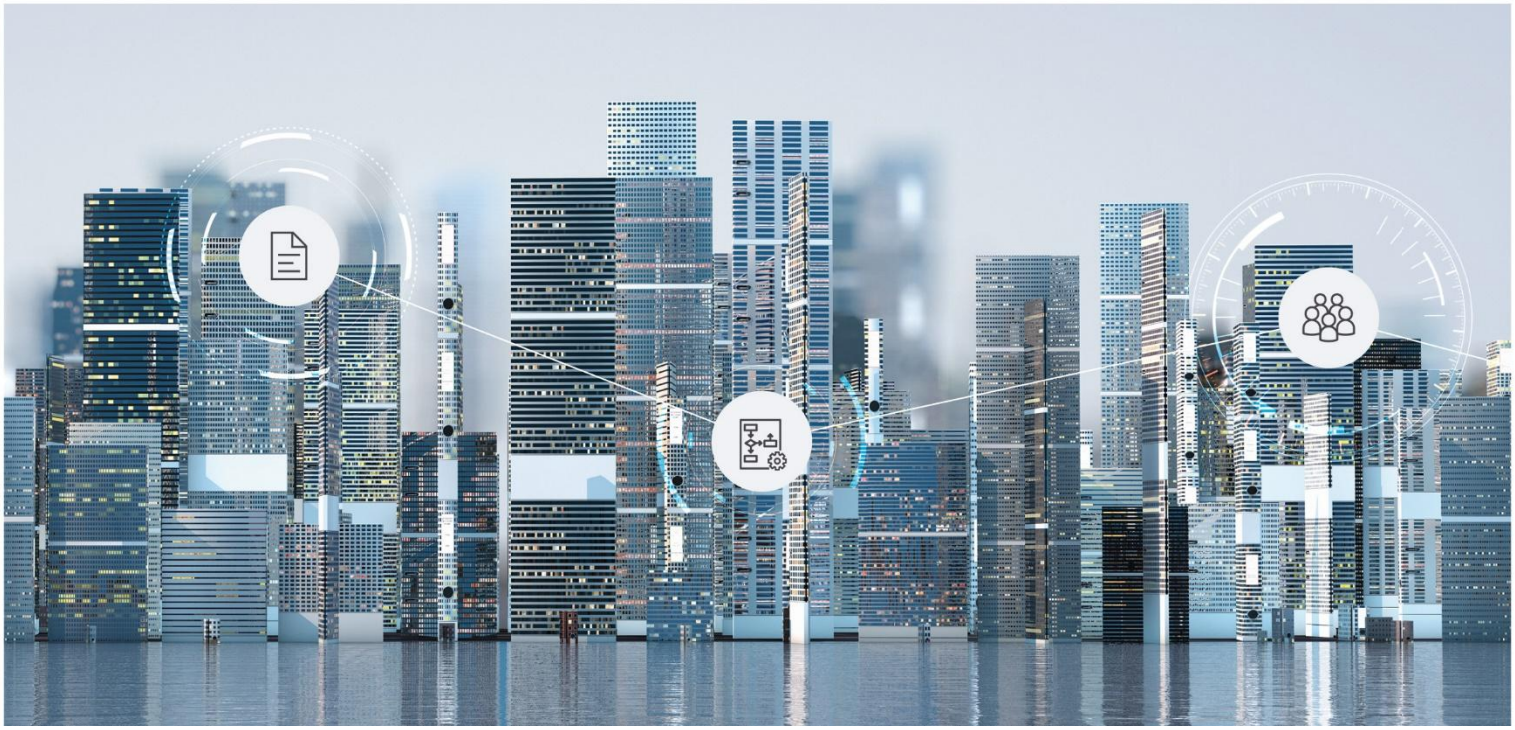
Fabasoft



White Paper

CA and User Certificate Management

2025 July Release

Contents

1 Introduction

To allow members of your organization to use Fabasoft Cloud with client-certificates, you need a certificate authority (CA) for your organization. This CA is used to issue the user certificates for the members of your organization. In the following chapters you can learn how to create a CA and user certificates. Furthermore, you can find information about how to configure the log-in with certificate for your organization in Fabasoft Cloud.

In the user certificates you may use these characters: a-z, A-Z, 0-9. The common name (CN) of the user certificate may consist additionally of those special characters: ö,ä,ü,ß,-;

2 Create a CA via OpenSSL

2.1 Preparation

Create a directory for your CA and configure it in your openssl.cnf (Parameter “dir”).

In this Case “/etc/pki/CA“ will be used.

2.2 Create a Private Key

```
mkdir -p /etc/pki/CA/private
cd /etc/pki/CA/

openssl genrsa -des3 -out private/cakey.pem 2048
```

2.3 Create a CSR

```
openssl req -new -key private/cakey.pem \
                -out careq.pem
```

Fill out the fields for the DN (Distinguished Name) like the country name, the name of your organization and the common name of your certificate authority.

2.4 Create a Certificate

```
openssl x509 -days 1095 -signkey private/cakey.pem \
                        -CAserial serial \
                        -set_serial 00 \
                        -in careq.pem -req \
                        -out cacert.pem
```

2.5 Convert a Certificate

```
openssl x509 -in cacert.pem \
             -out cacert.cer \
             -outform DER
```

2.6 Create a CA Serial File

```
echo -n '00' > serial
```

2.7 Add a CA to index.txt

The `index.txt` is a tab separated file with the following columns:

- State: “V” for Valid, “E” for Expired and “R” for revoked
- Enddate: in the format YYMMDDHHmmssZ (the “Z” stands for Zulu/GMT)
- Date of Revocation: same format as “Enddate”
- Serial: serial of the certificate
- Path to Certificate: can also be “unknown”
- Subject: subject of the certificate

You can parse the values from the certificate:

```
openssl x509 -in cacert.pem -serial -enddate -subject
```

2.8 Create an Entry for the CA Certificate

```
echo -e "V\t120522135101Z\t\t00\tcacert.pem\t/C=AT/ST=Upper
Austria/L=Linz/O=MyCompany/CN=MY Companys CA" > index.txt
```

3 Create User Certificates via OpenSSL

3.1 Create a Private Key

```
mkdir -p /etc/pki/CA/newcerts
openssl genrsa -out newcerts/username_key.pem 2048
```

3.2 Create a CSR

```
openssl req –utf8 –nameopt oneline,utf8 -new -key newcerts/username_key.pem \
                -out newcerts/username_req.pem
```

3.3 Create a Certificate

```
openssl x509 -days 365 -CA cacert.pem \
                       -CAkey private/cakey.pem \
                       -CAserial serial \
                       -in newcerts/username_req.pem -req \
                       -out newcerts/username.pem
```

3.4 Convert a Certificate

```
openssl pkcs12 -export -in newcerts/username.pem \
                       -inkey newcerts/username_key.pem \
                       -out newcerts/username.p12
```

