Frequently Asked Questions

Certificate Provisioning Portal FAQs, Release 2.7

Revised: November 20, 2019

Certificate Provisioning Portal FAQs

What does the Certificate Provisioning Portal do?

The Certificate Provisioning Portal issues certificates to devices that cannot go through the onboarding flow. For example, devices such as point-of-sale terminals cannot go through the BYOD flow and need to be issued certificates manually. The Certificate Provisioning Portal allows a privileged set of users to upload a certificate request for such devices; generate key pairs, if needed; and download the certificate.

Why can't I log in?

To log in to the Certificate Provisioning Portal, your user account should belong to a specific Identity Group that your administrator has configured for the Certificate Provisioning Portal. Please contact your administrator for support.

How do I change my password?

You can change your password from the Certificate Provisioning Portal only if you are a Cisco ISE internal user (your user information should be present in the Cisco ISE internal database). To change your password:

1. Log in to the Certificate Provisioning Portal using your credentials.
2. Click the **Account** menu drop-down list at the right upper corner.
3. Click **Change Password**.
4. Follow the instructions on screen to change your password.

How can I generate a single certificate with attributes?

To generate a single certificate with attributes:

1. Log in to the Certificate Provisioning Portal with your credentials.
2. From the **I want to** drop-down list, choose generate single certificate (no certificate signing request).
3. Enter your username (the username that you used to log in to the Certificate Provisioning Portal) in the **Common Name** field.
4. Enter the MAC address of the device for which you are requesting the certificate in the **Subject alternative name (SAN)** field.
5. Choose a certificate template.
6. (Optional) Enter a description.
7. Choose the certificate download format.
8. Enter a password to secure the client certificate. At the time of installing this certificate on the device, you must enter this password.
9. Click **Generate**.

A certificate zip file is generated that you can download to your system.

What is Common Name (CN)?

The authentication server uses the value that is presented in the Common Name field in the client certificate to authenticate a user. In the Common Name field, enter the username (that you used to log in to the Certificate Provisioning Portal).

What is Subject Alternative Name or SAN? What are the formats that we support?

Subject Alternative Names (SAN) is an X.509 extension that allows various values to be associated with a security certificate. Cisco ISE, Release 2.0 supports MAC address only. Hence, in the SAN/MAC address field, enter the MAC address of your device in any one of the following formats:

- 00-11-22-33-44-55
- 00:11:22:33:44:55
- 0011.2233.4455
- 001122-334455
- 001122334455

What is a certificate template?

A certificate template is used by the Certificate Authority (CA) to issue a certificate to an end entity. The certificate template is created by a Cisco ISE administrator, who defines a set of fields that the CA uses when validating a request and issuing a certificate. Fields such as the Common Name (CN) are used to validate the request (CN should match the username)). Other fields are used by the CA while issuing the certificate.

What are the available certificate formats?

You can choose to download the end entity certificate in any one of the following formats. The term, end entity, refers to the user/device to whom the certificate is issued.

- PKCS12 format (including certificate chain; one file for both the certificate chain and key): A binary format to store the root CA certificate, the intermediate CA certificate(s), and the end entity's certificate and private key in one encrypted file.
- PKCS12 format (one file for both certificate and key): A binary format to store the end entity certificate and the private key in one encrypted file.
- Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain): The root CA certificate, the intermediate CA certificate(s), and the end entity certificate are represented in the PEM format. PEM formatted certificates are BASE64-encoded ASCII files. Each certificate starts with the "-------BEGIN CERTIFICATE-----" tag and ends with the "-----END CERTIFICATE-----" tag. The end entity's private key is stored using PKCS8 PEM and starts with the "----------BEGIN ENCRYPTED PRIVATE KEY-----" tag and ends with the "-----END ENCRYPTED PRIVATE KEY-----" tag.

- Certificate in PEM format, key in PKCS8 PEM format: The end entity certificate is represented in the PEM format. PEM formatted certificates are BASE64-encoded ASCII files. Each certificate starts with the "-------BEGIN CERTIFICATE-----" tag and ends with the "-----END CERTIFICATE-----" tag. The end entity's private key is stored using PKCS8 PEM and starts with the "----------BEGIN ENCRYPTED PRIVATE KEY-----" tag and ends with the "-----END ENCRYPTED PRIVATE KEY-----" tag.

Why do I need a certificate password? Are there any password rules that I must follow?

You need a certificate password to secure your certificate. You must supply the certificate password to view the contents of the certificate and to import the certificate on a device. Your password must conform to the following rules:

- Password must contain at least 1 uppercase letter, 1 lowercase letter, and 1 digit
- Password must be between 8 and 15 characters long
- Allowed characters include A-Z, a-z, 0-9, _, #

What is a Certificate Signing Request or CSR? How do I obtain it?

A certificate signing request (CSR) is a request sent from an end entity (user/device) to a Certificate Authority (CA) requesting for a certificate. The CSR contains important information that identifies the end entity (such as Common Name, Subject Alternative Name, Department Name, and so on). OpenSSL is one of the most popular tools used to generate a CSR. Contact your administrator for information on how to obtain a CSR.

How can I obtain a single certificate with CSR?

To generate a single certificate with CSR with attributes:

1. Log in to the Certificate Provisioning Portal with your credentials.
2. From the **I want to** drop-down list, choose generate single certificate (with certificate signing request).
3. Enter the CSR details.
4. Choose a certificate template.
5. (Optional) Enter a description.
6. Choose the certificate download format.
7. Enter a password to secure the client certificate. At the time of installing this certificate on the device, you must enter this password.
8. Click **Generate**.

A certificate zip file that includes a CSR is generated. Download it to your system.

Can I make a bulk certificate request?

