

White Paper

CA and User Certificate Management

2025 July Release

Copyright © Fabasoft R&D GmbH, Linz, Austria, 2025.

All rights reserved. All hardware and software names used are registered trade names and/or registered trademarks of the respective manufacturers.

No rights to our software or our professional services, or results of our professional services, or other protected rights can be based on the handing over and presentation of these documents.

Contents

1 Introduction	5
2 Create a CA via OpenSSL	5
2.1 Preparation	5
2.2 Create a Private Key	5
2.3 Create a CSR	5
2.4 Create a Certificate	5
2.5 Convert a Certificate	5
2.6 Create a CA Serial File	5
2.7 Add a CA to index.txt	6
2.8 Create an Entry for the CA Certificate	6
3 Create User Certificates via OpenSSL	6
3.1 Create a Private Key	6
3.2 Create a CSR	6
3.3 Create a Certificate	6
3.4 Convert a Certificate	6
3.5 Add a Certificate to index.txt	6
4 Certificate Revocation List via OpenSSL	7
4.1 Create a CRL	7
4.2 Revoke a Certificate	7
5 Create a CA via Apple Keychain	7
6 Create User Certificates via Apple Keychain	9
7 Certificates in a Microsoft Windows Environment	11
7.1 Certificate Authority (CA)	11
7.2 Install Active Directory Certificate Services	11
7.3 Configure Active Directory Certificate Services	12
7.4 Define an Automatic Rollout of User Certificates	17
7.5 Export Root and Issuing Certificates	17
8 Configure the Certificate Log-in for a Fabasoft Cloud Organization	17
8.1 Configure the Cloud Organization	18
8.2 Assign Common Names for the User Certificates	18
8.3 Use Certificates on an iOS Device	19

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

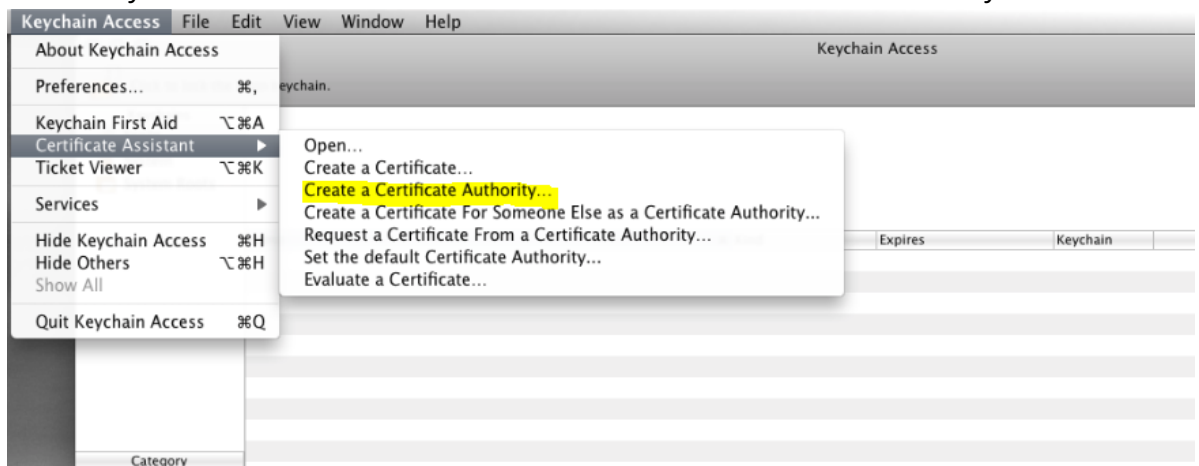
```
echo -ne '00' > crlnumber  
openssl ca -gencrl -out crl.pem
```