3.5 Add a Certificate to index.txt

```
openssl x509 -in newcerts/username.pem -serial -enddate -subject
```

```
echo -e "V\t120522155648Z\t\t01\tnewcerts/username.pem\t/C=AT/ST=Upper
Austria/L=Linz/O=MyCompany/CN=Username/emailAddress=username@mycompany.com" >>
index.txt
```

4 Certificate Revocation List via OpenSSL

4.1 Create a CRL

```
echo -ne '00' > crlnumber
```

```
openssl ca -gencrl -out crl.pem
```

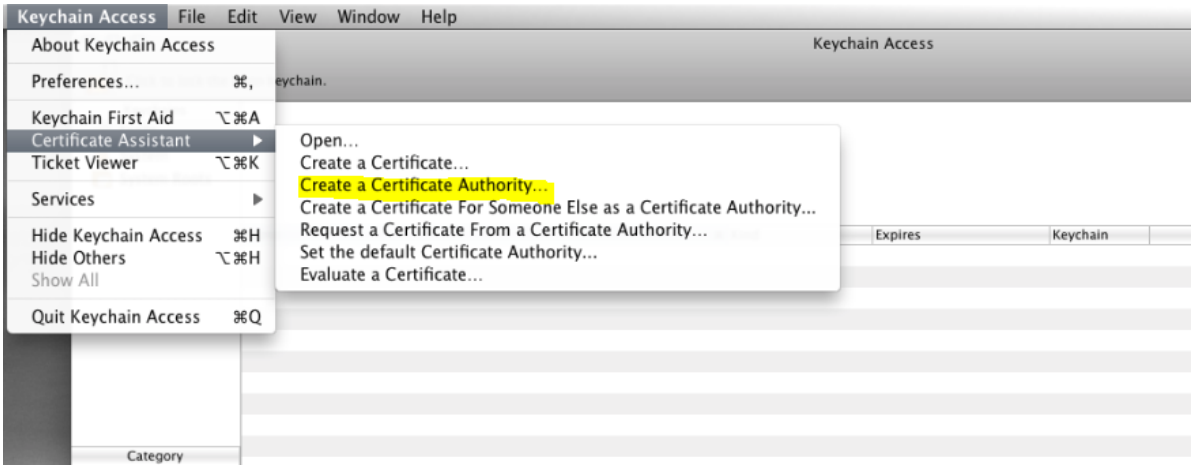
4.2 Revoke a Certificate

```
openssl ca -revoke newcerts/username.pem
```

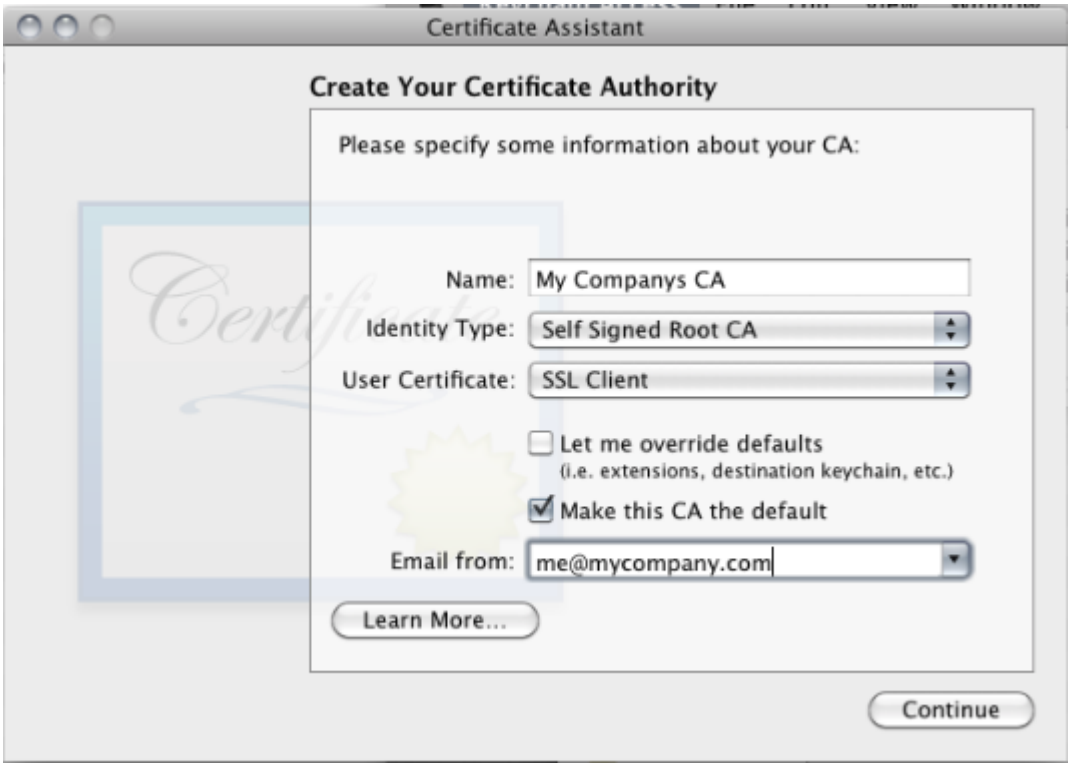
```
openssl ca -gencrl -out crl.pem
```

5 Create a CA via Apple Keychain

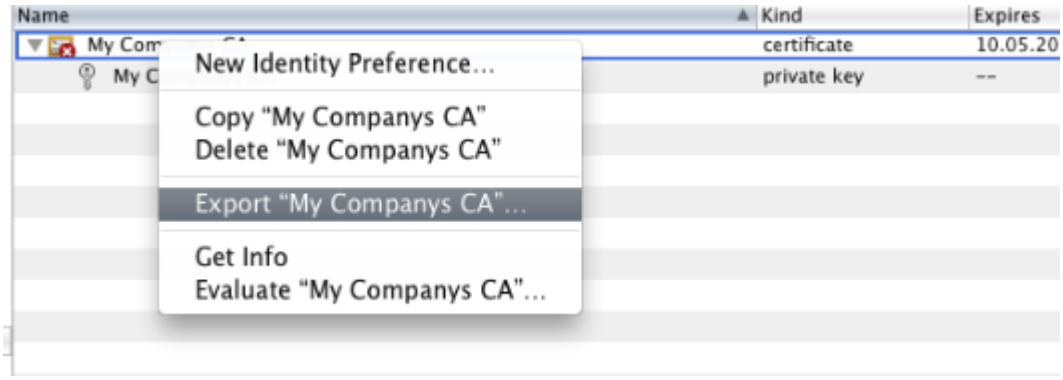
1. Open “Keychain Access“.
2. Select “Keychain Access” > “Certificate Assistant” > “Create a Certificate Authority“.



