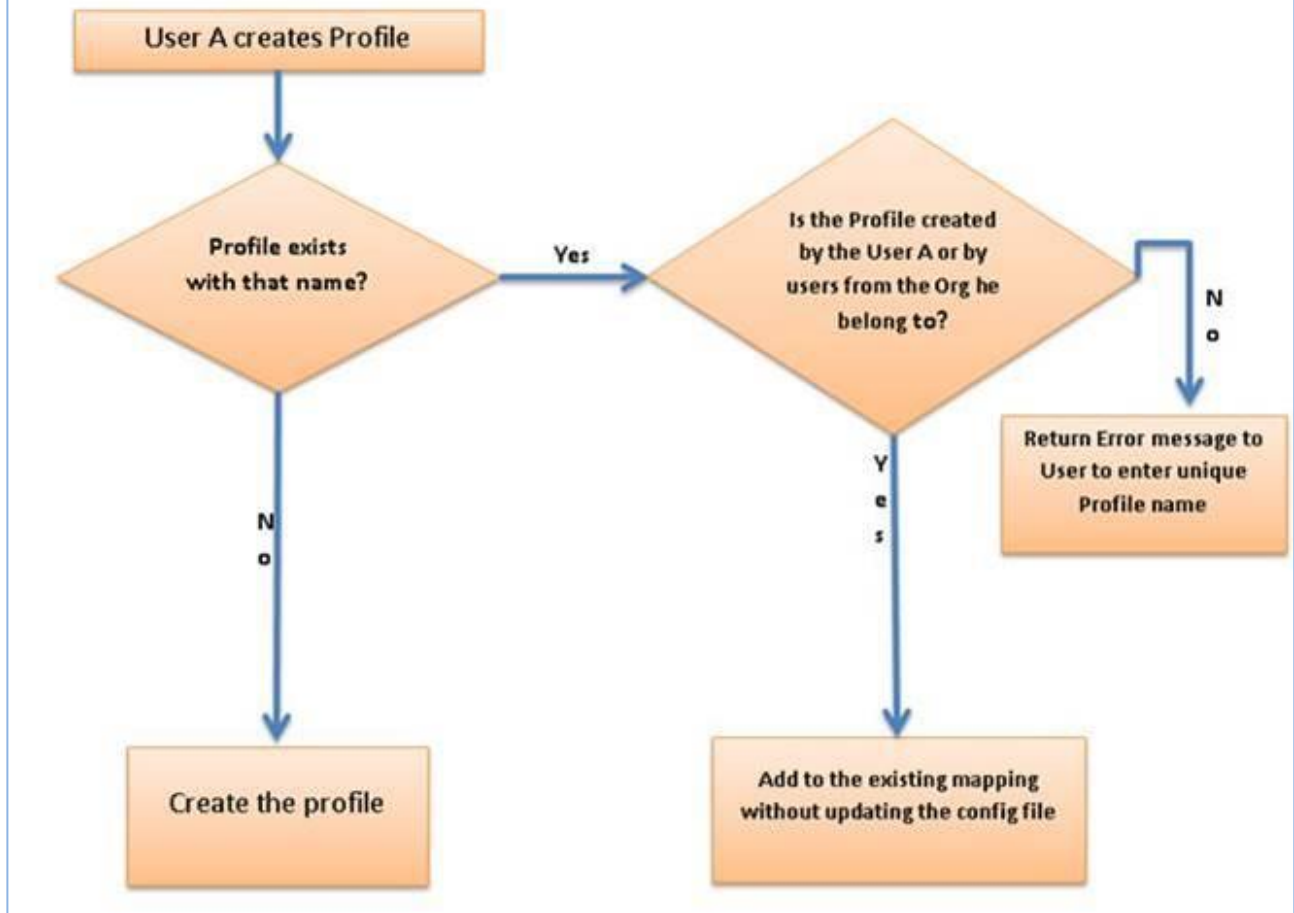
- Select the PID from the dropdown.
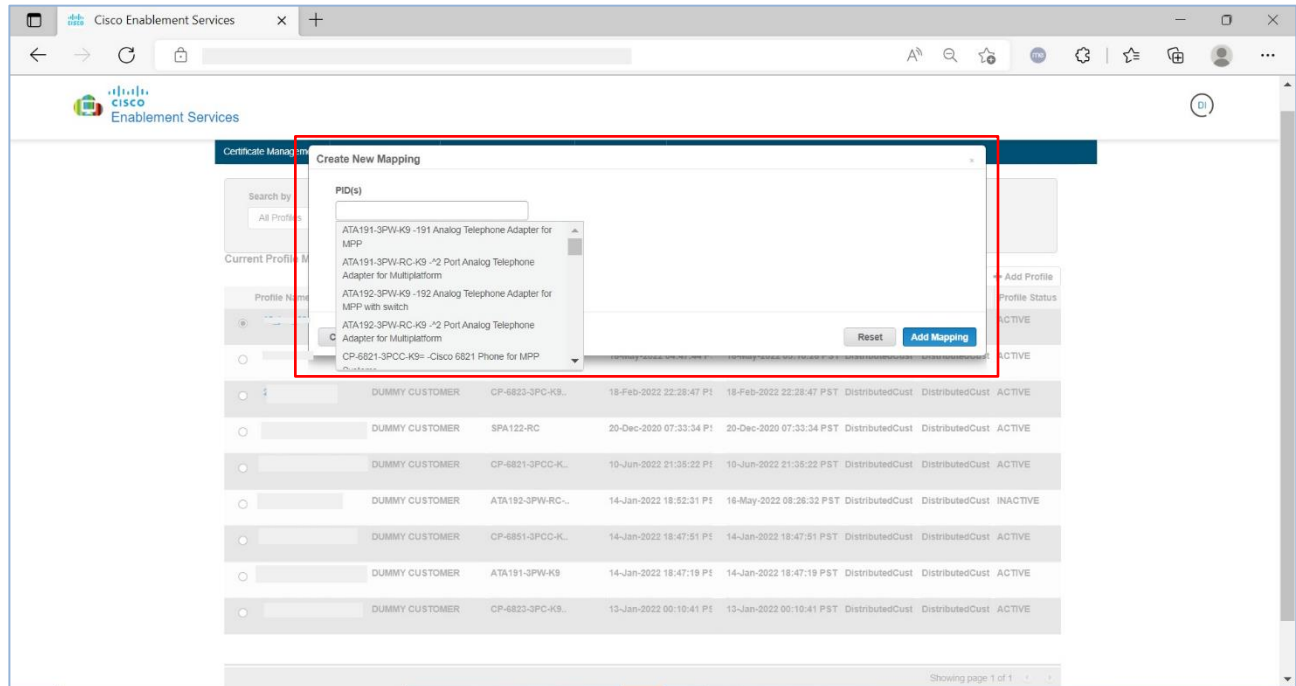
- Select 'Create a New Profile' to add another profile or select an existing profile from the dropdown.
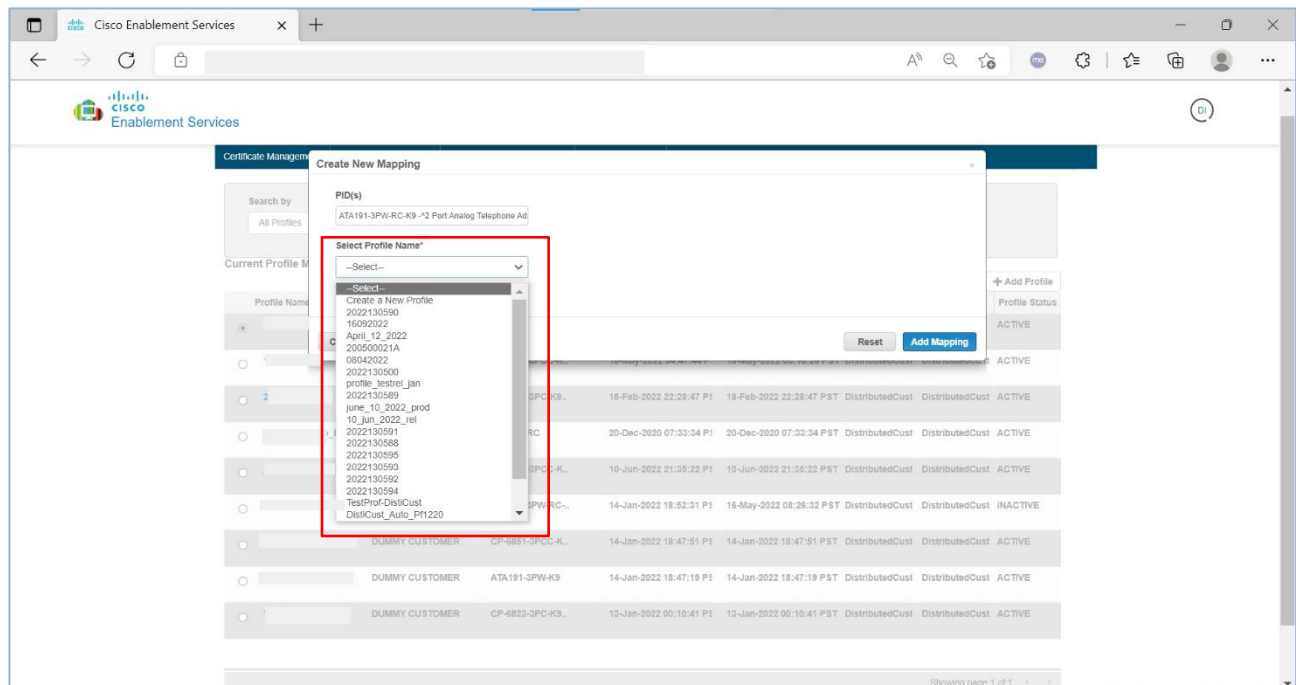
- If 'Create a New Profile' option is selected, enter the profile name in the 'Enter Profile Name' textbox.
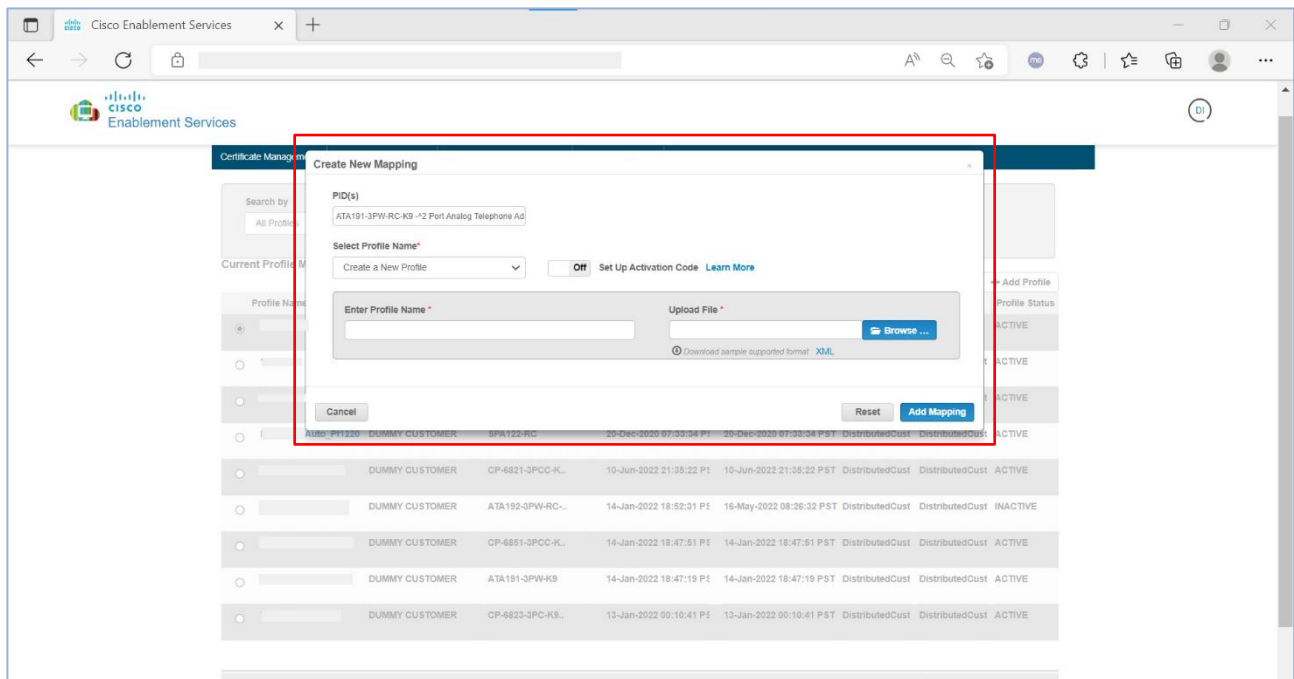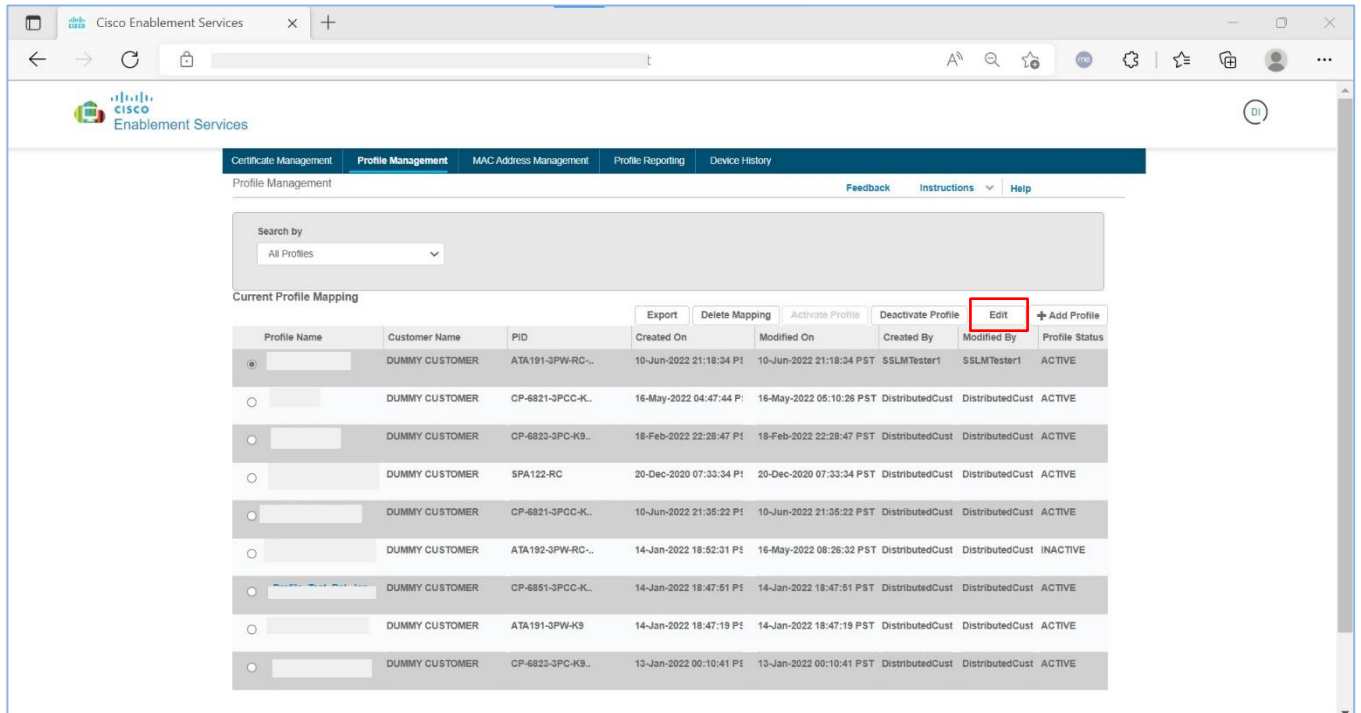
- Browse and upload the config file. *(Supported file format .XML)*
- On click of 'Add Mapping', a pop up will be shown confirming that the profile has been successfully saved.
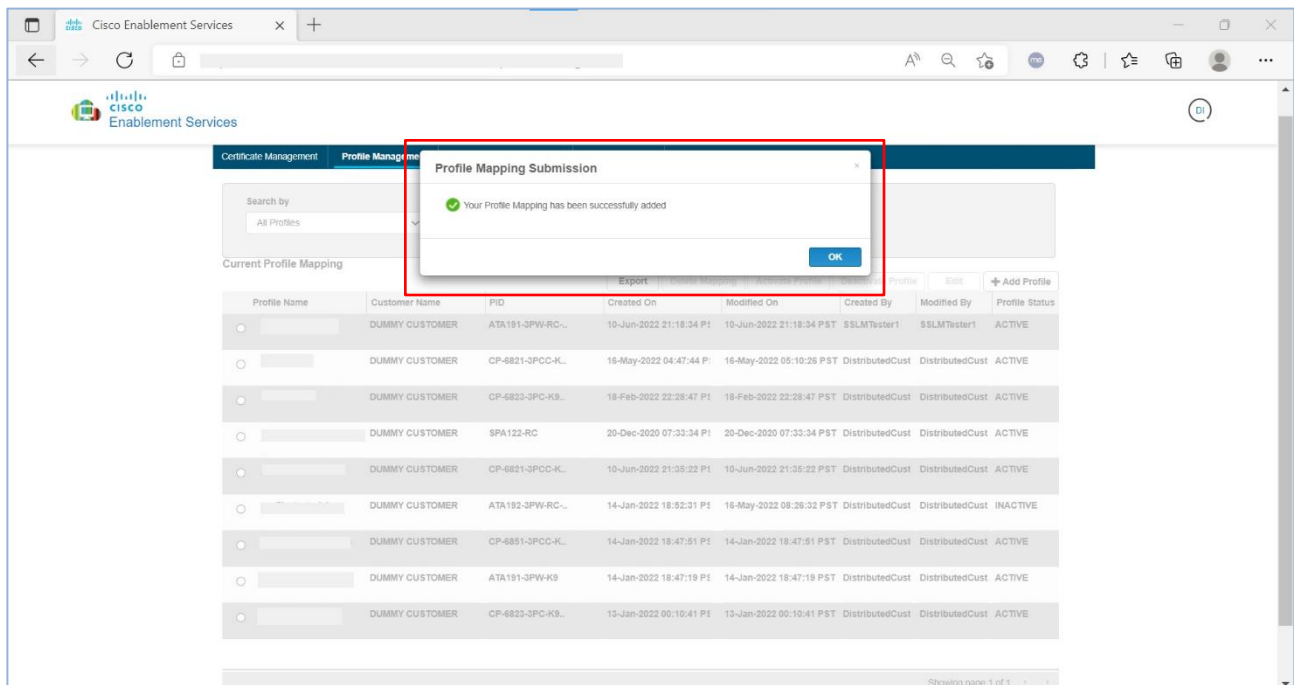
2. Edit Profile
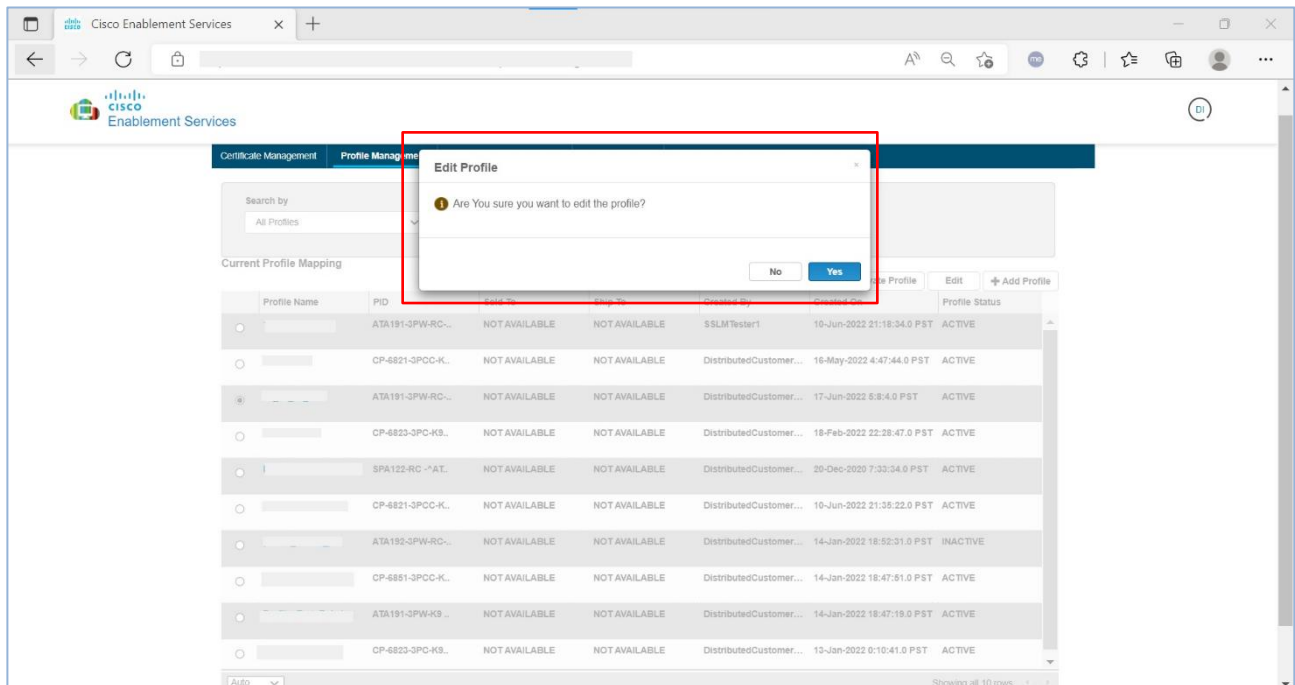
- Select profile and click on 'Edit' button to edit the profile.