4.2 Revoke a Certificate

```
openssl ca -revoke newcerts/username.pem  
openssl ca -gencrl -out crl.pem
```

5 Create a CA via Apple Keychain

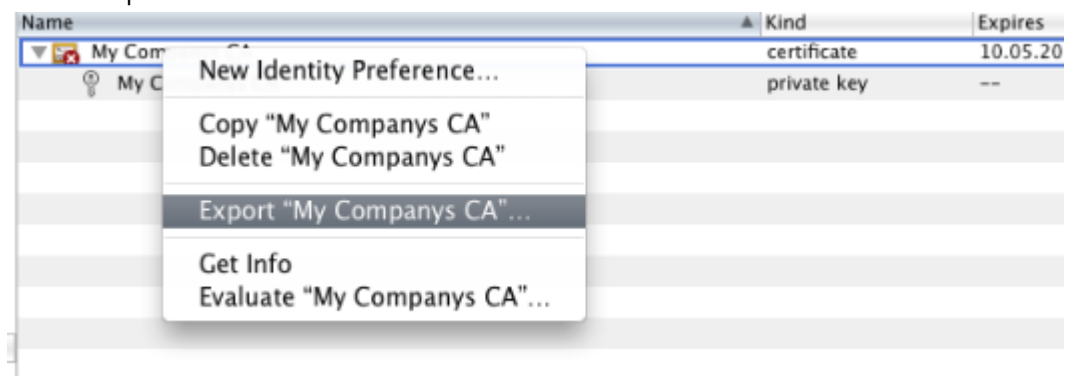
1. Open "Keychain Access".
2. Select "Keychain Access" > "Certificate Assistant" > "Create a Certificate Authority".



3. Define "Name" and "Email" for the CA.



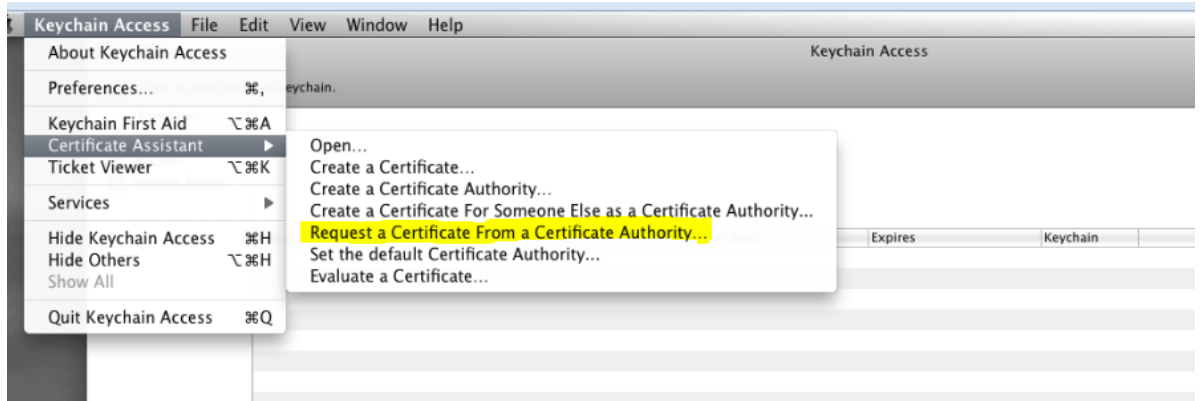
4. Open the context menu of the created CA.
5. Select "Export".



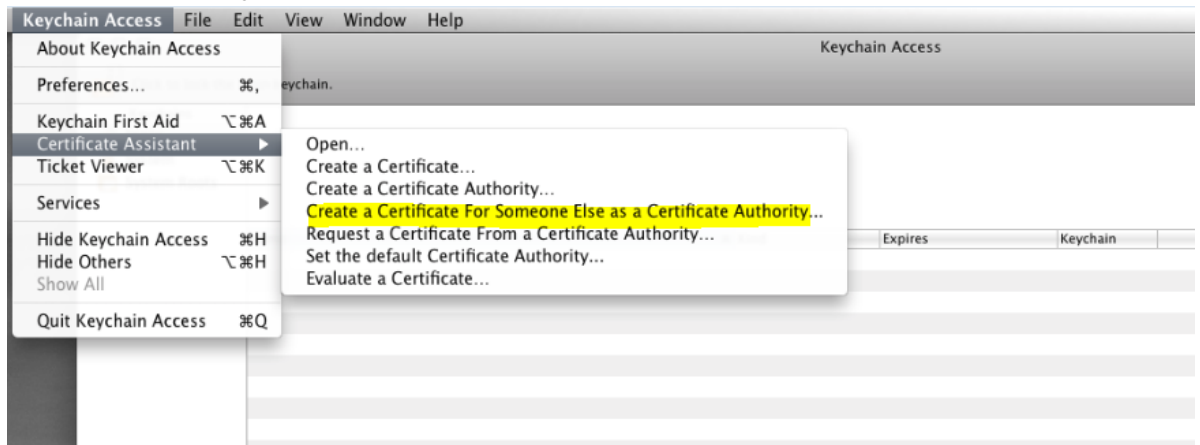
6. Select "Certificate (.cer)" as file format.