3. Define “Name” and “Email” for the CA.



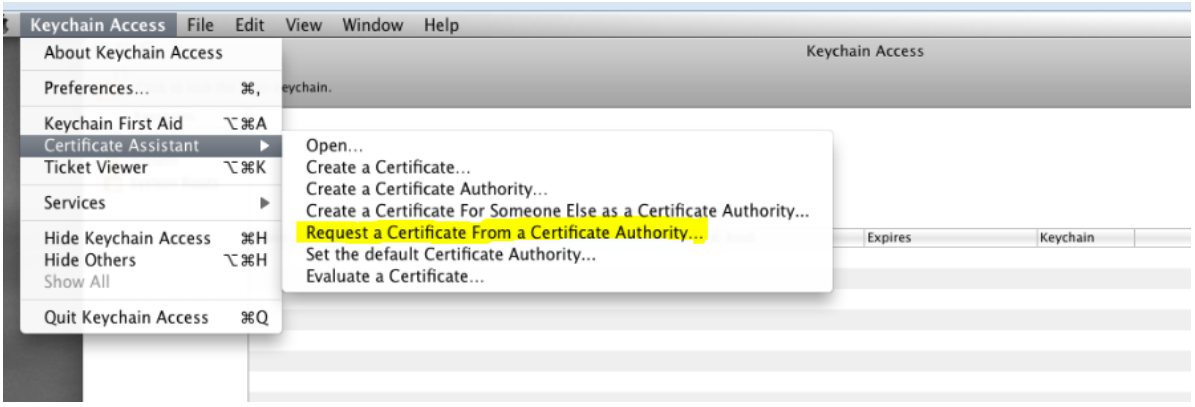
4. Open the context menu of the created CA.
5. Select “Export”.



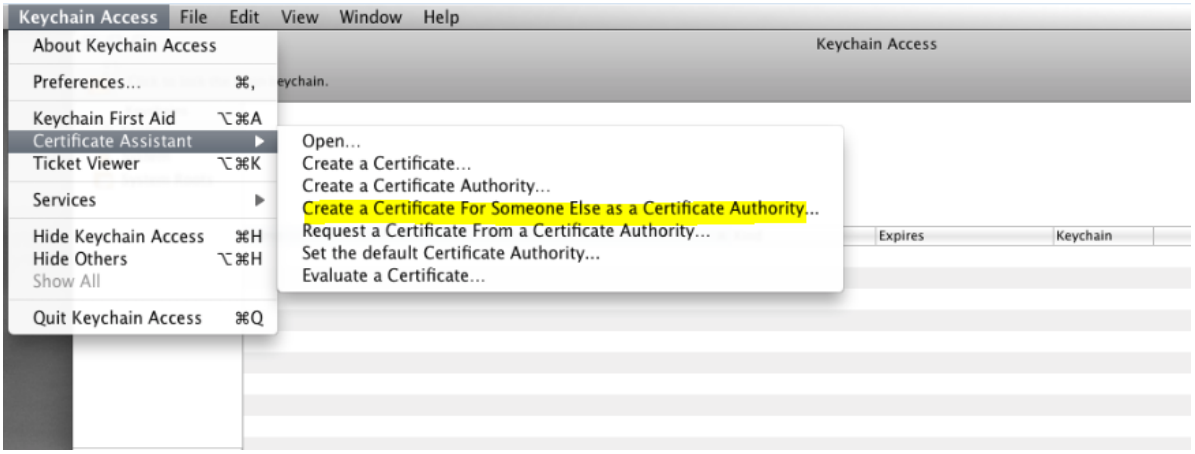
6. Select “Certificate (.cer)” as file format.

6 Create User Certificates via Apple Keychain

1. Open “Keychain Access“.
2. Select “Certificate Assistant“ > “Request a Certificate From A Certificate Authority“.



3. Define “Name” and “Email” for the user.
4. Select “Save to disk”.
5. Click “Continue”.
6. Select “Keychain Access“ > “Certificate Assistant“ > “Create Certificate For Someone Else as a Certificate Authority“.



7. Drag the request created before.

8. Select your CA created before.

7 Certificates in a Microsoft Windows Environment

Before you start, you have to plan your CA hierarchy. The following is only an example and may not fit for your organization.

For more information see:

- http://social.technet.microsoft.com/wiki/contents/articles/pki-design-brief-overview.aspx
- http://technet.microsoft.com/en-us/library/cc772393(v=ws.10).aspx
- http://technet.microsoft.com/en-us/library/cc731522.aspx

To carry out the following steps, you need a running Active Directory, all necessary licenses and an external web server.

7.1 Certificate Authority (CA)

In the following example, only a single root is chosen. The CA uses a SHA-512 hash algorithm, a 4096 character key and a 5-year validation time. Set the parameters according to your company guidelines.

The CRL in this example is available here (you may adapt it for your organization):
`http://localhost/certenroll/<CA common name>.crl`

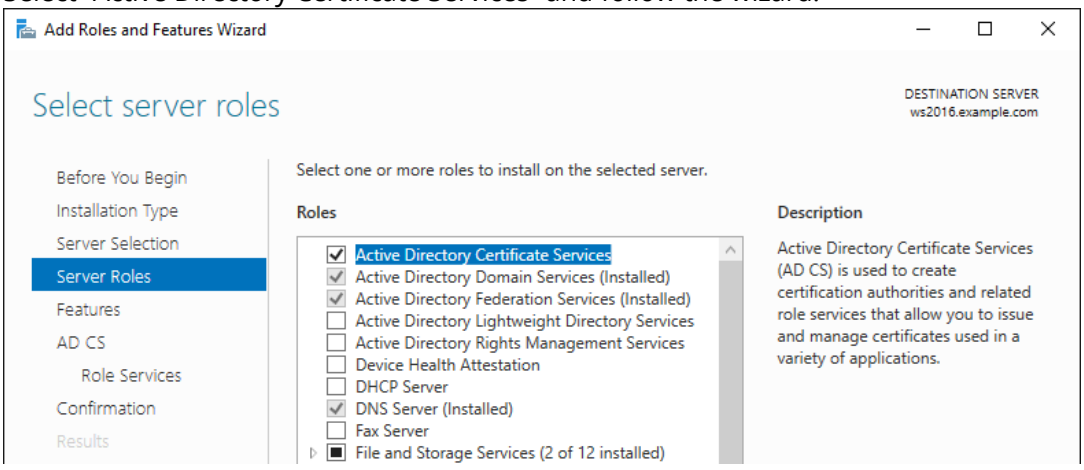
For information about how to use your Public Key Infrastructure (PKI) with the Fabasoft Cloud, see chapter 8 “Configure the Certificate Log-in for a Fabasoft Cloud Organization”.

The Active Directory is used for the automatic user certificate enrollment.