- Click on 'Yes' to continue editing the profile. Click on 'No' to go back to the page.
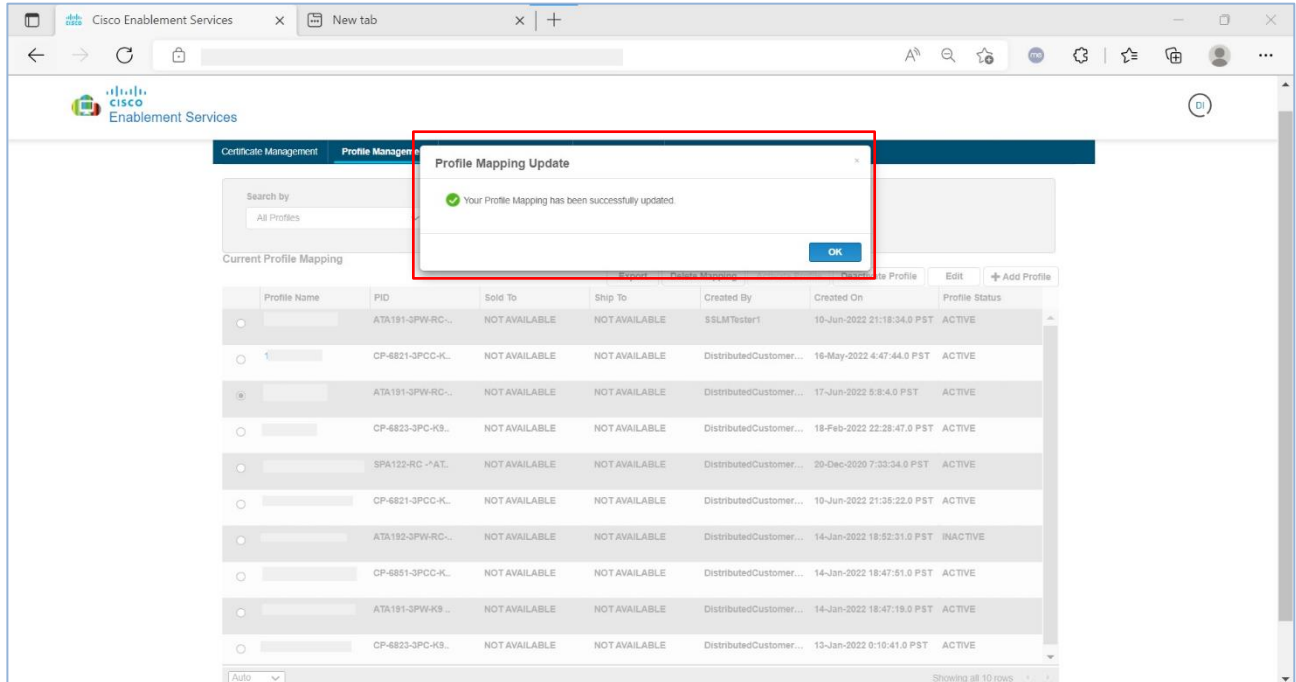
- Browse and upload a profile configuration in 'Upload File' section.
- Click on the XML to download sample profile configuration in XML format.
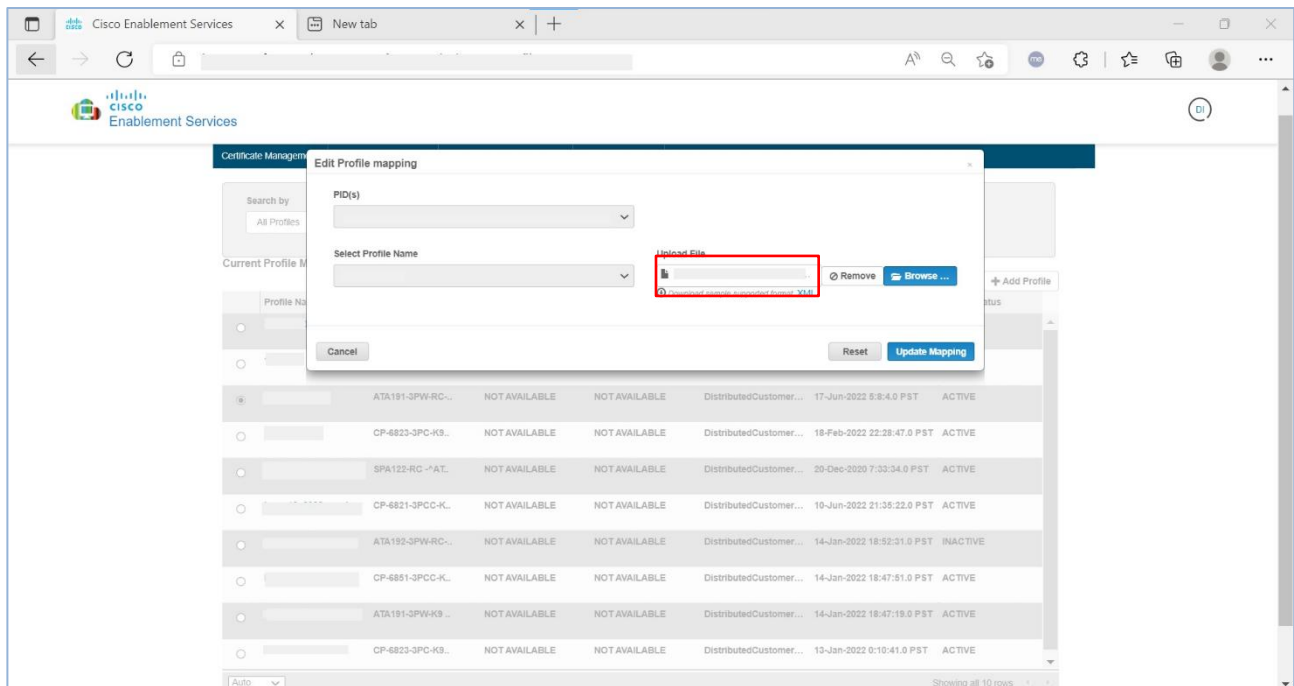
- Click on 'Update Mapping' to update the profile.
- Click on 'Reset' to reset the form. Click on 'Cancel' to close the 'Edit Profile Mapping' dialog box.
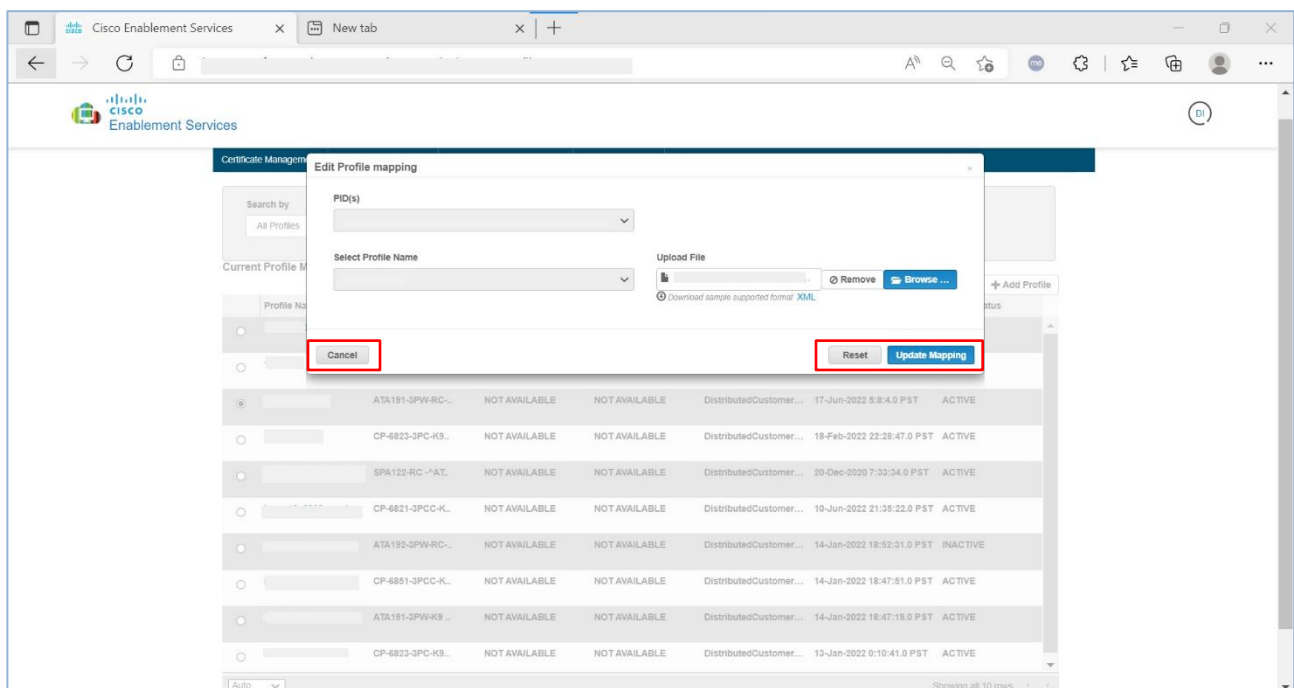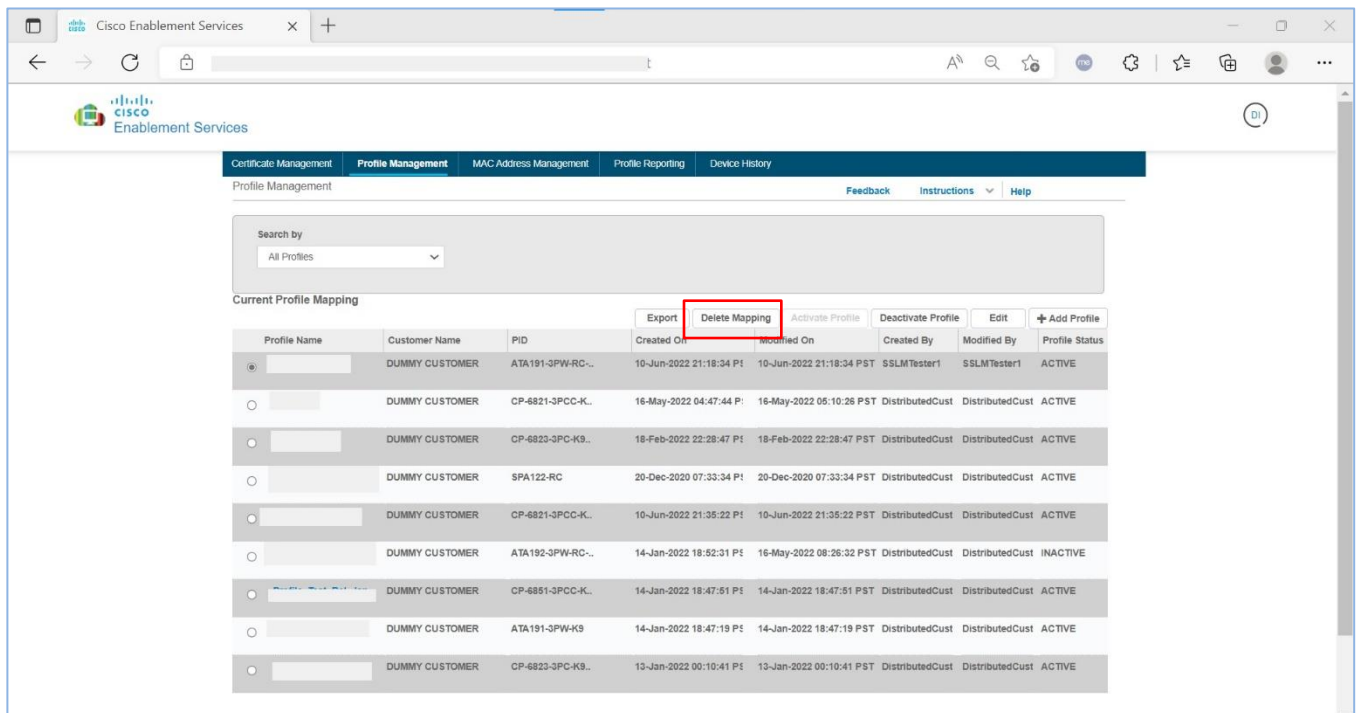
- On clicking 'Update Mapping' a success message will appear confirming the same.
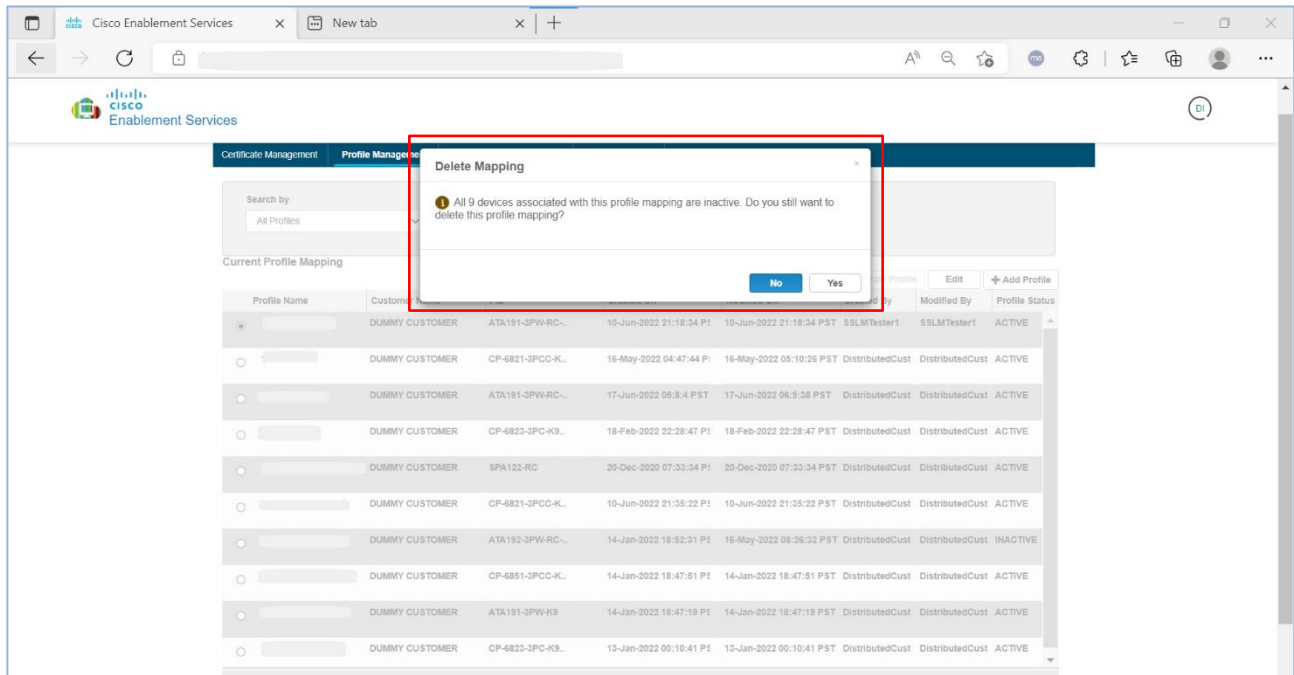