6 Create User Certificates via Apple Keychain

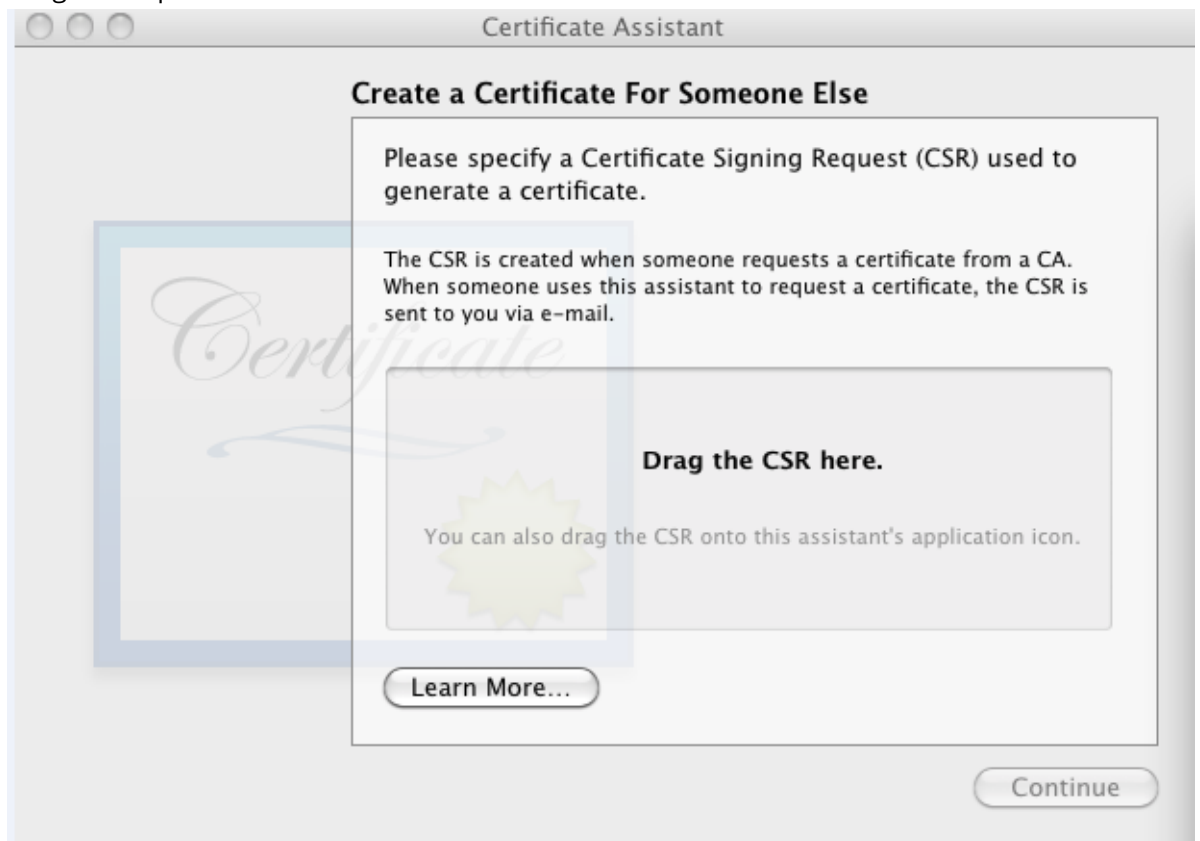
1. Open "Keychain Access".
2. Select "Certificate Assistant" > "Request a Certificate From A Certificate Authority".