7.2 Install Active Directory Certificate Services

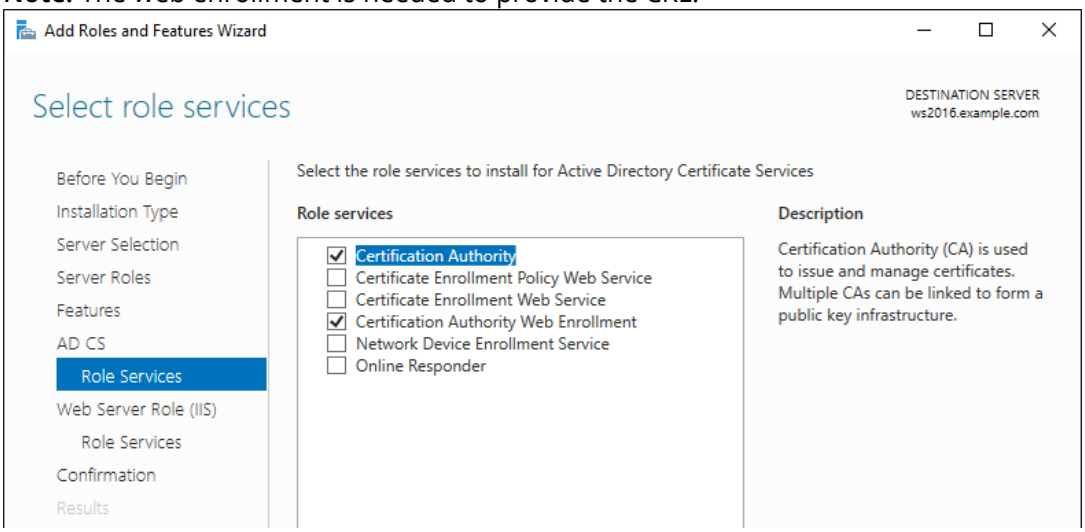
To add the “Active Directory Certificate Services” role, proceed as follows:

1. Start the “Add Roles and Features Wizard” (“Server Manager” > “Manage” > “Add Roles and Features”).
2. Carry out a *Role-based or feature-based installation* on the desired server.
3. Select “Active Directory Certificate Services” and follow the wizard.



4. As *Role services* select “Certification Authority” and “Certification Authority Web Enrollment” and follow the wizard.

Note: The web enrollment is needed to provide the CRL.

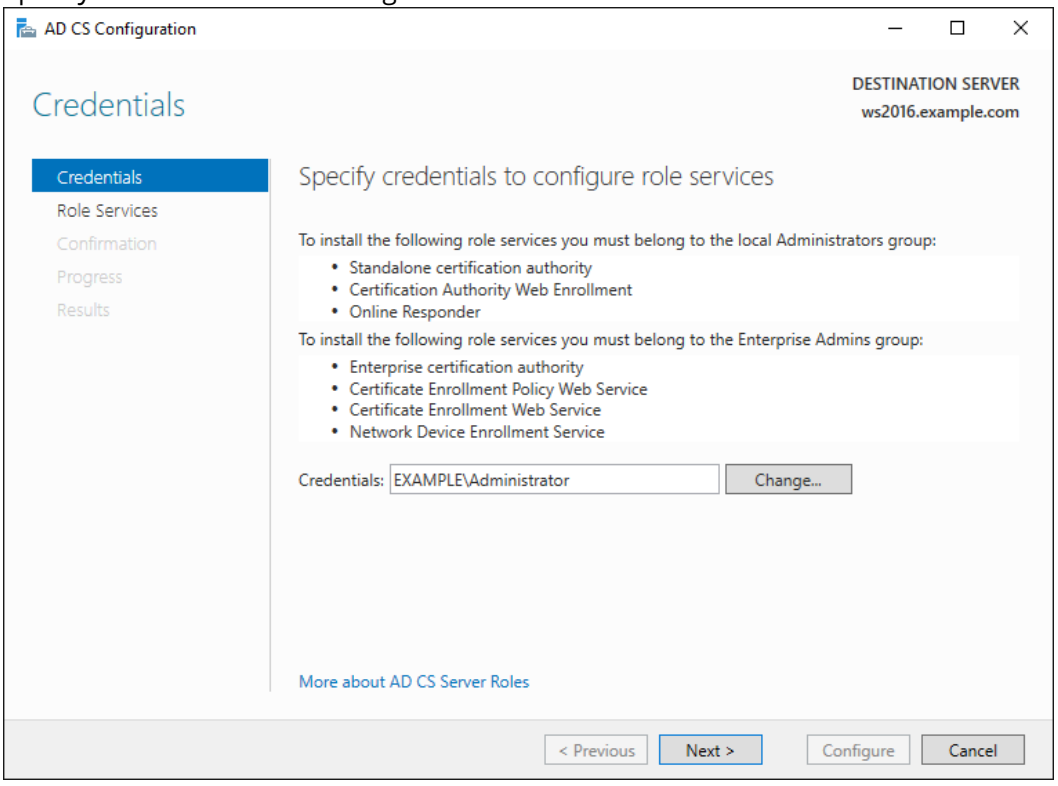


5. Click “Install”.

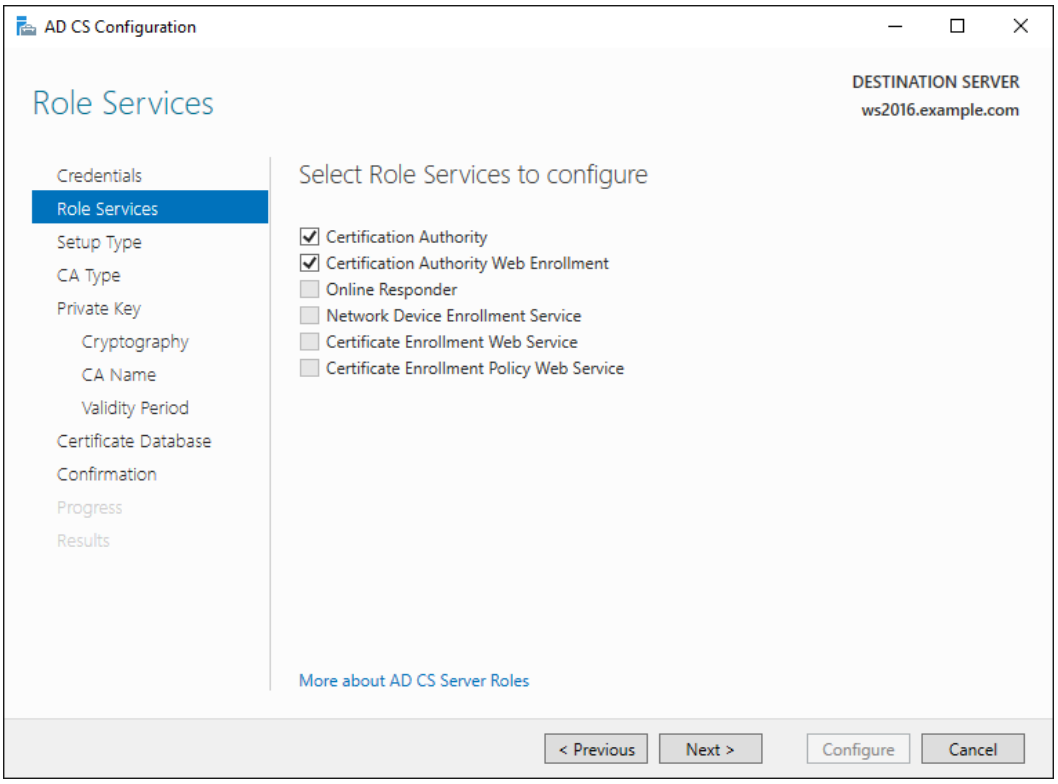
7.3 Configure Active Directory Certificate Services