3. Delete Profile

- Select a profile name and click on 'Delete Mapping' button to delete the profile.

- A warning message stating that this profile is mapped with one or more devices and do you want to proceed with the profile deletion would be displayed.
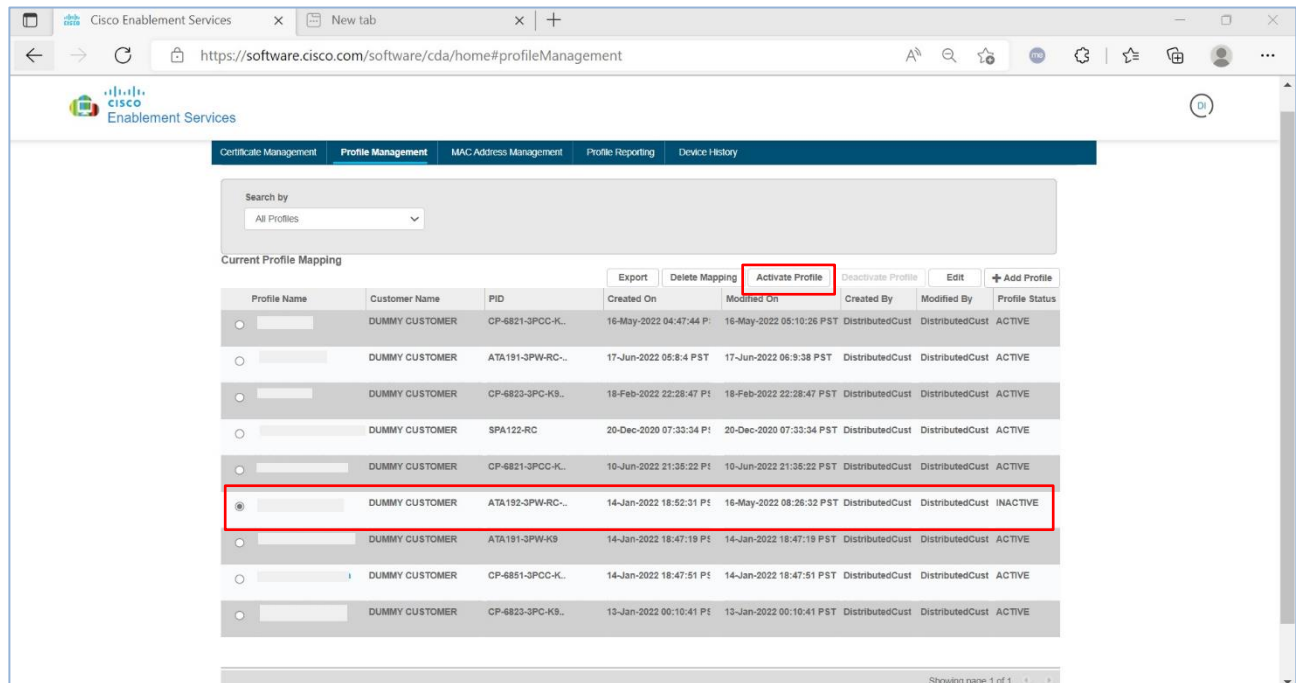

- Click 'Yes' to delete the profile. Click 'No' to close without any deletion of profile.
- On clicking 'Yes', a confirmation message will appear.
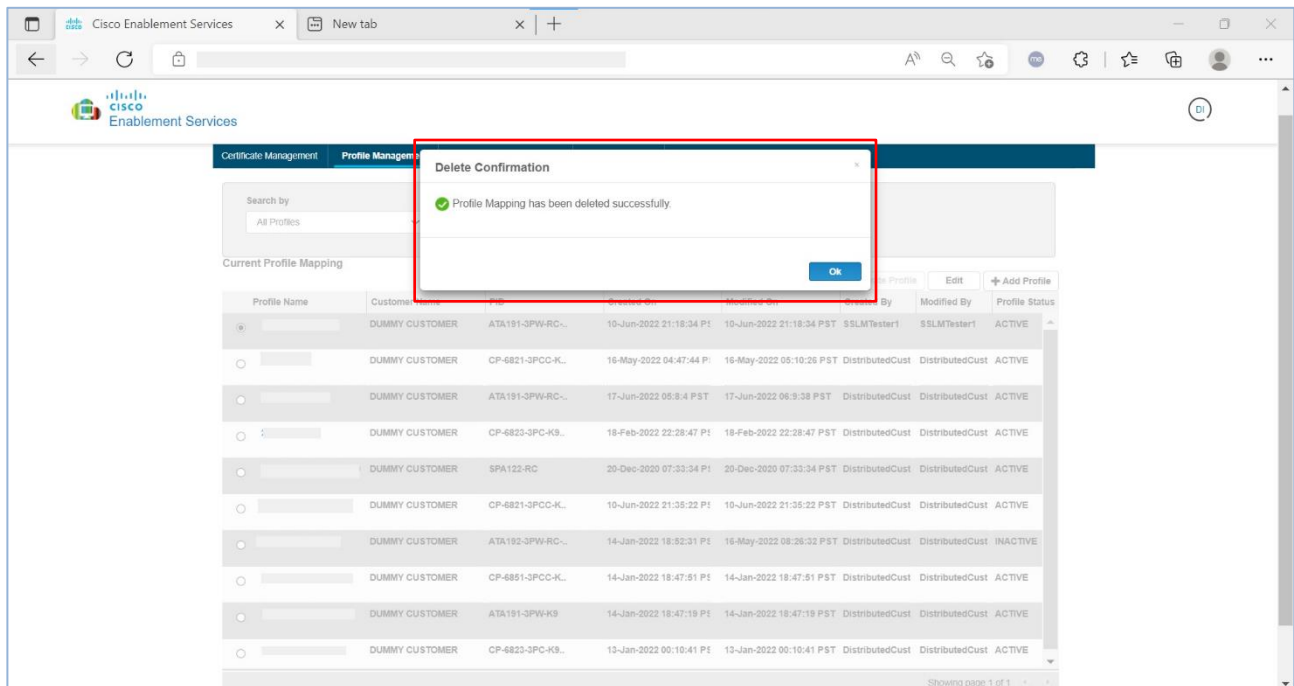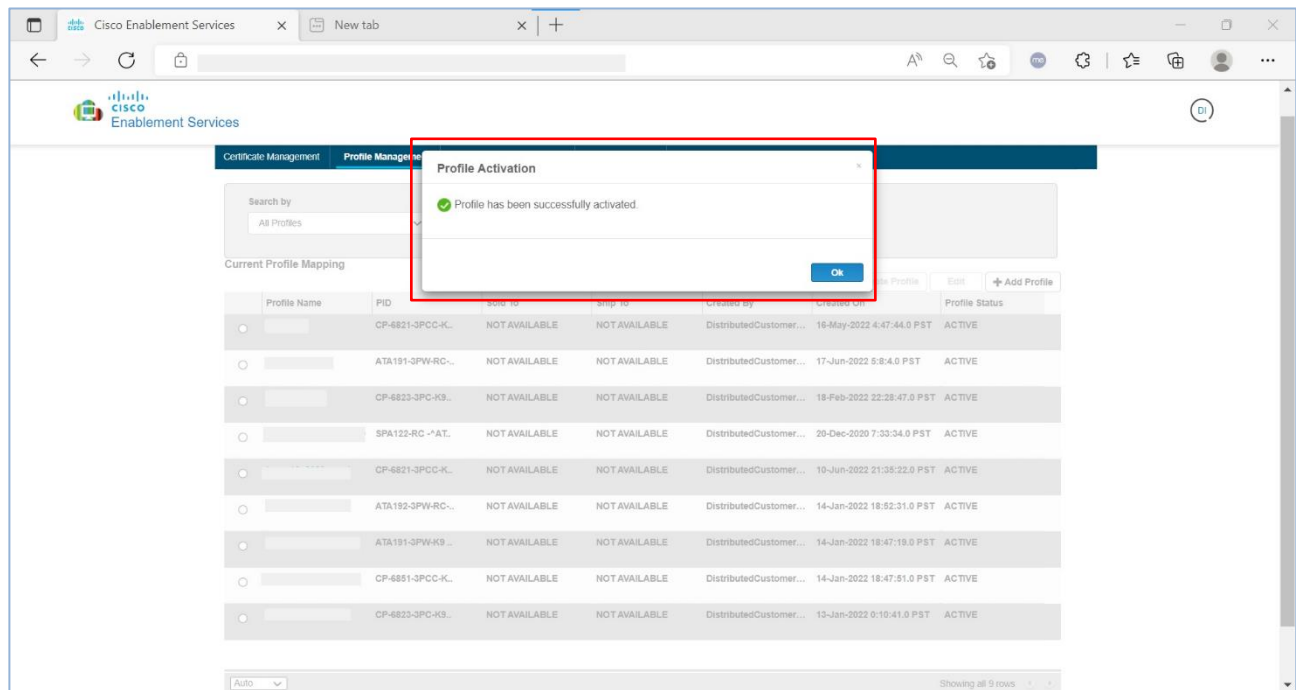
4. Activate Profile

- Select an Inactive profile and click on 'Activate Profile'. The setup will get activated.