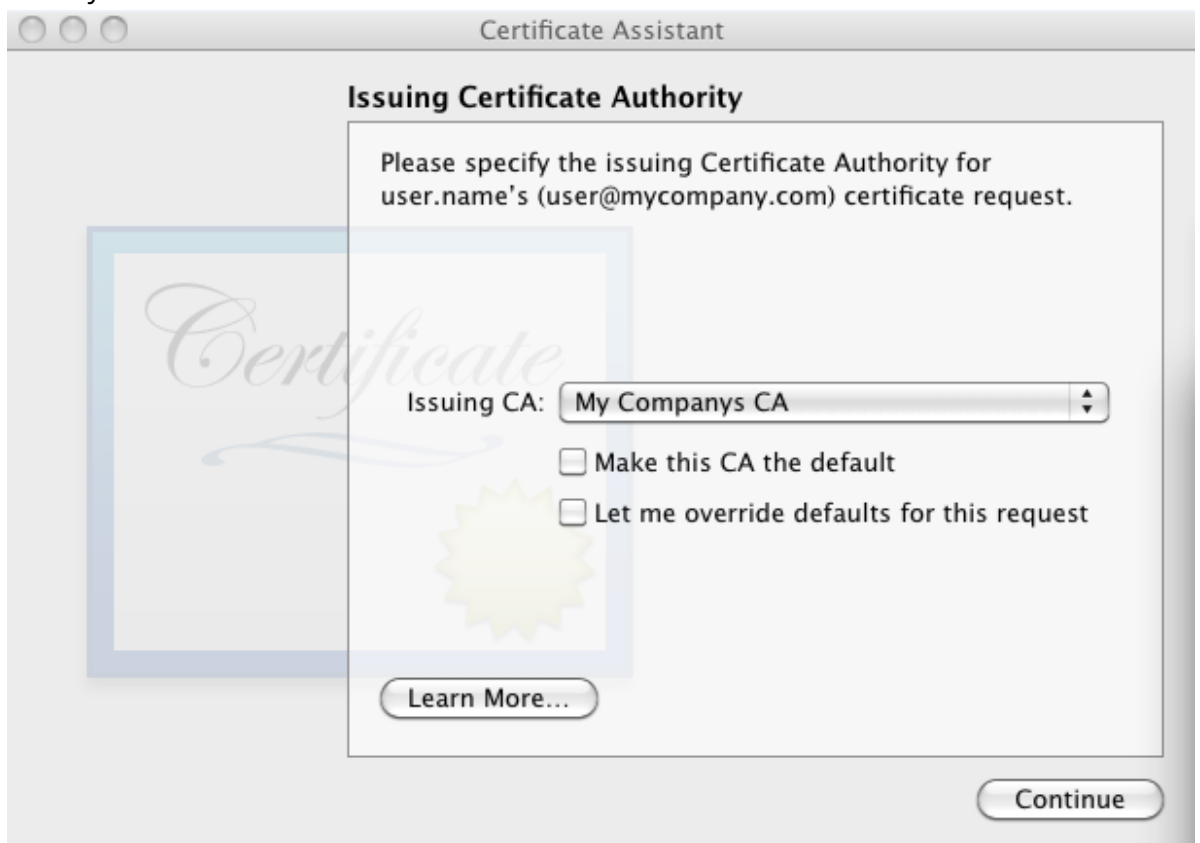
3. Define "Name" and "Email" for the user.
4. Select "Save to disk".
5. Click "Continue".
6. Select "Keychain Access" > "Certificate Assistant" > "Create Certificate For Someone Else as a Certificate Authority".