To configure Active Directory Certificate Services, proceed as follows:

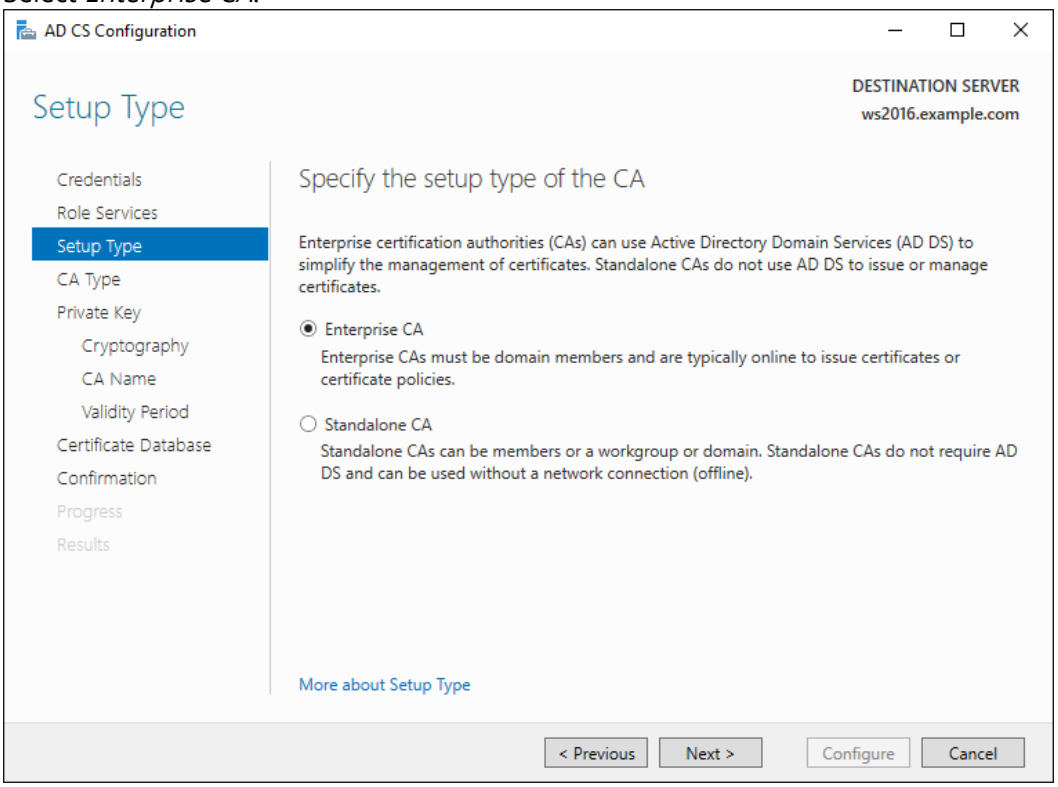
1. Start the “AD CS Configuration Wizard” (“Server Manager” > “Notifications” > “Configure Active Directory Certificate Services”).
2. Specify the credentials to configure role services.



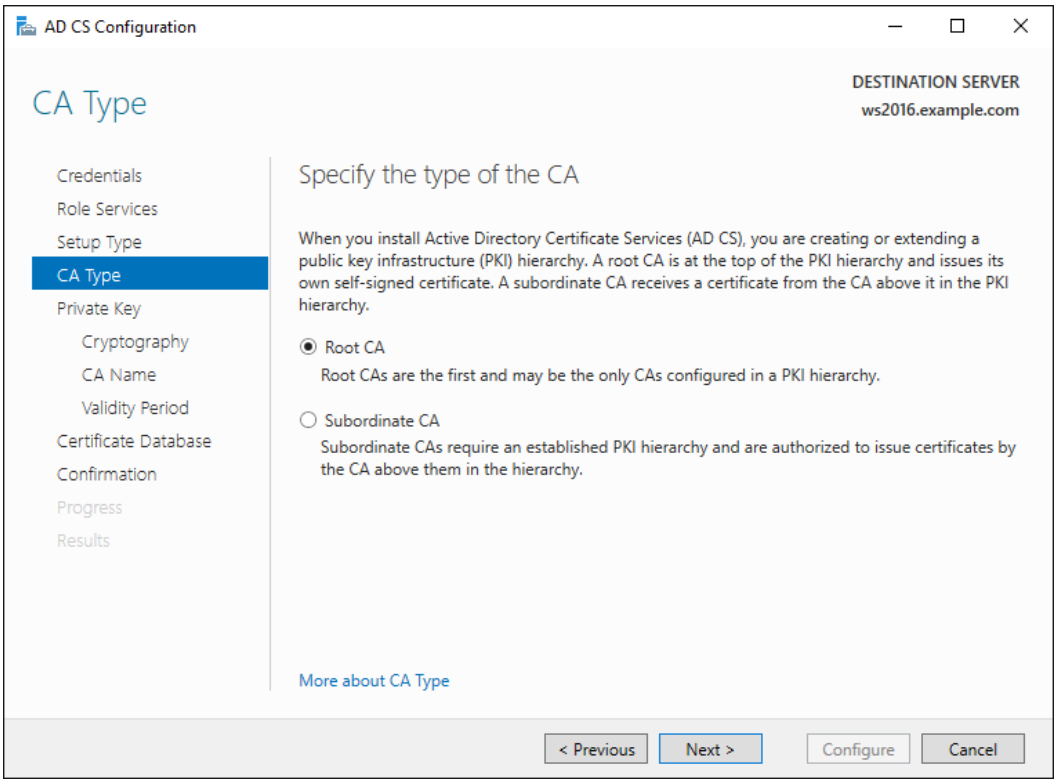
3. Select the “Certification Authority” and “Certification Authority Web Enrollment” role services.