- A confirmation message will appear.

5. Deactivate Profile

- Select an active profile to deactivate and click on 'Deactivate Profile'. The setup will get deactivated.

6. Search a Profile

- To search a profile, select 'Profile Name' in 'Search by'.
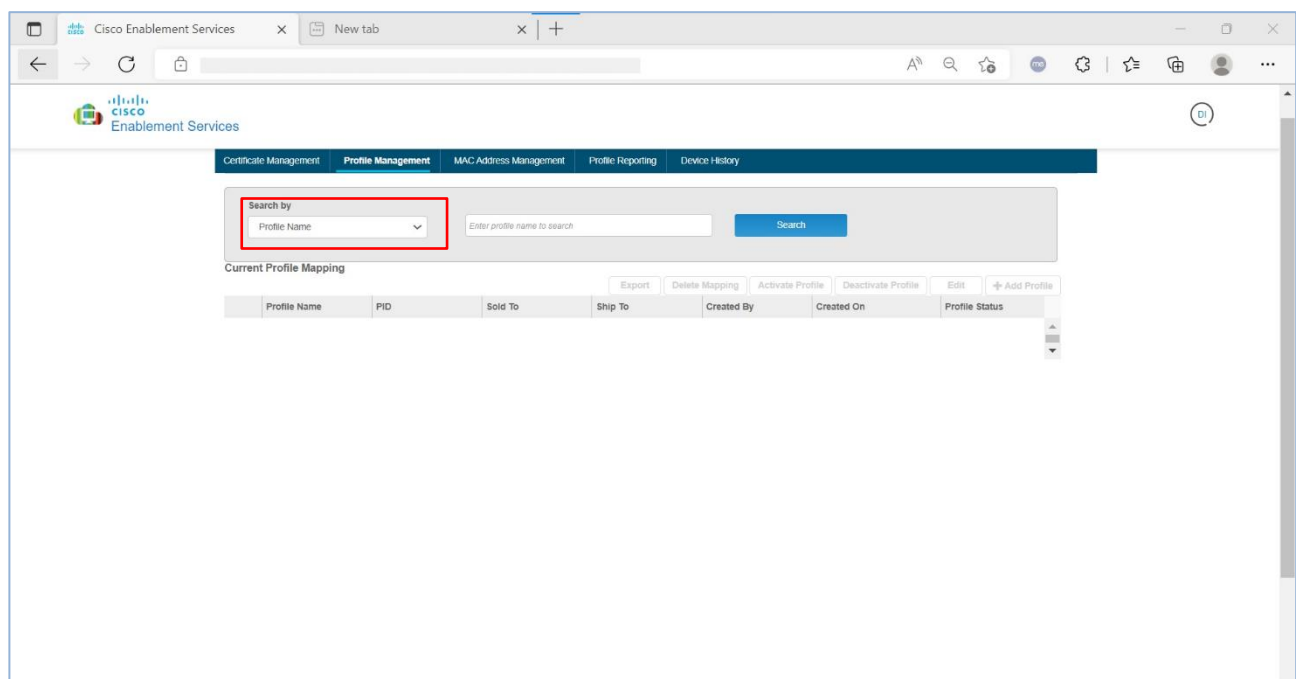
- Enter the name of a profile or select a profile from dropdown.
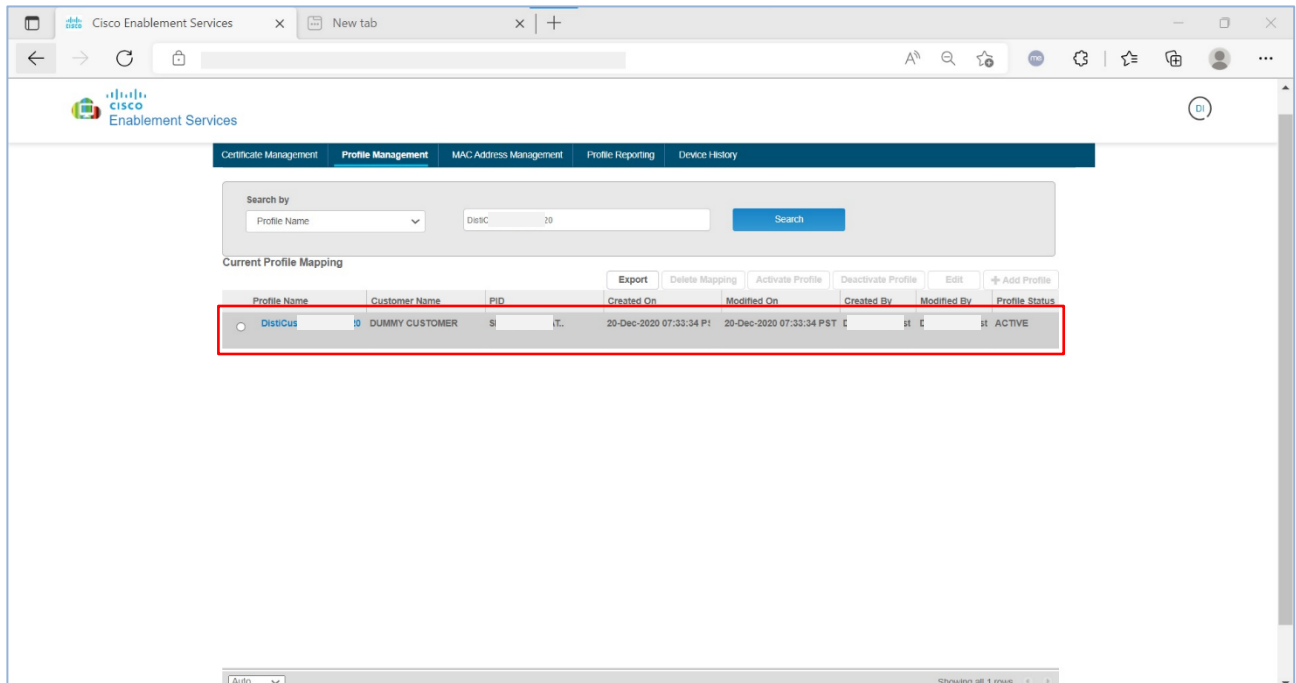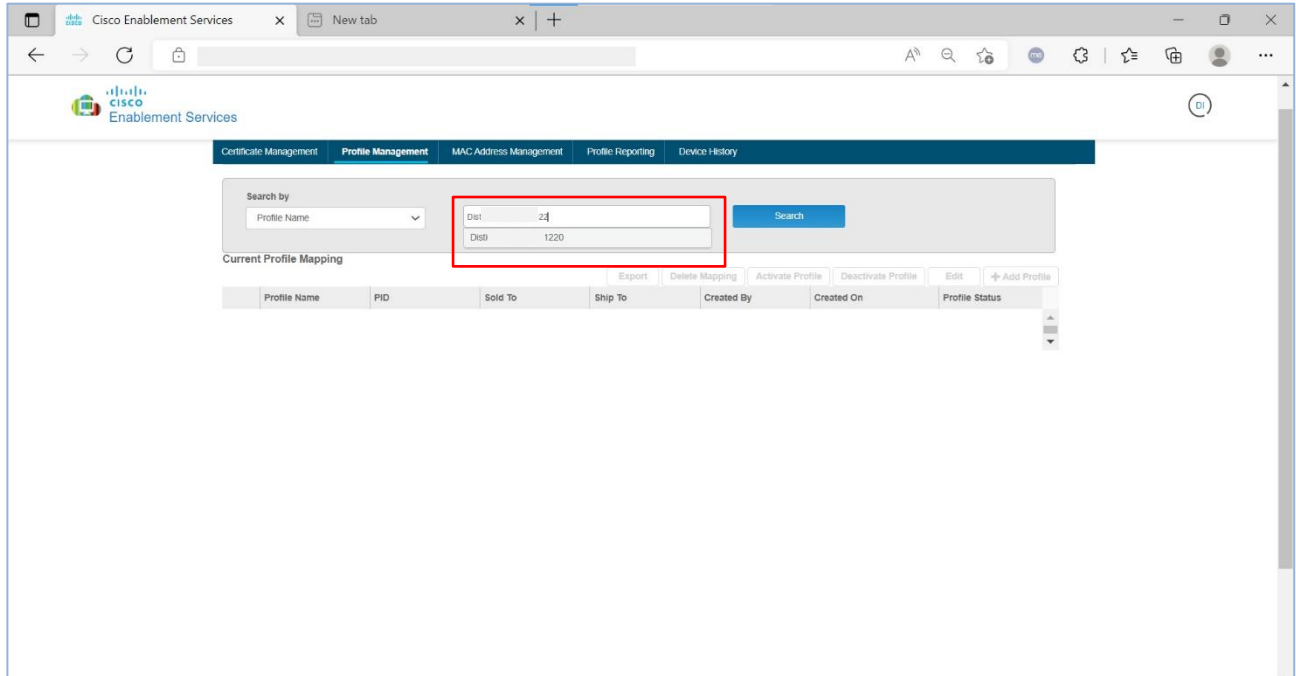
3.4 MAC Address management

Users can use 'MAC Address Management' tab to map their devices to a profile. Each device is mapped to profile to connect the device to a respective Service Provider. Users have option to map MAC addresses to a profile by entering manually or by uploading an excel file containing bulk MAC addresses.

- Click on 'MAC Address management' tab.
- Enter a MAC Address and click on 'Proceed'.

  OR

  Click on 'Switch to Multiple MAC Address' and upload excel file with multiple MAC Addresses for bulk operations; click on 'Proceed'.
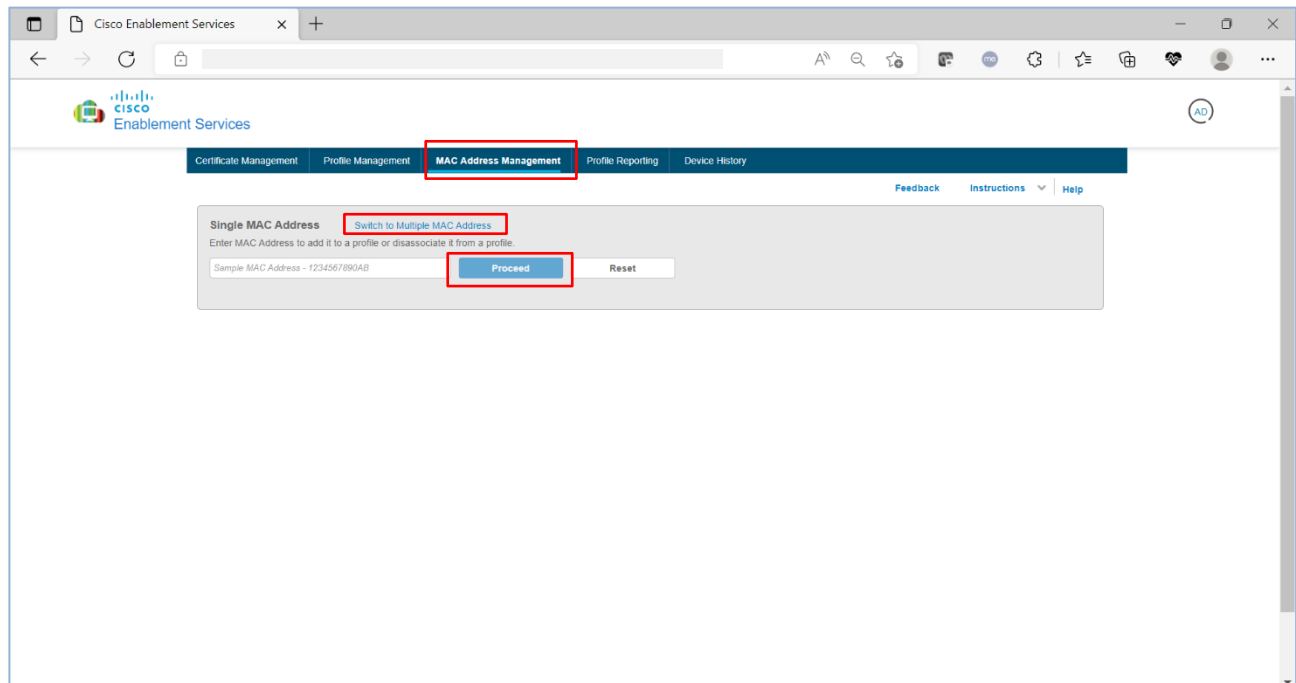
1. **Available**