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/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`

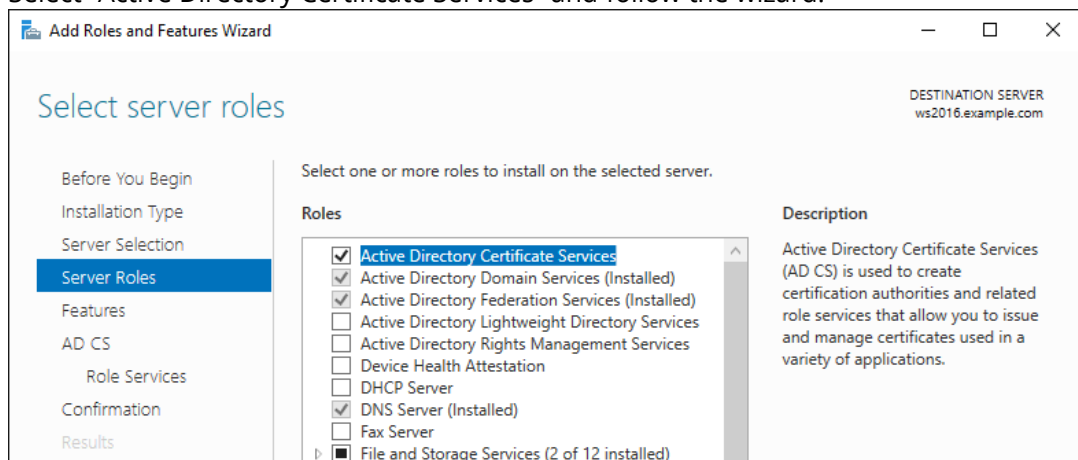
For information about how to use your Public Key Infrastructure (PKI) with the Fabasoft Cloud, see chapter 8 “Configure the Certificate Log-in for a Fabasoft Cloud Organization”.

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

7.2 Install Active Directory Certificate Services

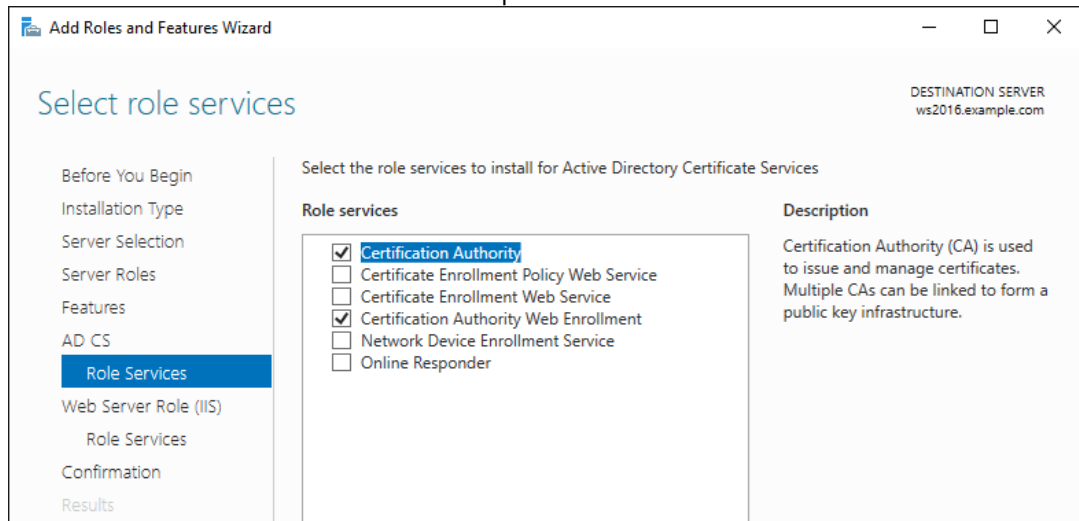
To add the “Active Directory Certificate Services” role, proceed as follows:

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.