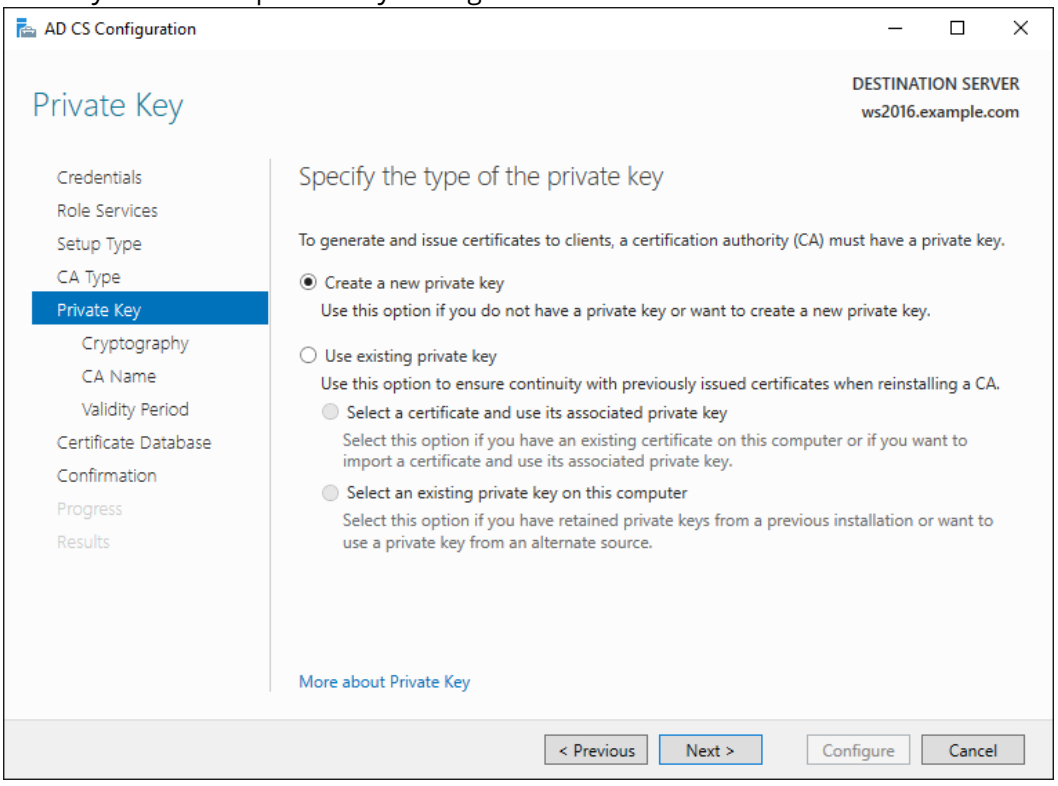
4. Select *Enterprise CA*.



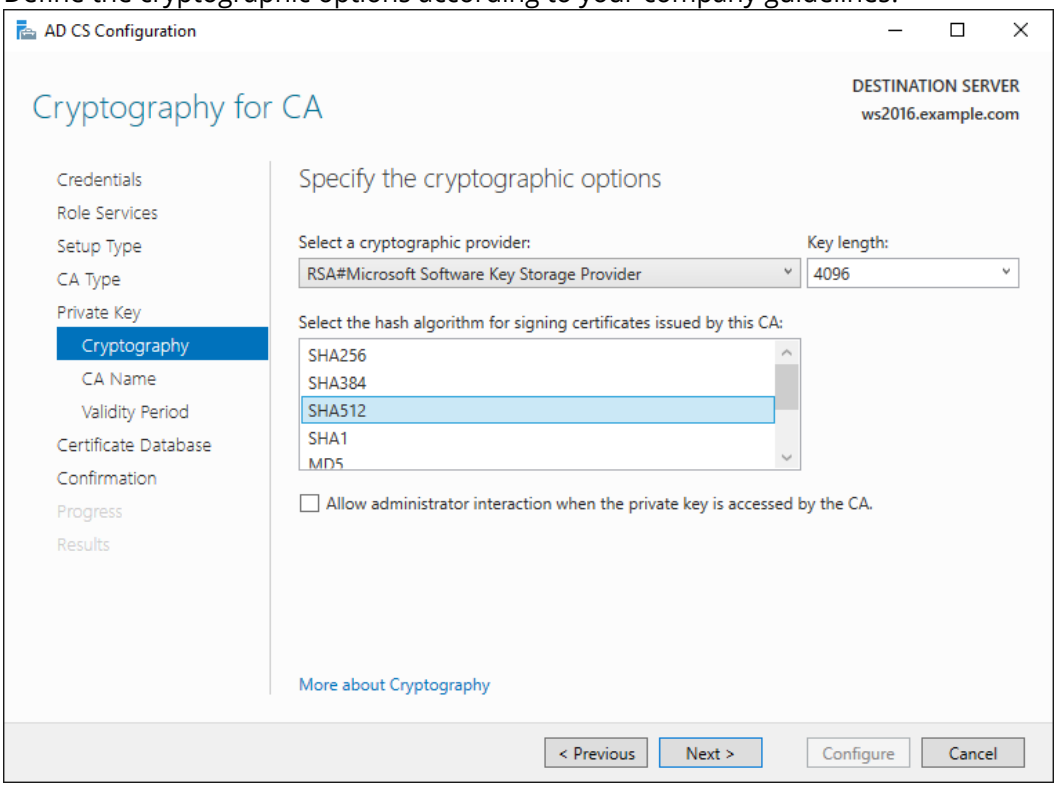
5. Select *Root CA*.



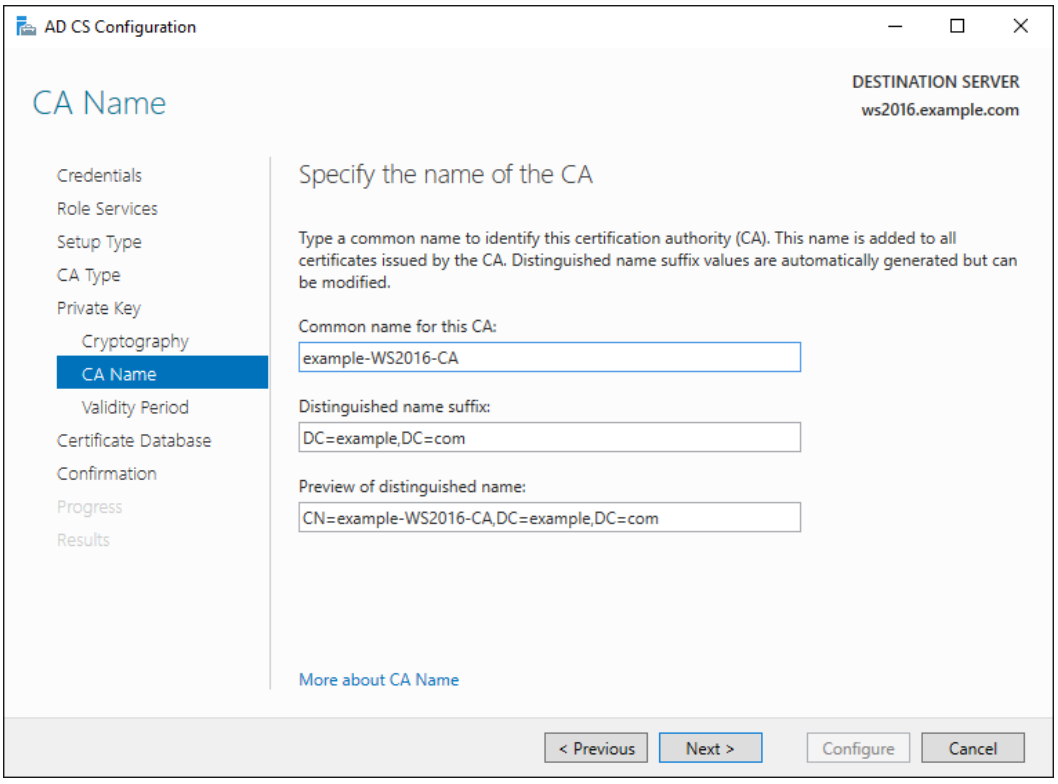
6. Define your desired private key settings.