- If the MAC address is not mapped to any profile and is in a valid format, the below pop-up will open. Click on 'Proceed' to map it to a profile.
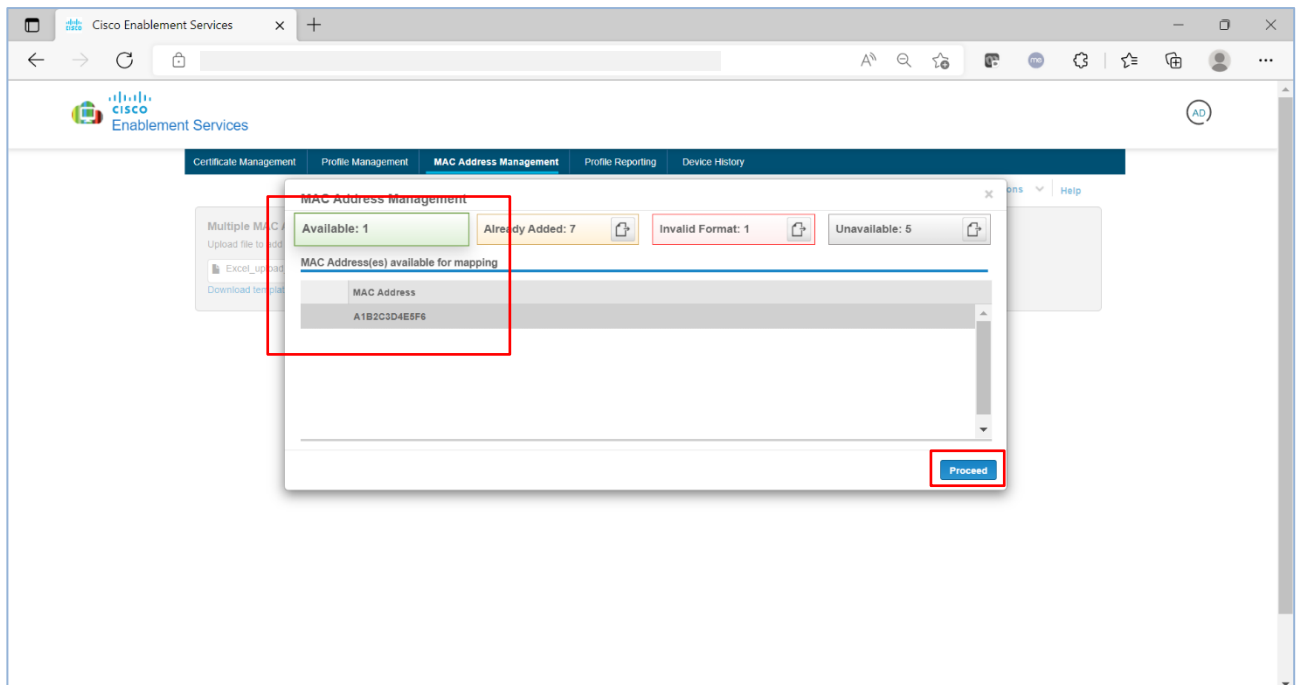
- Select any profile from the drop down.
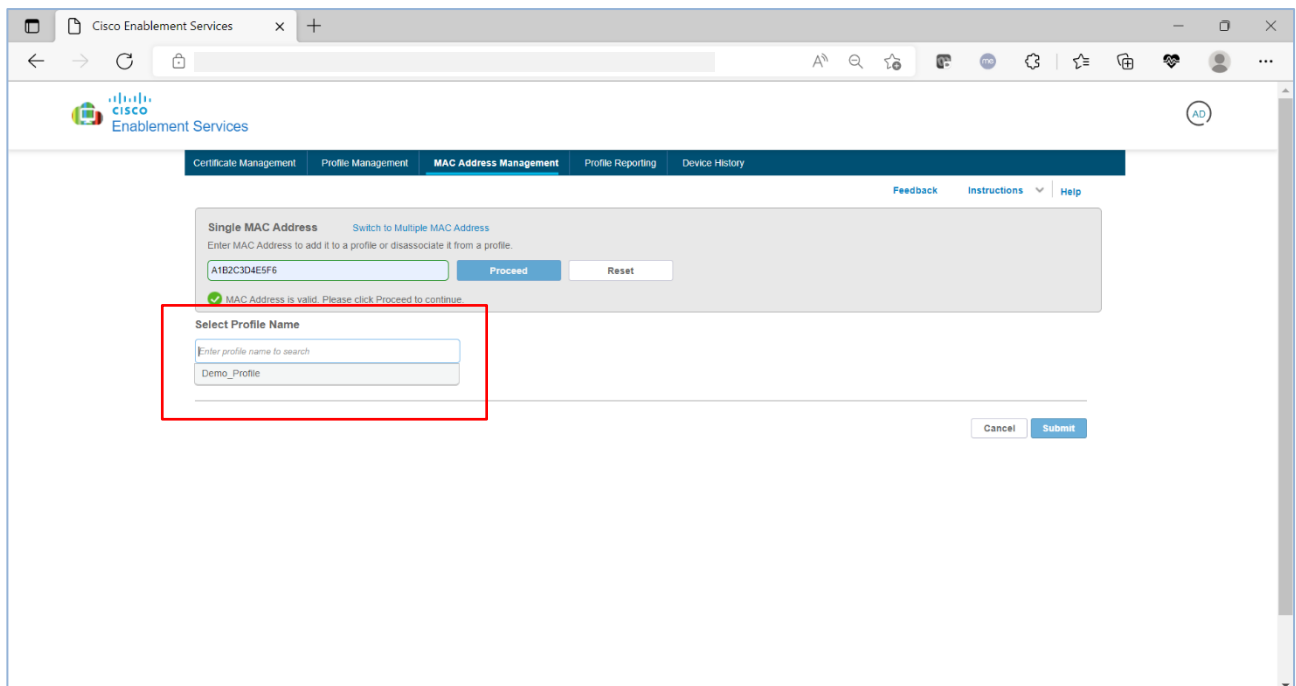
- All the setup profiles which can be associated to the MAC address will be displayed. Select one and click on "Submit' to complete the association.
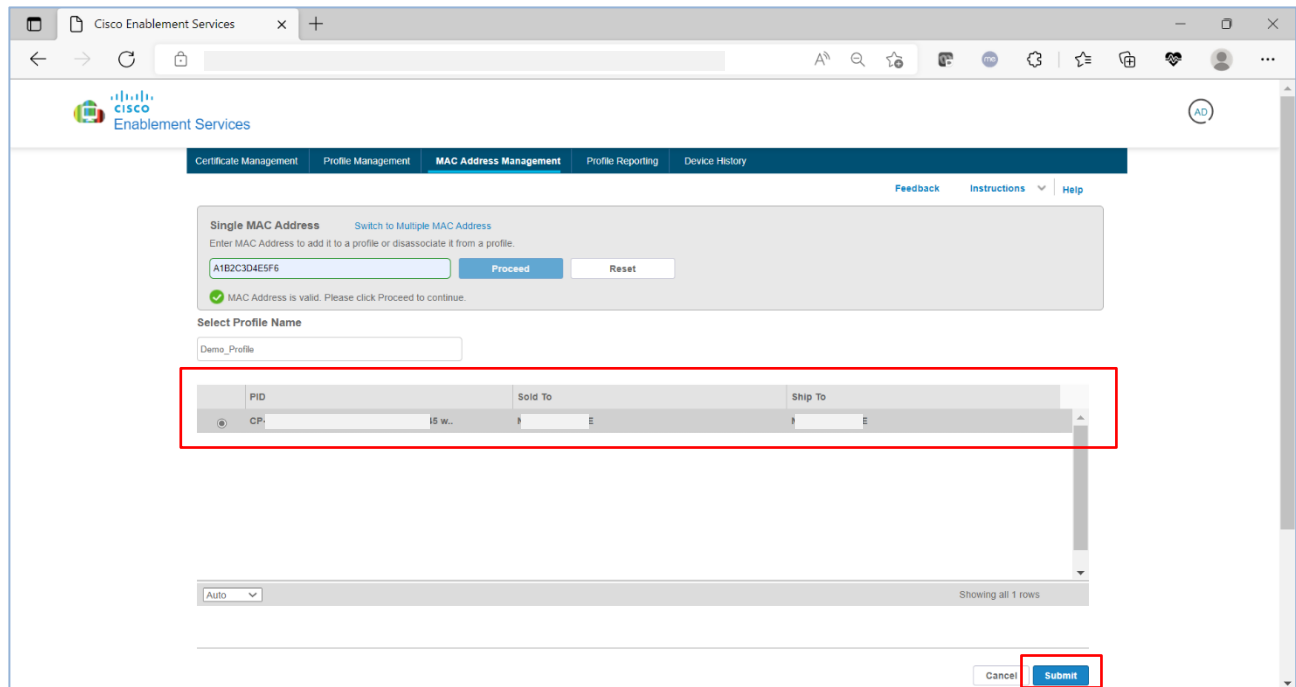
- A confirmation message will be displayed on successful addition.
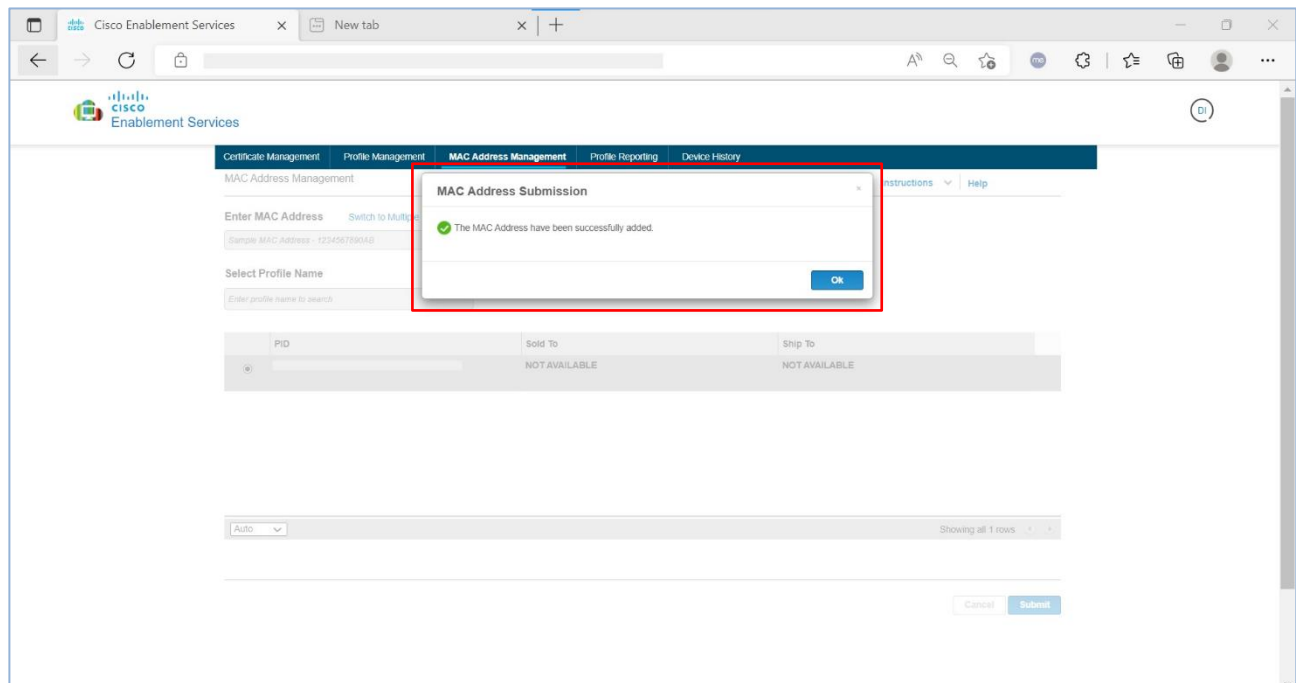
2. **Unavailable**

- If the MAC address is mapped to a profile that is owned by other users, the below pop-up will open. Please raise a case by clicking on "Raise Case" button to overwrite the mapping.
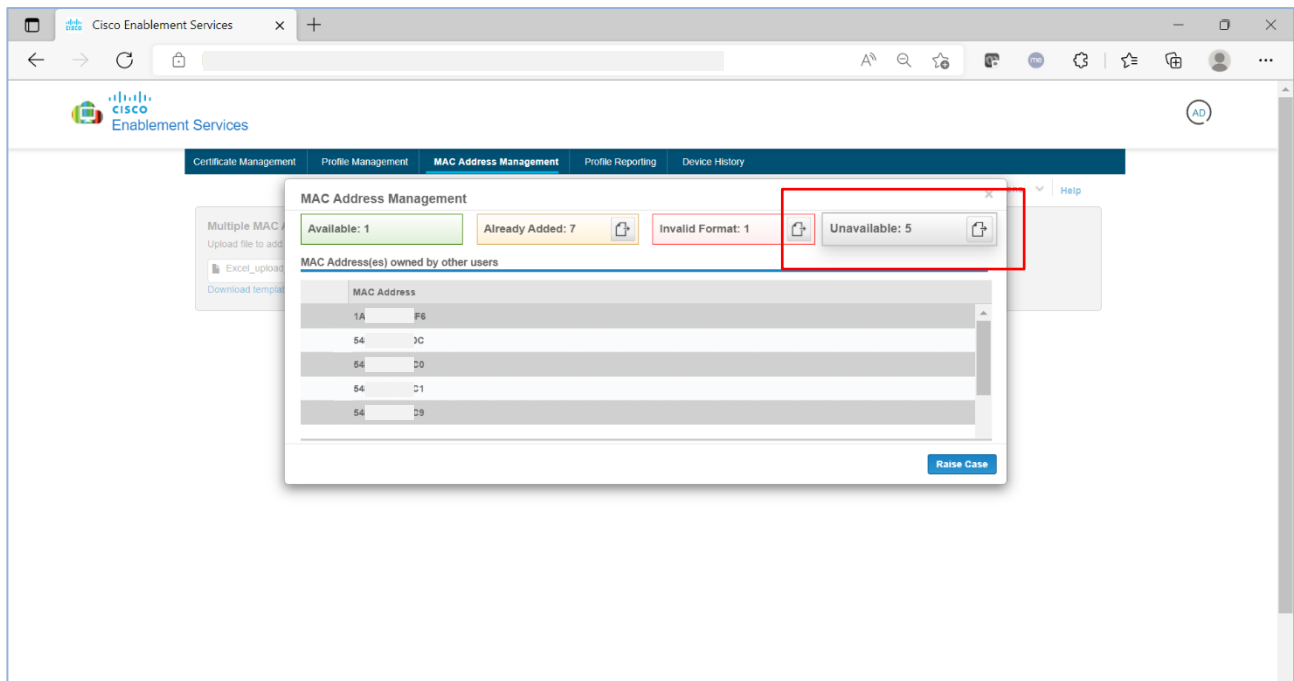
3. **Already Mapped**

