How can I generate a certificates on the Cisco Device Activation (CDA) portal?

Contents

For External Customer / Partner Use Only: These instructions are provided to help customers / partners perform the following action themselves to resolve the issue. If the customer / partner runs into issues following the instructions, please have them open a case with licensing support (https://www.cisco.com/go/scm) To help resolve. Please **DO NOT** perform these actions yourself if you are an internal Cisco resource outside of the Licensing Support team.

Before You Start Ensure You Have the Following:

- Active Cisco.com account

- User needs to have CDA Portal Access
- User needs to have Certificate Management Access

Step 1: Click on Certificate Management Link Cisco Enablement Services.

Step 2: Click on '**Certificate Management**' Tab.

Step 3: Click on **'Sign CSR**' Tab.

Step 4: Select a product from the '**Select Product**' drop down.

Step 5**: 'Encryption Type**', '**Sign in Duration**' and the CSR File attributes will be enabled only upon selecting the Product.

Step 6: Select the type of encryption from the under the '**Encryption Type**' drop down (MD5/SHA1/SHA256). By default, the value selected is SHA1.

Step 7: Select the duration for the certificate from the '**Sign-In Duration**' drop down (1 year/2 years/3 years/5 years/180 days).

Step 8: The '**Sign in Duration**' for the SHA1 and MD5 encryption is defaulted to 180 days and limited to 1 year. Only for the SHA256 type of encryption the certificates can be signed for durations of 180 days/ 1 year/ 2 years/ 3 years/ 5 years.

Note: When MD5 encryption is selected below warning message will pop up to confirm the encryption selection

Step 9: Upload the **CSR file** in the CSR File field.

Step 10: Click on '**Sign Certificate Request**' to sign the certificate file that was uploaded. File will now be signed

Step 11: Once the certificate is signed successfully the message, 'C**ertificate is signed successfully**' will appear on the screen. Click **OK**.

Step 12: Click on '**Download**' to download the signed certificate.

Step 13: Under '**Certificate Receive Method**' - Enter an email address in the email address field to send the signed certificate to an email address.

Step 14: 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.

Troubleshooting:

If you experience an issue with this process, that you cannot address, please open a case at Support Case Manager

For feedback on the content of this document, please submit here.