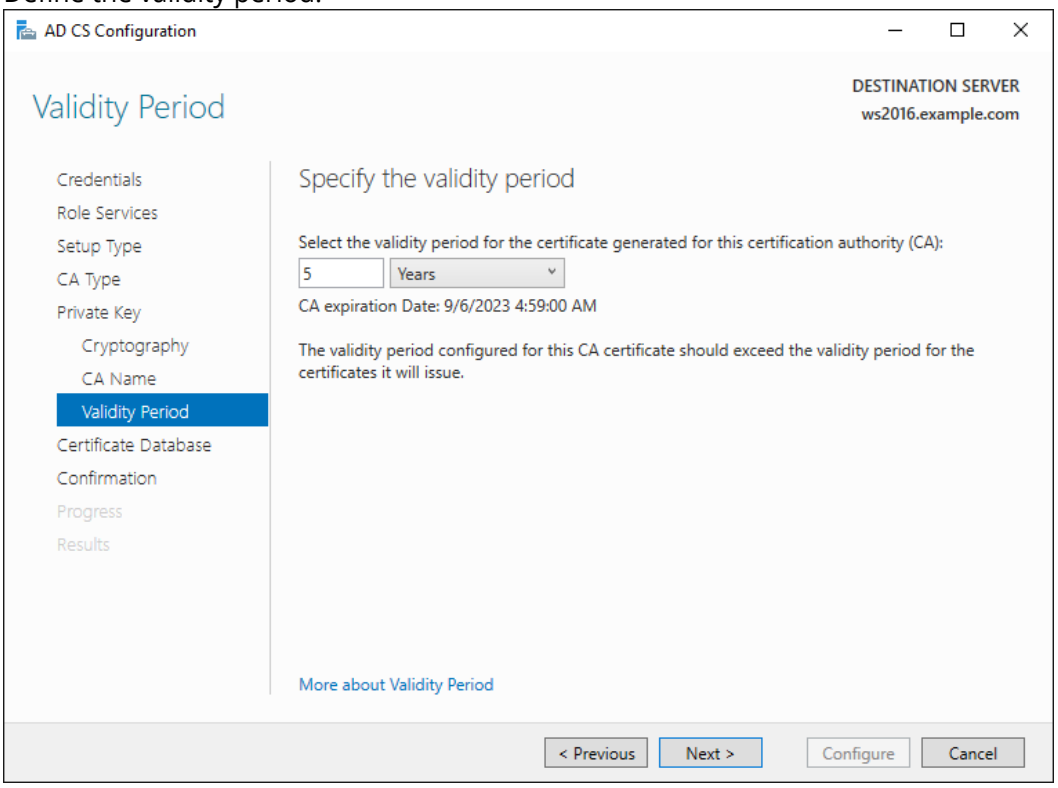
7. Define the cryptographic options according to your company guidelines.



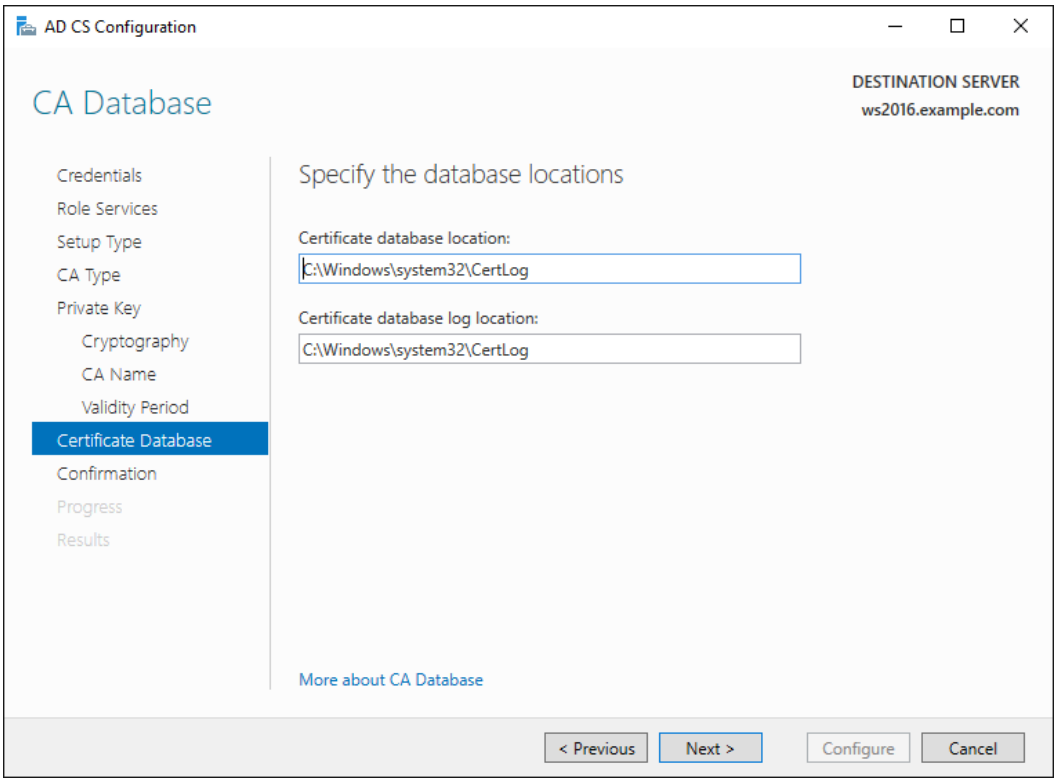
8. Enter a common name for the CA.