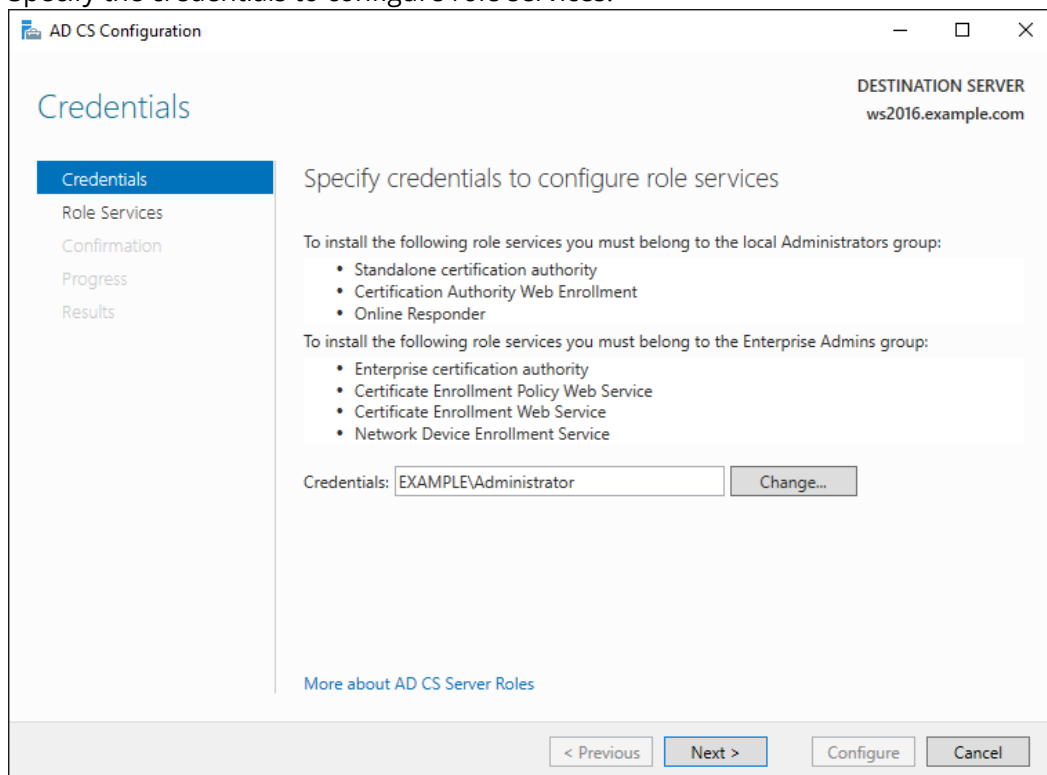


5. Click "Install".

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.

The screenshot shows the 'AD CS Configuration' window at the 'Role Services' step. The left sidebar lists steps: Credentials, Role Services (selected), Setup Type, CA Type, Private Key, Cryptography, CA Name, Validity Period, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Select Role Services to configure'. It contains a list of services with checkboxes: 'Certification Authority' (checked), 'Certification Authority Web Enrollment' (checked), 'Online Responder' (unchecked), 'Network Device Enrollment Service' (unchecked), 'Certificate Enrollment Web Service' (unchecked), and 'Certificate Enrollment Policy Web Service' (unchecked). A link 'More about AD CS Server Roles' is at the bottom. The top right shows 'DESTINATION SERVER ws2016.example.com'. The bottom has navigation buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

4. Select *Enterprise CA*.

The screenshot shows the 'AD CS Configuration' window at the 'Setup Type' step. The left sidebar lists steps: Credentials, Role Services, Setup Type (selected), CA Type, Private Key, Cryptography, CA Name, Validity Period, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Specify the setup type of the CA'. It contains a paragraph: 'Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.' Below this are two radio button options: 'Enterprise CA' (selected) with the text 'Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.', and 'Standalone CA' with the text 'Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).' A link 'More about Setup Type' is at the bottom. The top right shows 'DESTINATION SERVER ws2016.example.com'. The bottom has navigation buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

5. Select *Root CA*.

The screenshot shows the 'AD CS Configuration' wizard window. The title bar includes the text 'AD CS Configuration' and standard window controls. The main window has a sidebar on the left with the following items: 'Credentials', 'Role Services', 'Setup Type', 'CA Type' (highlighted in blue), 'Private Key', 'Cryptography', 'CA Name', 'Validity Period', 'Certificate Database', 'Confirmation', 'Progress', and 'Results'. The main area is titled 'CA Type' and contains the following text: 'Specify the type of the CA'. Below this is a paragraph explaining that when installing Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy. There are two radio button options: 'Root CA' (selected) and 'Subordinate CA'. The 'Root CA' option has a description: 'Root CAs are the first and may be the only CAs configured in a PKI hierarchy.' The 'Subordinate CA' option has a description: 'Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.' At the bottom of the main area is a link 'More about CA Type'. The bottom of the window has four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'. In the top right corner, it says 'DESTINATION SERVER ws2016.example.com'.