- If MAC is mapped to another profile, below screen with the mapping details will be displayed.
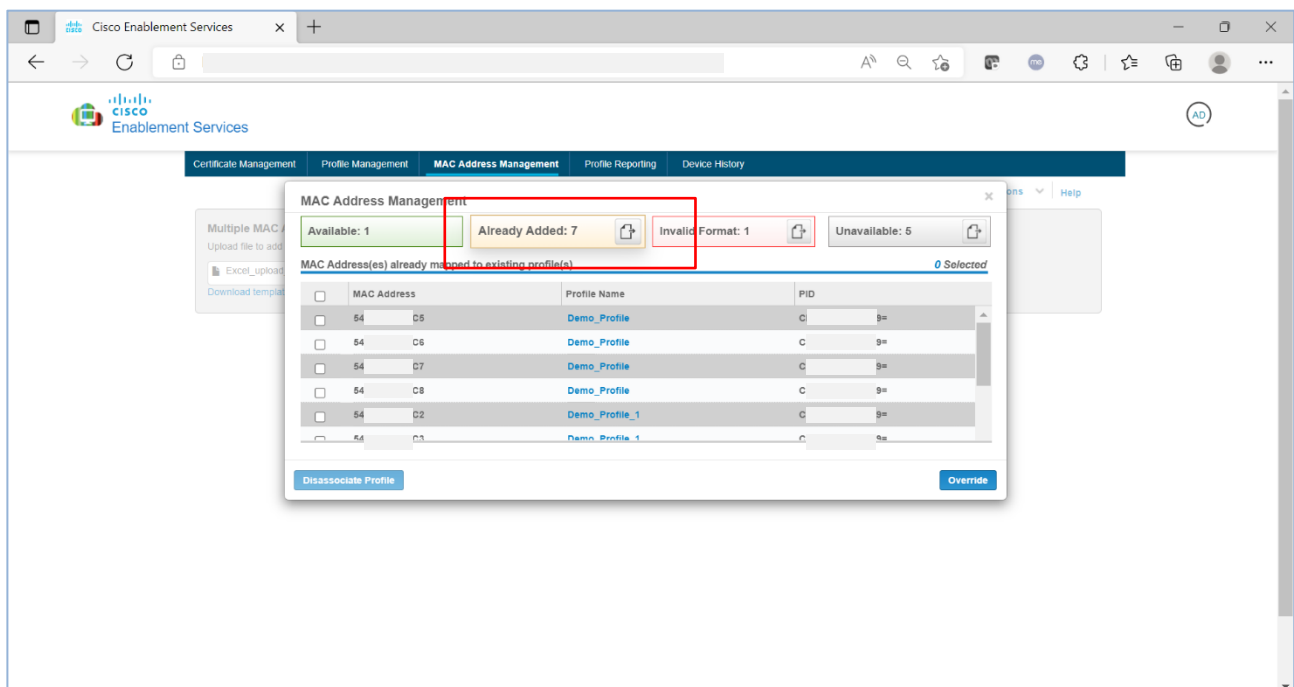
a. Override

- Select the checkboxes and click on "Override" button to override the mapping.
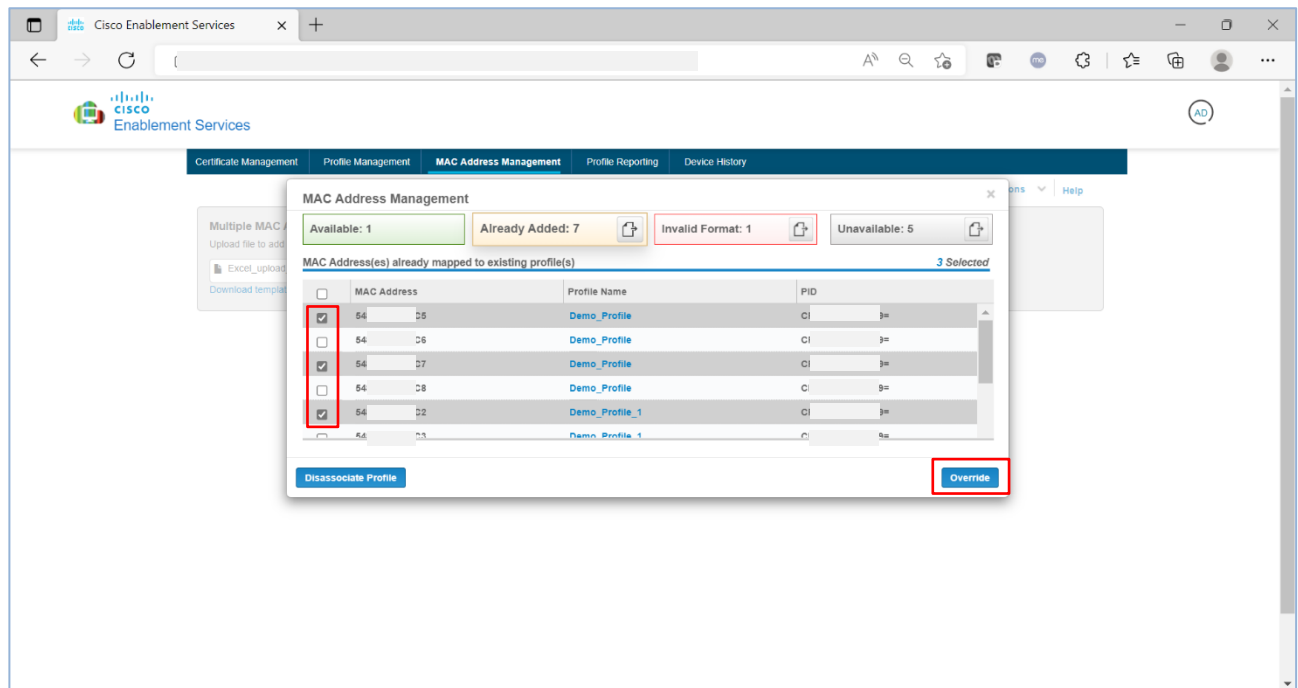
- Select a profile name from the Profile Name dropdown.
- All the setup profiles which can be associated to the selected MAC addresses will be displayed. Select one and click on "Submit' to complete the association.
- A confirmation message will appear.

b. Disassociate Profile

- Select the checkboxes and click on "Disassociate Profile" button to remove the mapping.
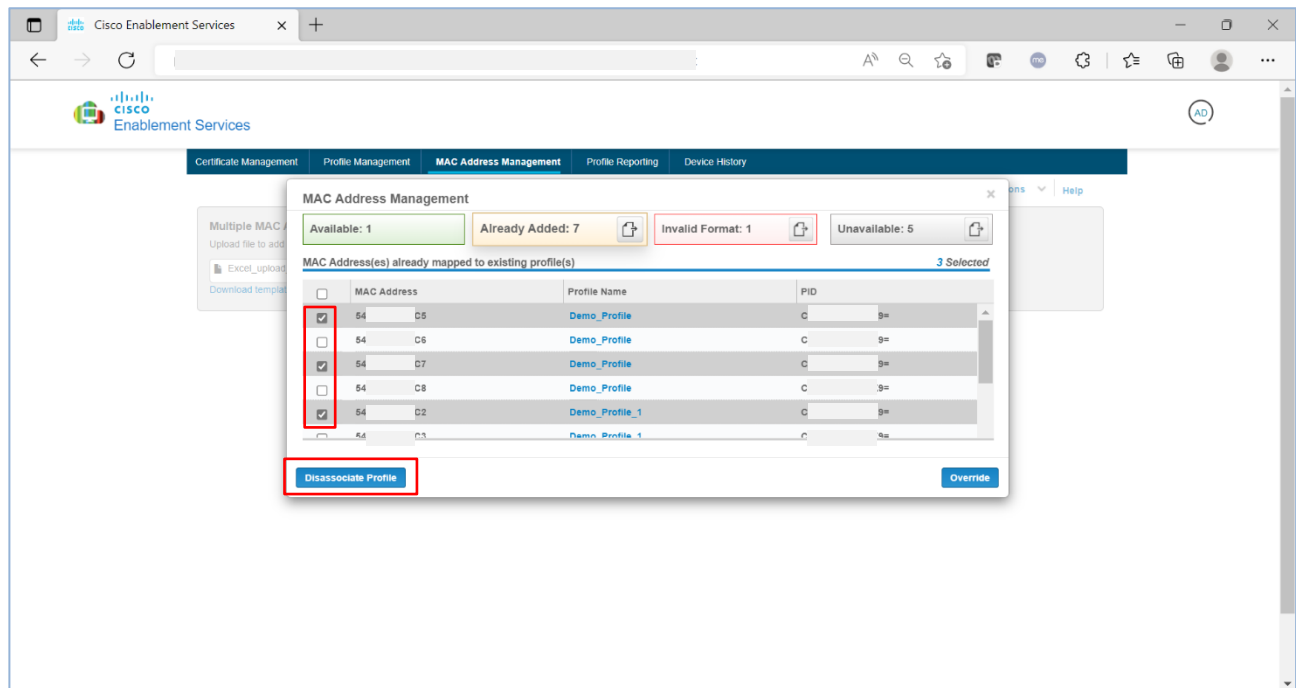
- A confirmation message will appear.
- The disassociated MAC addresses will be moved under 'Available' tab.

c. Download Profile Configuration

- Click on any 'Profile Name' to view the contents of the profile.
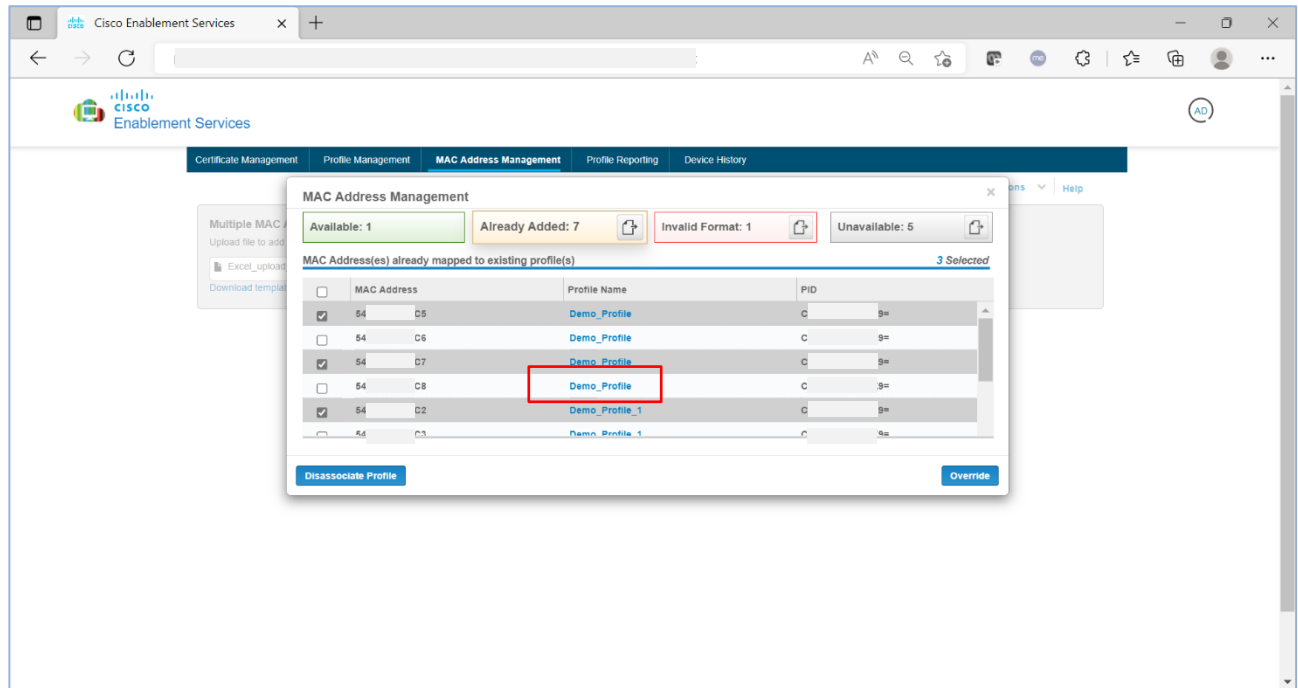
- The following 'Profile Configuration' pop-up will open. Click on 'Download Profile' to download the contents in the profile.