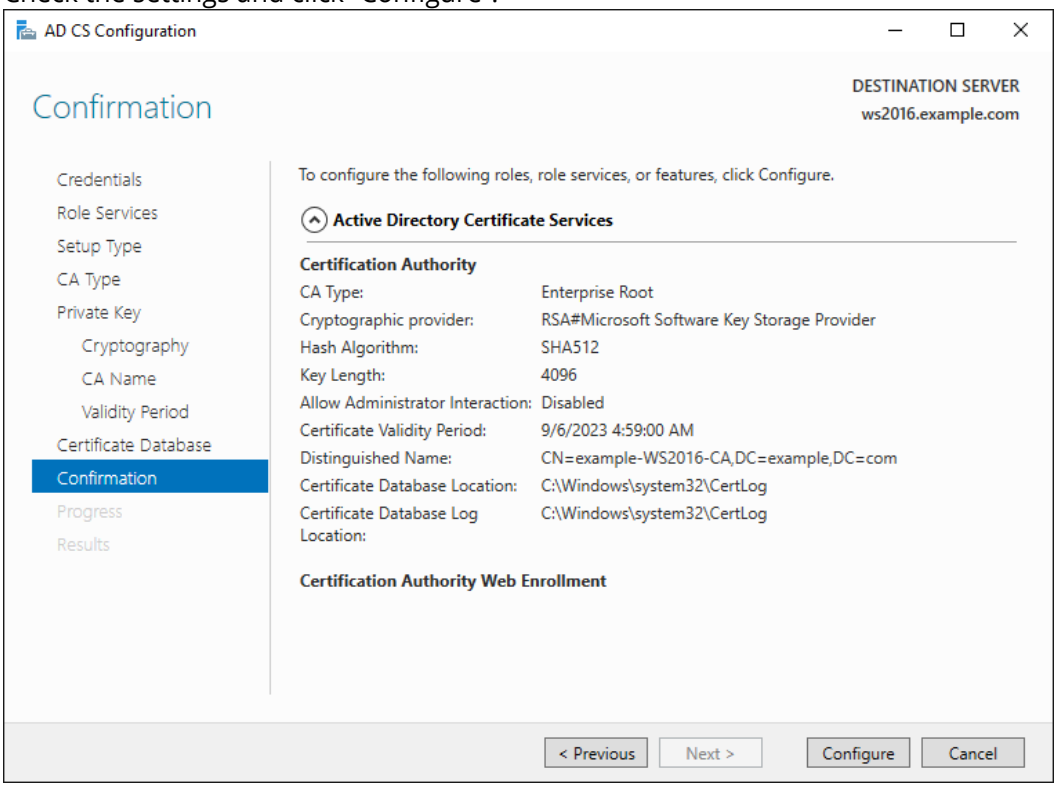
9. Define the validity period.



10. Define the database location.



11. Check the settings and click “Configure”.



7.4 Define an Automatic Rollout of User Certificates

To enable an automatic rollout of user certificates via group policies check the corresponding properties in the default domain policy.

Make sure that the every domain user can auto-enroll the specific certificate template.

7.5 Export Root and Issuing Certificates

Start `certmgr.msc` and export the root certificate (“Trusted Root Certification Authority” > “Certificates” > certificate’s context menu > “All Tasks” > “Export” > “DER encoded binary X.509”). If you have intermediate CAs, repeat the export for all these certificates.

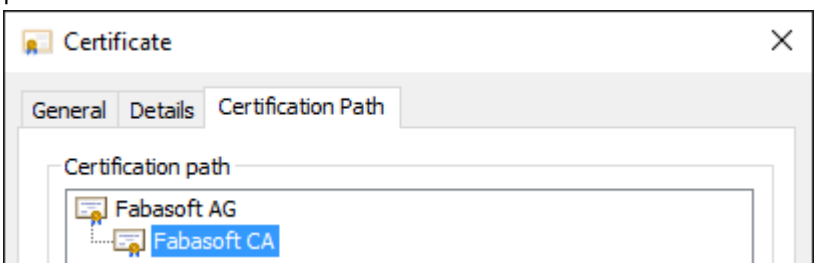
The usage of these files is described in the next chapter.

8 Configure the Certificate Log-in for a Fabasoft Cloud Organization

To allow members of your organization to log in with certificates, the following requirements must be met:

- All certificates as files (CER files in PEM format) from the certification path to the root certificate of your organization.
  In the example below, the certificate “Fabasoft AG” is the root certificate of the organization and the certificate “Fabasoft CA” is the only other required certificate from the certification

path.



- URLs to the Certificate Revocation Lists (CRLs).

8.1 Configure the Cloud Organization

In order that members of your organization can log in via a client certificate, all certificate authorities that are allowed to issue client certificates for your organization, have to be stored in the corresponding field as CER files in PEM format.

Additionally, you have to store the superordinate root and intermediate certificate authorities for the issuing certificate authorities in the corresponding field as CER files in PEM format. Provide for each root, intermediate and issuing certificate authority the corresponding certificate revocation list URLs. You can define whether a two-factor authentication is necessary when using the certificate log-in.

The CN of the certificates and the DN of the issuer must not contain special characters.

To complete the certificate configuration for your organization, you have to add the common name of the corresponding client certificates to the members (see next chapter).

Note: You can also define certificate settings for external organizations. This way you can provide a client certificate log-in for your external members, too.

To configure your cloud organization, proceed as follows:

1. Navigate in your organization, open the “Advanced Settings” widget and click the “Login Options” > “Certificate” action.
2. Import the certificates authorities and enter the certificate revocation list URLs.
3. Click “Save”.

8.2 Assign Common Names for the User Certificates

To complete the configuration of the log-in with certificates for your organization, you have to register the common name of the user certificates for all members of your organization.

To assign a common name to a user, proceed as follows:

1. Navigate in the desired member and click the “Properties” action.
2. On the “Account” tab, enter the *Common Name (CN)*.
3. Click “Next” to save the changes.

Note: You may open the user certificate with `certmgr.msc` on a Microsoft Windows system. The common name can be found in the *Subject* field.

8.3 Use Certificates on an iOS Device

In order to use the certificate in Safari on your iPhone or iPad you have to install the certificate via a profile on your device. You may use Apple's "iPhone Configuration Utility" to install configuration profiles with the certificate of the user on your device.

If you want to use the certificate to log in with the Fabasoft Cloud App, you have to upload the certificate as PKCS #12 file to the Fabasoft Cloud App documents on the iOS device.

To export the certificate file by using e.g. the `certmgr.msc` utility on a Microsoft Windows system, proceed as follows:

1. Navigate to the certificate.
2. On the context menu of the certificate, click "All Tasks" > "Export".
3. Include the private key.
4. Select the PKCS #12 file format.
5. Enter a password to protect the private key.
6. Define the file name.

To upload the certificate to the Fabasoft Cloud App, proceed as follows:

1. Connect your device to your PC and start iTunes.
2. Select your device in iTunes and click "File Sharing" in the left area.
3. In the "Apps" section, click "Fabasoft Cloud". Drag the previously created certificate file on the Fabasoft Cloud documents list.
4. Start the Fabasoft Cloud app on your iOS device. The "Import Certificate" dialog is shown. Enter the password you have chosen during export and press the "Open" button. Confirm the import by pressing the "Import" button.
5. Now you can use the certificate on the log-in dialog of the Fabasoft Cloud.

Note: Alternatively, certificates can be uploaded to Teamrooms in the Fabasoft Cloud. To install a certificate, the respective user must navigate to the certificate and press the "Import Certificate" action. This way, administrators can conveniently provide certificates for all organization members.