6. Define your desired private key settings.

The screenshot shows the 'AD CS Configuration' wizard window, now on the 'Private Key' step. The sidebar on the left is the same as in the previous screenshot, but 'Private Key' is now highlighted in blue. The main area is titled 'Private Key' and contains the following text: 'Specify the type of the private key'. Below this is a paragraph explaining that to generate and issue certificates to clients, a certification authority (CA) must have a private key. There are two radio button options: 'Create a new private key' (selected) and 'Use existing private key'. The 'Create a new private key' option has a description: 'Use this option if you do not have a private key or want to create a new private key.' The 'Use existing private key' option has a description: 'Use this option to ensure continuity with previously issued certificates when reinstalling a CA.' Below this are two sub-options, each with a radio button: 'Select a certificate and use its associated private key' and 'Select an existing private key on this computer'. The 'Select a certificate and use its associated private key' option has a description: 'Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.' The 'Select an existing private key on this computer' option has a description: 'Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.' At the bottom of the main area is a link 'More about Private Key'. The bottom of the window has four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'. In the top right corner, it says 'DESTINATION SERVER ws2016.example.com'.

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

The screenshot shows the 'Cryptography for CA' step in the AD CS Configuration wizard. The left-hand navigation pane lists several steps: Credentials, Role Services, Setup Type, CA Type, Private Key, **Cryptography** (highlighted), CA Name, Validity Period, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Specify the cryptographic options'. It contains two dropdown menus: 'Select a cryptographic provider:' set to 'RSA#Microsoft Software Key Storage Provider' and 'Key length:' set to '4096'. Below these is another dropdown menu 'Select the hash algorithm for signing certificates issued by this CA:' with 'SHA512' selected. A checkbox labeled 'Allow administrator interaction when the private key is accessed by the CA.' is currently unchecked. At the bottom of the main area is a link 'More about Cryptography'. The bottom of the wizard features four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

8. Enter a common name for the CA.

The screenshot shows the 'CA Name' step in the AD CS Configuration wizard. The left-hand navigation pane is the same as in the previous step, with 'CA Name' now highlighted. The main area is titled 'Specify the name of the CA'. It includes a text box for 'Common name for this CA:' containing 'example-WS2016-CA'. Below that is a text box for 'Distinguished name suffix:' containing 'DC=example,DC=com'. A third text box, 'Preview of distinguished name:', shows 'CN=example-WS2016-CA,DC=example,DC=com'. A link 'More about CA Name' is at the bottom of the main area. The bottom of the wizard features the same four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

9. Define the validity period.

The screenshot shows the 'Validity Period' step of the 'AD CS Configuration' wizard. The left sidebar contains a list of steps: Credentials, Role Services, Setup Type, CA Type, Private Key, Cryptography, CA Name, **Validity Period**, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Specify the validity period' and includes the text 'Select the validity period for the certificate generated for this certification authority (CA):'. Below this, there is a text input field containing '5' and a dropdown menu set to 'Years'. The 'CA expiration Date' is displayed as '9/6/2023 4:59:00 AM'. A note states: 'The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.' A link 'More about Validity Period' is at the bottom. The bottom navigation bar has buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'.

AD CS Configuration

DESTINATION SERVER
ws2016.example.com

Validity Period

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the validity period

Select the validity period for the certificate generated for this certification authority (CA):

5 Years

CA expiration Date: 9/6/2023 4:59:00 AM

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

[More about Validity Period](#)

< Previous Next > Configure Cancel

10. Define the database location.

The screenshot shows the 'CA Database' step of the 'AD CS Configuration' wizard. The left sidebar contains a list of steps: Credentials, Role Services, Setup Type, CA Type, Private Key, Cryptography, CA Name, Validity Period, **Certificate Database**, Confirmation, Progress, and Results. The main area is titled 'Specify the database locations' and includes the text 'Certificate database location:'. Below this, there is a text input field containing 'C:\Windows\system32\CertLog'. The text 'Certificate database log location:' is followed by another text input field containing 'C:\Windows\system32\CertLog'. A link 'More about CA Database' is at the bottom. The bottom navigation bar has buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'.