Yes. You can make bulk certificate request by creating a CSV file and uploading it to the Certificate Provisioning Portal.

How do I create the CSV file for bulk certificate request? How many certificates can I obtain in a single request?

To create the CSV file for bulk certificate request:

1. Log in to the Certificate Provisioning Portal using your credentials.
2. From the **I want to** drop-down list, choose generate bulk certificates.
3. Click **Download CSV template here**. The CSV template is downloaded to your system.
4. Open the downloaded file in a spreadsheet such as MS Excel.
5. Enter the CN and SAN values for the devices, one row for each device.
6. Save the file.
7. From the Certificate Provisioning Portal, click **Upload**.
8. Click **Browse** and select the CSV file from your system.
9. Choose a certificate template.
10. (Optional) Enter a description.

11. Choose the certificate download format.
12. Enter a password to secure the client certificate. At the time of installing this certificate on the device, you must enter this password.
13. Click **Generate**.

A certificate zip file containing all the certificates is generated. Download it to your system.

In a bulk certificate request, you can request for a maximum of 500 certificates.

How can I cancel an existing bulk certificate request?

When a bulk certificate request is in progress, click **Cancel** from the Certificate Generation Status page.

Can I submit more than one bulk certificate request?

You can submit only one request at a time. After the certificates are generated and you confirm that download is complete, you can submit another request.

What happens if I close my browser when a bulk certificate request is running?

If you close your browser or log out when a bulk certificate request is in progress, you will be automatically redirected to the Certificate Generation Status page where you can see the progress of your request. When certificate generation is complete, you can view the summary and download the generated certificates.

Can I generate certificate(s) on behalf of others?

You must be a user with administrator privileges (Super Admin or ERS Admin privilege) to be able to generate certificate(s) for someone else. All other users can request for certificate(s) only for themselves.

What are the contents of the certificate zip file?

Depending on the certificate download format that you have chosen, the zip file contains the following:

- Certificate for the end entity—A certificate for the end entity that matches the information provided by you such as the Common Name, Subject Alternative Name (SAN), and so on. For example, if a requester whose username is Joe submits a request for his device with MAC address (SAN) 11-22-33-44-55-66, then the certificate file is named as Joe_11-22-33-44-55-66.cer.
- Private key (only for single certificate using attributes or bulk certificate requests)—A private key for the end entity certificate. If a requester whose username is Joe submits a request for his device with MAC address (SAN) 11-22-33-44-55-66, then the private key file is named as Joe_11-22-33-44-55-66.key.
- Certificate chain —All the certificates in the certificate chain leading up to the Root CA for the Cisco ISE Internal CA.
- For the end entity to trust the ISE server during EAP-TLS authentication, one of the following files is present in the zip file:
    - EAP certificate chain (if the Cisco ISE server certificates are signed by an external CA)
    - Cisco ISE self-signed certificate (if the ISE server uses a self-signed certificate for server authentication)

How do I use the certificates?

After you download the certificate zip file to your local system:

1. Import the certificates in to the client device's keystore. If you submitted a bulk certificate request, copy the relevant end entity certificate and private key to the device that has the relevant MAC address (based on the SAN).
2. Modify your wireless or wired settings to use EAP-TLS based authentication and select the end entity certificate.
3. Connect the device to the network. The authentication should pass.

What do I do when I see the following errors?

- **Invalid request - The given CSR has a CN that doesn't match the provided username, and that user doesn't have ERS Admin**

  This error message appears because the Common Name (CN) value in the request does not match the requester's username. The CN must match the username of the user who is requesting the certificate. This check ensures that users do not request certificates for someone else. However, a user who belongs to the ERS Admin Group (an admin user) can request certificates for other users, and the CN does not have to match the admin user's username.

  Workaround: Resubmit the request providing your username in the Common Name field.

- **The given CN is invalid. Cannot contain [] " : ; | = , + * ? < > characters**

  This error message appears when invalid characters are present in the CN. Invalid characters include [ ] " : ; | = , + * ? < >. These characters are not allowed in an Active Directory username, and hence they should not appear in the CN.

  Workaround: Resubmit the request with a valid CN.

- **Invalid MAC address**

  This error appears because the MAC address is invalid. A MAC address must be of the form 11-11-11-11-11-11, 11:11:11:11:11:11, 1111.1111.1111, 111111.111111, 111111111111. Apart from the delimiters "-", ":", and "." , the MAC address can only contain digits 0 through 9 and letters A through F.

  Workaround: Provide the MAC address in a supported format and resubmit the request.

- **CA server error - Certificate request to internal CA failed CN**

  This error indicates a general failure with the Cisco ISE Internal CA.

  Workaround: Resubmit the request. If requests continue to fail, contact your administrator.

- **ISE server error - The given CSR text is malformed**

  This error message appears because the CSR is not in a valid PEM format.

  Workaround: Provide the CSR in a valid PEM format.

- **Invalid request - The given CSR has an OU RDN that doesn't match what's defined in the provided Certificate Template**

  This error message appears because the OU RDN (or the RDN listed in the error message) does not match with what is provided in the certificate template.

  Workaround: Contact your administrator to find out what RDN values should be used in the CSR.

- **There are more than the max allowed entries in this CSV. Max is 500**

  This error message appears because the CSV file that you provided has more than 500 entries.

  Workaround: Divide the CSV file into multiple CSV files with no more than 500 entries in each file. Submit the CSV files for bulk certificate request, one file at a time. Proceed with the next request after the previous one is complete.

- **There are either missing or extra columns in the CSV file. Please stick to the template**

  This error message appears because the CSV file is not formatted correctly.

  Workaround: Ensure that each entry has values for two fields; a CN and a SAN provided for every entry. The SAN should be a MAC address. Resubmit the request.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.