3.5   Profile Reporting

Users can use 'Profile Reporting' tab to check the details of profile and related attributes such as Sold to, Ship to, PID, Profile name and MAC Addresses mapped to the profile. Users can also see the profile content of the profile. Search is based on MAC Address and Profile name.
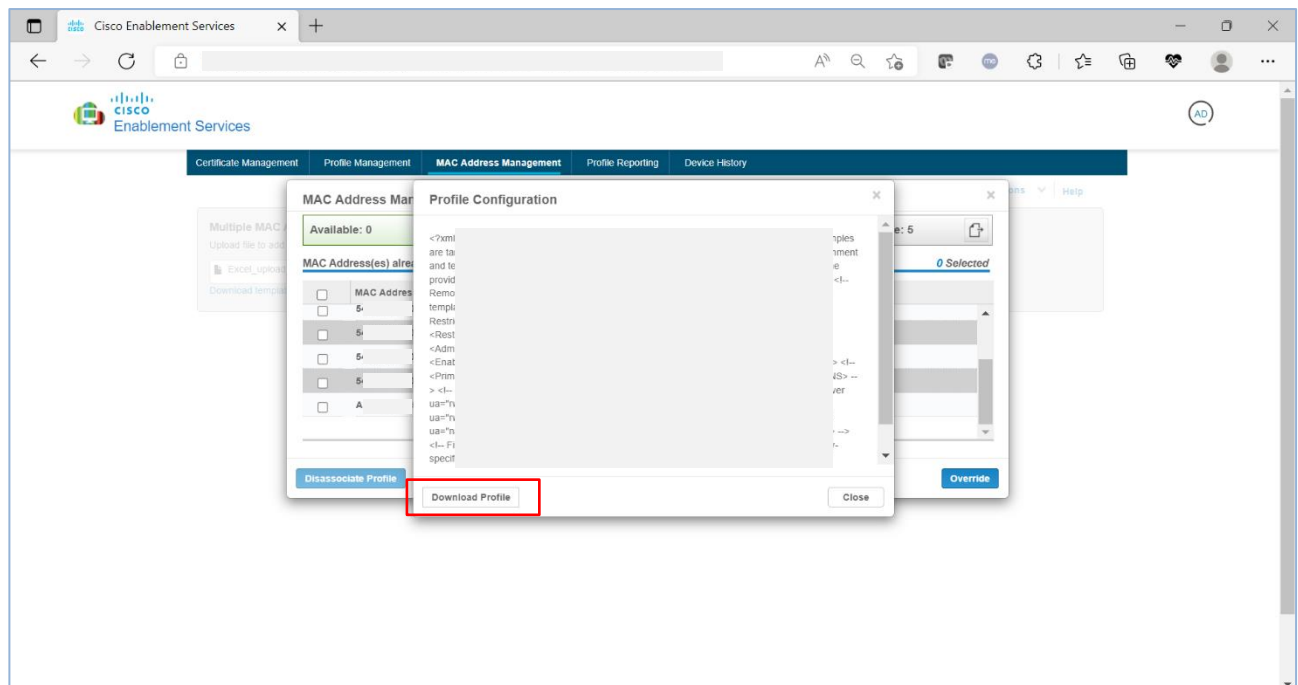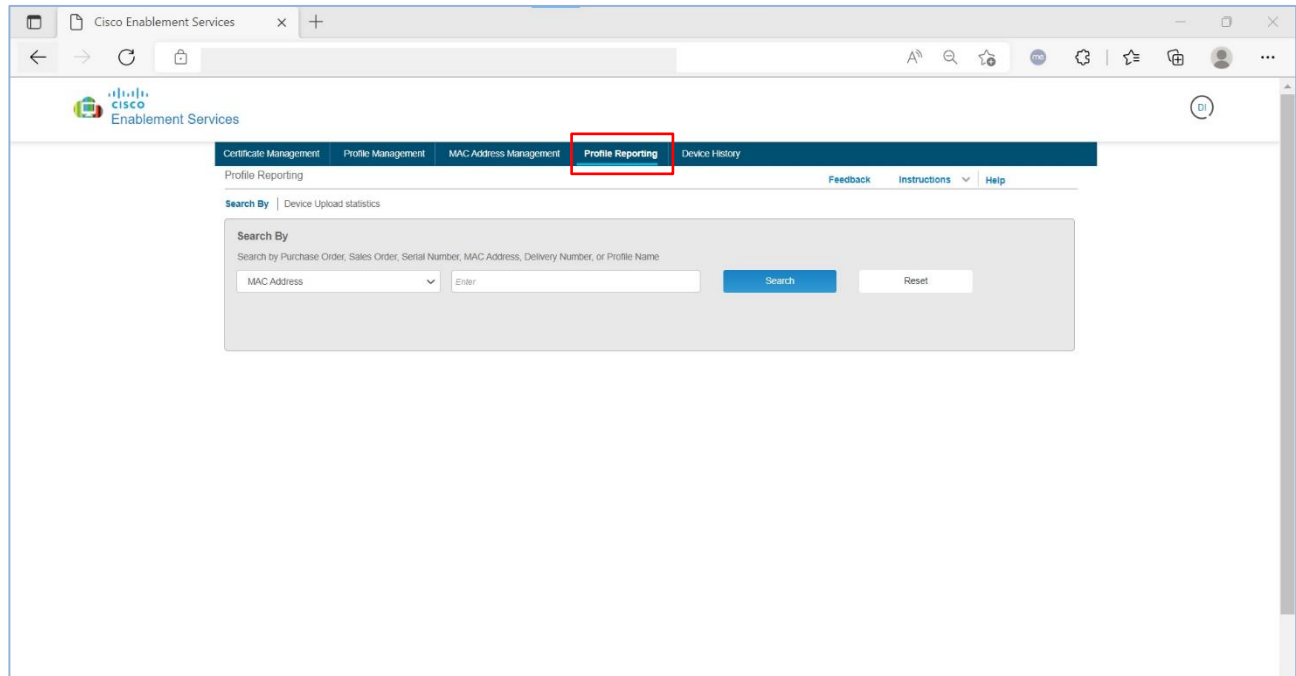
Users can also find the number of devices mapped during a time using the Device Upload Statistics tab. Users need to provide the date range to see the results.

- Click on 'Profile Reporting' tab to view the Profile Reporting page.

- Click on 'Search By' section to make a search based on a MAC Address or a Profile Name.
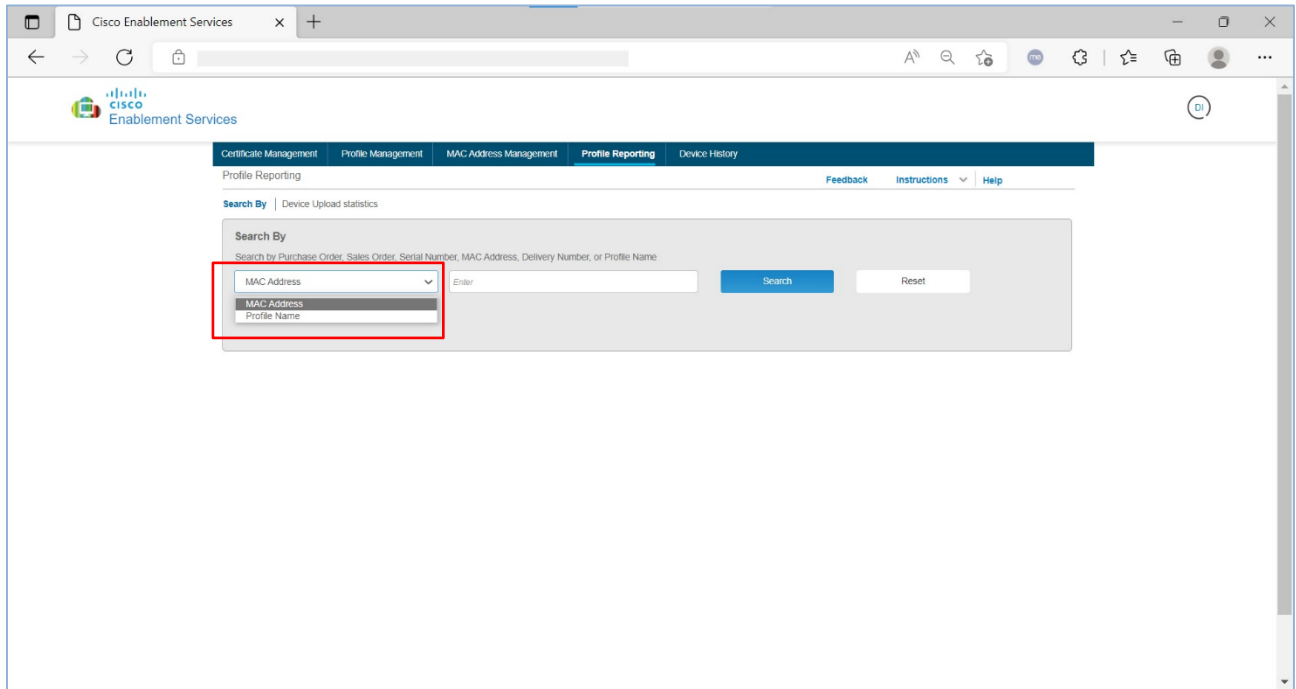
- Enter a value in the input box.
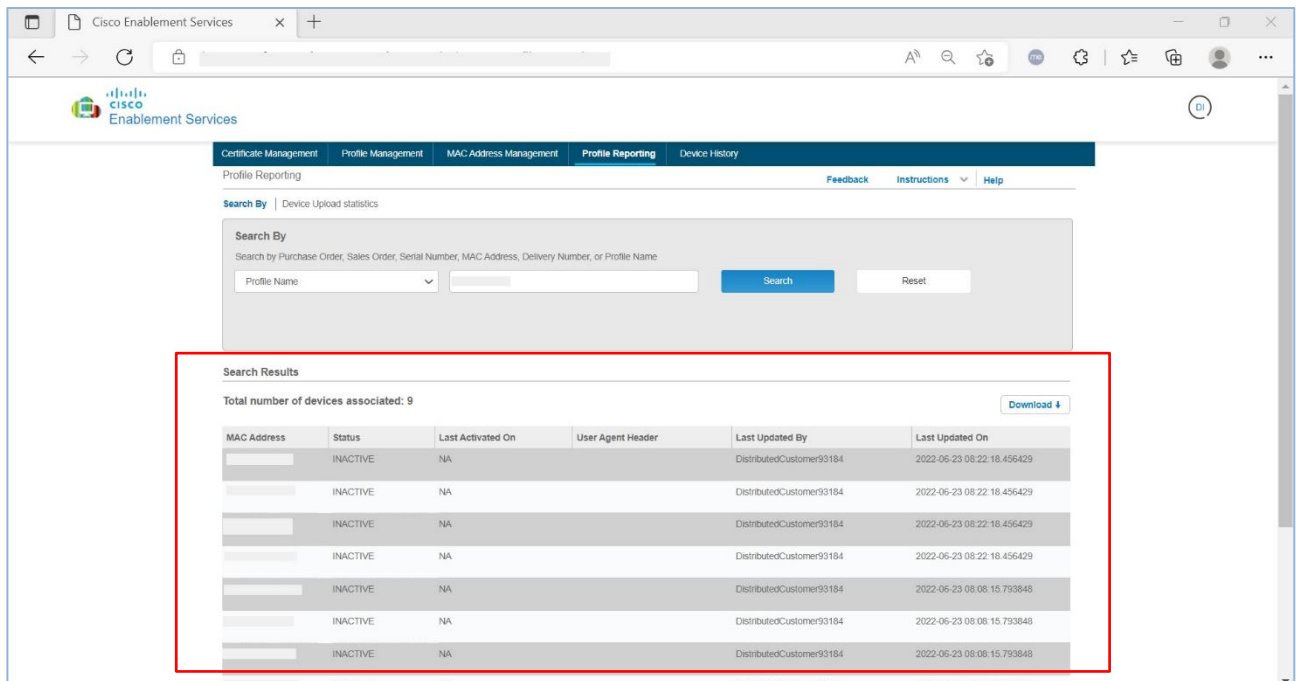- Click on 'Search' button to get the results.
- On click of search, search results will appear as shown in picture below. Click on profile name to see the profile content.
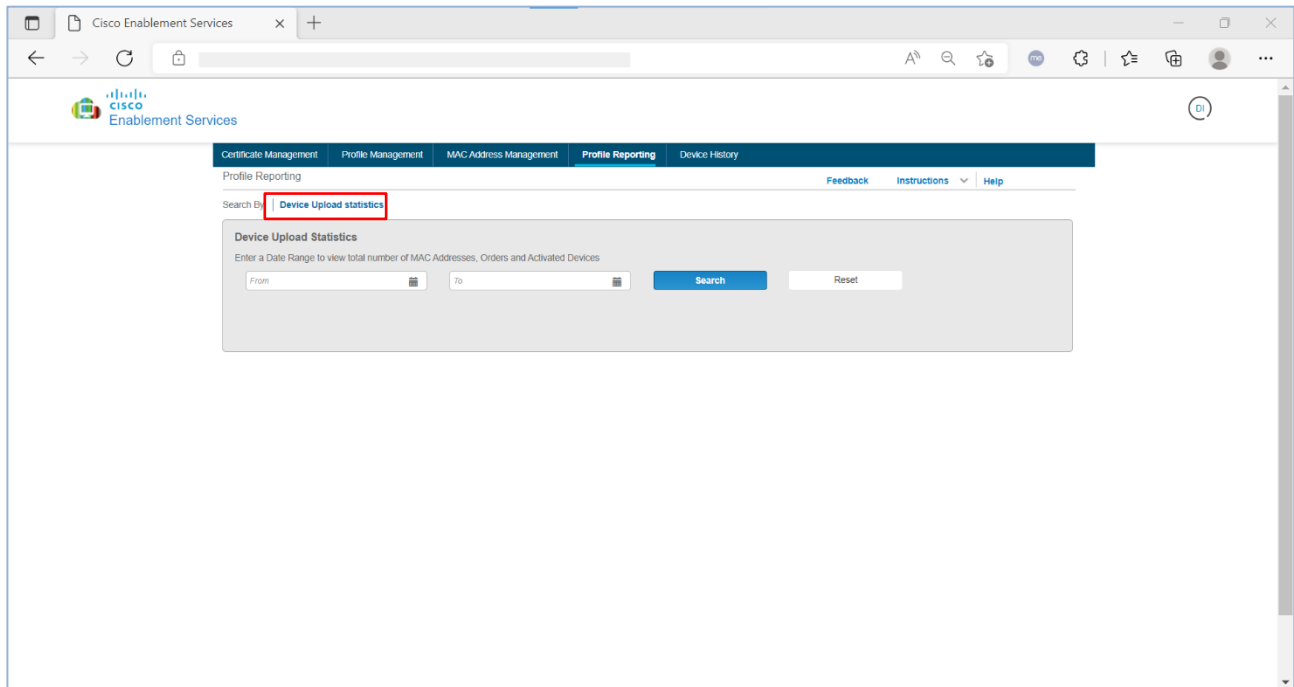
- Click on 'Export data to excel' link to download the table contents to an excel sheet.

- Click on 'Device Upload Statistics' section to get reports between different time intervals.