AD CS Configuration

DESTINATION SERVER
ws2016.example.com

CA Database

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the database locations

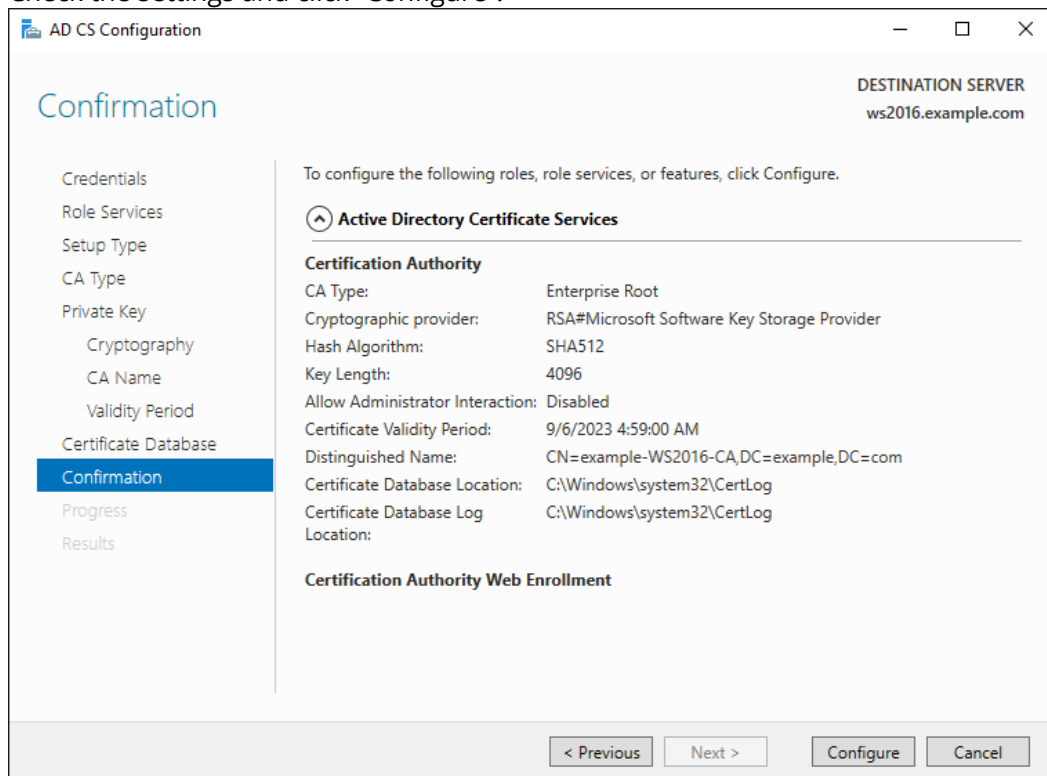
Certificate database location:
C:\Windows\system32\CertLog

Certificate database log location:
C:\Windows\system32\CertLog

[More about CA Database](#)

< Previous Next > Configure Cancel

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.

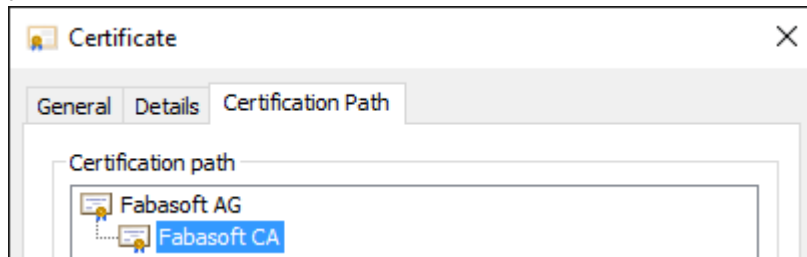
8 Configure the Certificate Log-in for a Fabasoft Cloud Organization

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.