- Click on the calendar icon to select from date and to date to search the statistics between those dates.
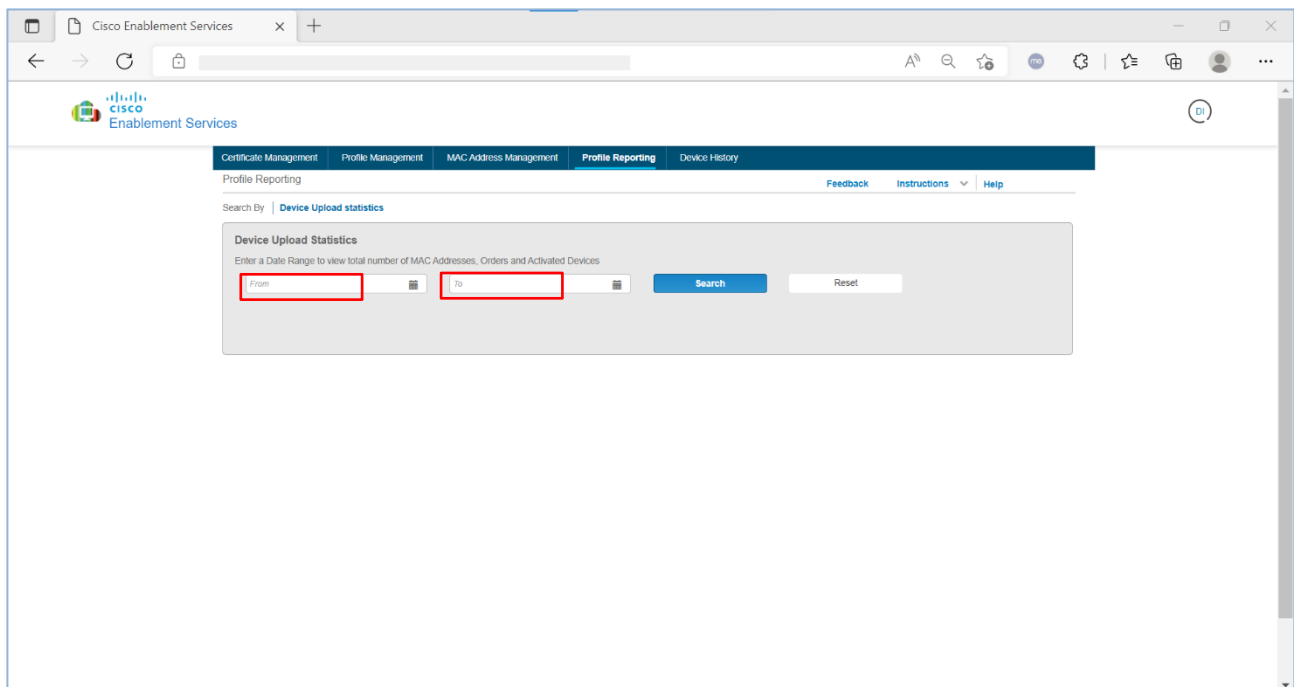
- After clicking 'Search' button, result will be shown. Click on the 'Download' button to download the file in .xls format.
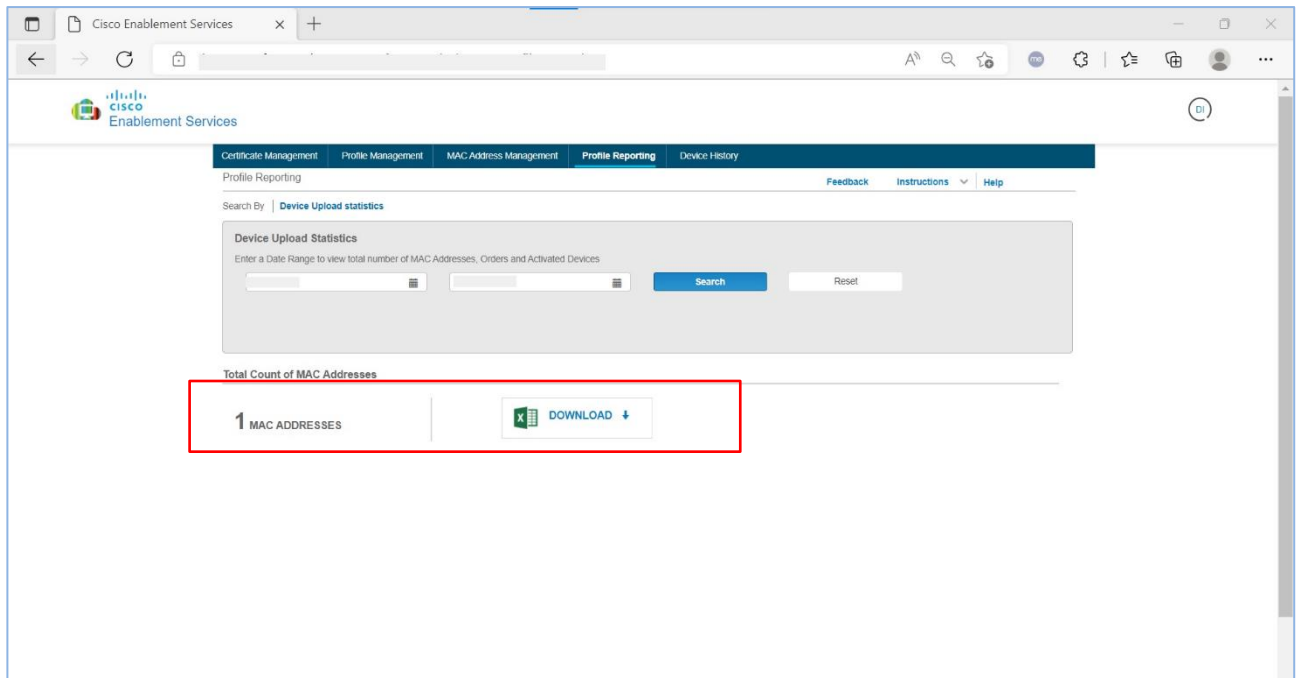
- If there are more than 50000 MAC address in the selected date range, then only the latest 50000 will be downloaded in the excel.
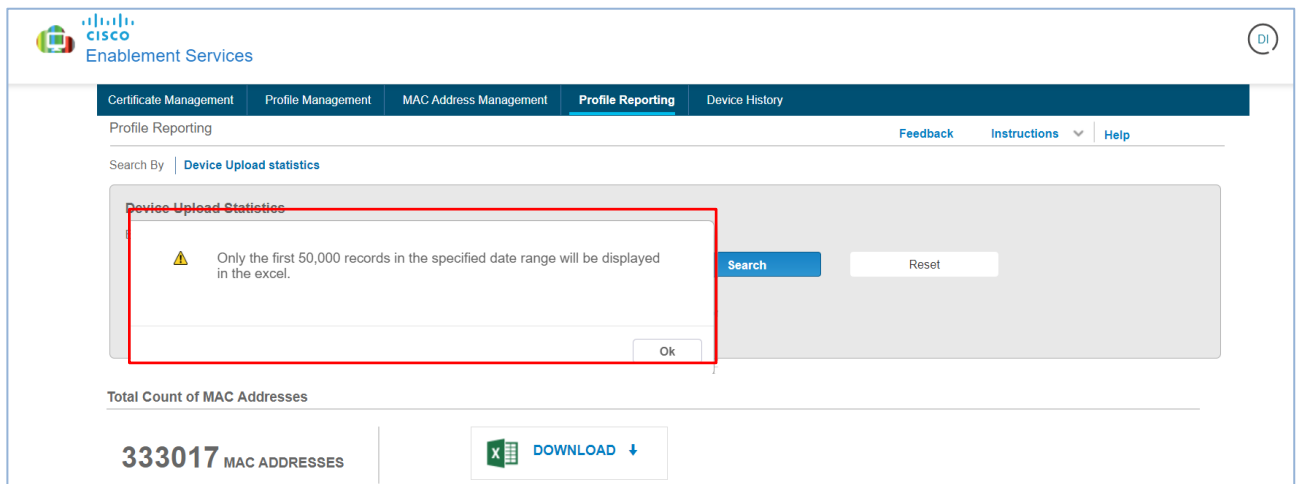
3.6   Device History

Users can use 'Device History' tab to view the history of MAC address and to find the status of the encryption of the devices. The MAC address of the device needs to be entered to see the results. The details of the MAC Address will be visible only if the user has access to the profile the MAC has been mapped to.

- Click on 'Device History' tab to view the device history page.
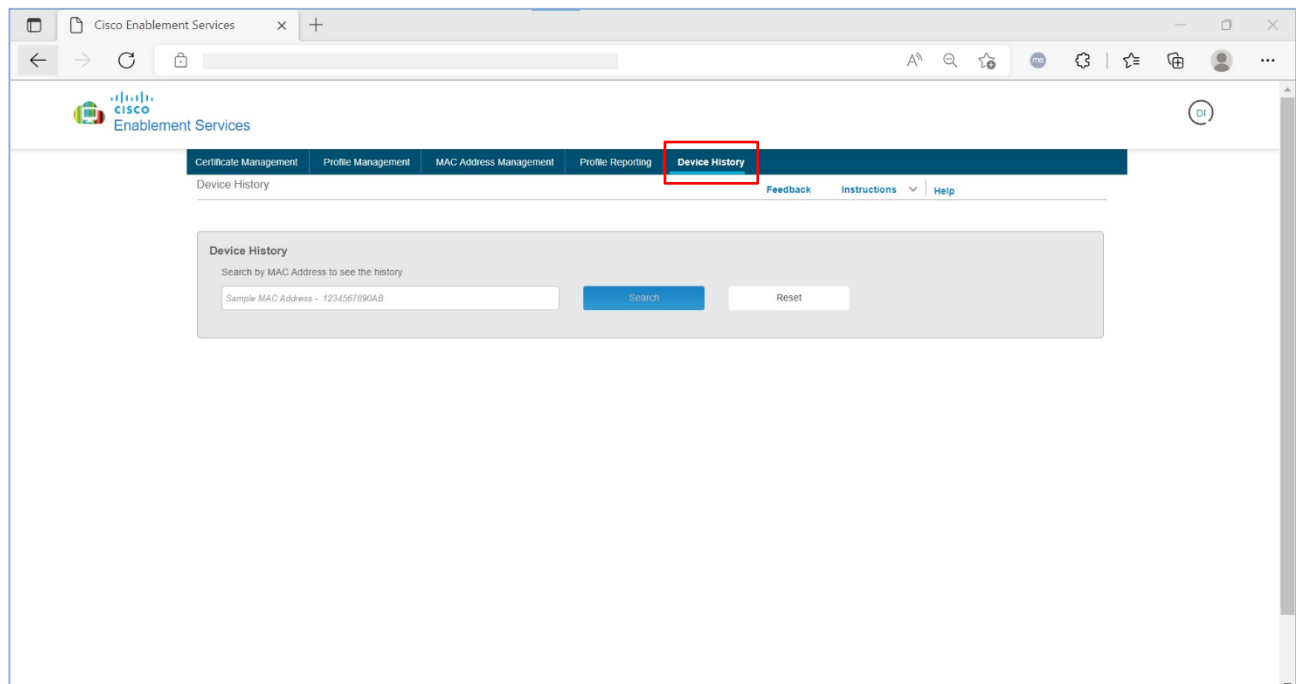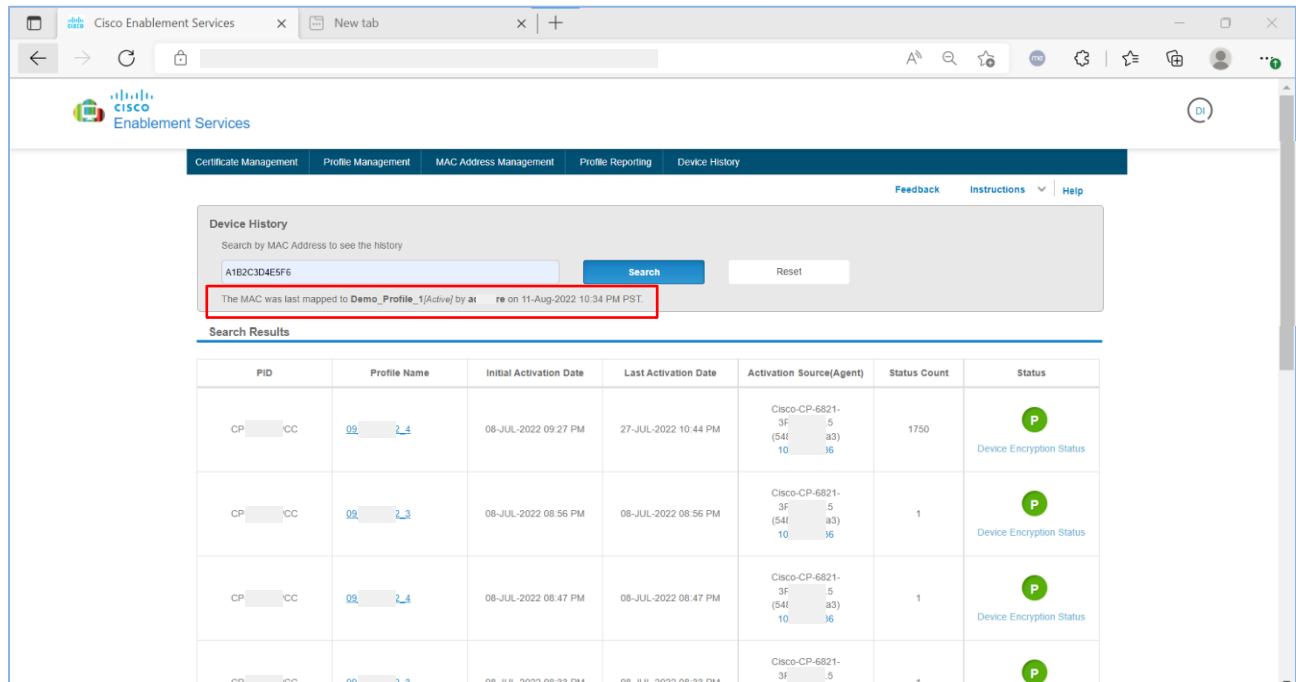

- Enter a MAC Address and click on 'Search' to view the details.

- Search results will appear as shown in picture below.
- The text below the MAC Address input box conveys the latest action performed on the MAC. It would be in the format:
    - The MAC was last mapped to <**profile name**> [<*profile status*>] by <**user id**> on <**time**> PST.

          OR

      The MAC was last disassociated from <**profile name**> [<*profile status*>] by <**user id**> on <**time**> PST.
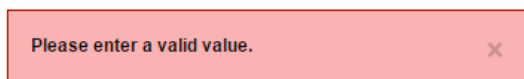
4   Error Messages

- Your session has timed due to inactivity. You must log in again to continue using Cisco Enablement Services Portal.
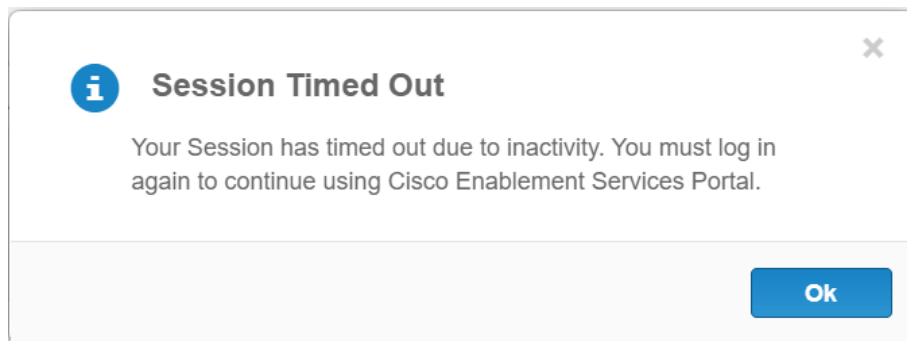
Resolution: Please click on ok button, it will redirect you to the login page.

- Please enter a valid value.

Resolution: The inputs entered is incorrect. Please enter a correct input value.

Operational Support

If you have support questions about the web portal, please open a case via [Support Case Manager](#) (SCM). This will allow for faster routing of issues and resolution. To learn more on how to open a case in SCM, click [here](#).