

# Installing an enterprise CA

Server 2012R2



## Installation progress

DESTINATION SERVER  
testserver.testserver.com

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD CS

Role Services

Confirmation

Results

### View installation progress

#### Feature installation

Configuration required. Installation succeeded on testserver.testserver.com.

#### Active Directory Certificate Services

Additional steps are required to configure Active Directory Certificate Services on the destination server

[Configure Active Directory Certificate Services on the destination server](#)

**Certification Authority**

**Network Device Enrollment Service**

**Certificate Enrollment Policy Web Service**

**Certificate Enrollment Web Service**

**Online Responder**

**Certification Authority Web Enrollment**

#### Remote Server Administration Tools



You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

[Export configuration settings](#)

< Previous

Next >

Close

Cancel



# Credentials

DESTINATION SERVER  
testserver.testserver.com

## Credentials

Role Services

Confirmation

Progress

Results

### Specify credentials to configure role services

To install the following role services you must belong to the local Administrators group:

- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

To install the following role services you must belong to the Enterprise Admins group:

- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: TESTSERVER0\Administrator

Change...

[More about AD CS Server Roles](#)

< Previous

Next >

Configure

Cancel



## AD CS Configuration



### Role Services

DESTINATION SERVER  
testserver.testserver.com

Credentials

**Role Services**

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Authentication Type for C...

Server Certificate

Confirmation

Progress

Results

Select Role Services to configure

- Certification Authority
- Certification Authority Web Enrollment
- Online Responder
- Network Device Enrollment Service
- Certificate Enrollment Web Service
- Certificate Enrollment Policy Web Service

[More about AD CS Server Roles](#)

< Previous

Next >

Configure

Cancel



## Setup Type

DESTINATION SERVER  
testserver.testserver.com

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Authentication Type for C...

Server Certificate

Confirmation

Progress

Results

### Specify the setup type of the CA

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.

Enterprise CA

Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

Standalone CA

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).

[More about Setup Type](#)

< Previous

Next >

Configure

Cancel



## CA Type

DESTINATION SERVER  
testserver.testserver.com

- Credentials
- Role Services
- Setup Type
- CA Type**
- Private Key
  - Cryptography
  - CA Name
  - Validity Period
- Certificate Database
- Authentication Type for C...
- Server Certificate
- Confirmation
- Progress
- Results

### Specify the type of the CA

When you install 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.

- Root CA  
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.
- Subordinate CA  
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

[More about CA Type](#)

< Previous

Next >

Configure

Cancel



## Private Key

DESTINATION SERVER  
testserver.testserver.com

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key**
- Cryptography
- CA Name
- Validity Period
- Certificate Database
- Authentication Type for C...
- Server Certificate
- Confirmation
- Progress
- Results

### Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

- Create a new private key**  
Use this option if you do not have a private key or want to create a new private key.
- Use existing private key**  
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.
  - Select a certificate and use its associated private key**  
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.
  - Select an existing private key on this computer**  
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

[More about Private Key](#)

< Previous

Next >

Configure

Cancel



# Cryptography for CA

DESTINATION SERVER  
testserver.testserver.com

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
- Cryptography**
- CA Name
- Validity Period
- Certificate Database
- Authentication Type for C...
- Server Certificate
- Confirmation
- Progress
- Results

## Specify the cryptographic options

Select a cryptographic provider:

Key length:

Select the hash algorithm for signing certificates issued by this CA:

- SHA256
- SHA384
- SHA512
- SHA1**
- MD5

Allow administrator interaction when the private key is accessed by the CA.

[More about Cryptography](#)





## Validity Period

DESTINATION SERVER  
testserver.testserver.com

Credentials

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Authentication Type for C...

Server Certificate

Confirmation

Progress

Results

### Specify the validity period

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

CA expiration Date: 5/31/2020 3:37:00 PM

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



## AD CS Configuration



# CA Database

DESTINATION SERVER  
testserver.testserver.com

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
  - Cryptography
  - CA Name
  - Validity Period
- Certificate Database**
- Authentication Type for C...
- Server Certificate
- Confirmation
- Progress
- Results

### Specify the database locations

Certificate database location:

Certificate database log location:

[More about CA Database](#)

< Previous

Next >

Configure

Cancel



## Authentication Type for CEP

DESTINATION SERVER  
testserver.testserver.com

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
  - Cryptography
  - CA Name
  - Validity Period
- Certificate Database
- Authentication Type for C...**
- Server Certificate
- Confirmation
- Progress
- Results

Select the type of authentication

- Windows integrated authentication
- Client certificate authentication
- User name and password

[More about Authentication Type for CEP](#)

< Previous

Next >

Configure

Cancel



# Server Certificate

DESTINATION SERVER  
testserver.testserver.com

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
  - Cryptography
  - CA Name
  - Validity Period
- Certificate Database
- Authentication Type for C...
- Server Certificate**
- Confirmation
- Progress
- Results

## Specify a Server Authentication Certificate

When communicating with clients, the web service(s) uses Secure Sockets Layer (SSL) protocol to encrypt network traffic.


- Choose an existing certificate for SSL encryption (recommended)

Issued To	Issued By	Expiration Date

Properties

Refresh

- Choose and assign a certificate for SSL later

 For this role service to function, you must configure this server with a valid certificate.

[More about Server Certificate](#)

< Previous

Next >

Configure

Cancel



## AD CS Configuration



# Confirmation

DESTINATION SERVER  
testserver.testserver.com

Credentials

Role Services

Setup Type

CA Type

Private Key

    Cryptography

    CA Name

    Validity Period

Certificate Database

Authentication Type for C...

Server Certificate

**Confirmation**

Progress

Results

To configure the following roles, role services, or features, click Configure.

Hash Algorithm:	SHA1
Key Length:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	5/31/2020 3:37:00 PM
Distinguished Name:	CN=testserver-TESTSERVER-CA,DC=testserver,DC=com
Certificate Database Location:	F:\Windows\system32\CertLog
Certificate Database Log Location:	F:\Windows\system32\CertLog

### Certification Authority Web Enrollment

### Online Responder

### Certificate Enrollment Policy Web Service

Authentication Type:	Windows Integrated Authentication
Enable Key-based Renewal:	False
Server Authentication:	Choose a certificate later
Certificate:	

< Previous

Next >

Configure

Cancel



## Results

DESTINATION SERVER  
testserver.testserver.com

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
  - Cryptography
  - CA Name
  - Validity Period
- Certificate Database
- Authentication Type for C...
- Server Certificate
- Confirmation
- Progress

### Results

The following roles, role services, or features were configured:

#### ^ Active Directory Certificate Services

##### Certification Authority

✔ Configuration succeeded

[More about CA Configuration](#)

##### Certification Authority Web Enrollment

✔ Configuration succeeded

[More about Web Enrollment Configuration](#)

##### Online Responder

✔ Configuration succeeded

[More about OCSP Configuration](#)

##### Certificate Enrollment Policy Web Service

✔ Configuration succeeded

**i** Before clients can use this web service, a server authentication certificate must be configured to encrypt communication between clients and the service. Use the IIS snap-in to verify the server authentication certificate.

**i** Before clients can use the Certificate Enrollment Policy Web service, Group Policy settings must be applied to their computers to direct certificate enrollment requests to the web service.

[More about CEP Configuration](#)

< Previous

Next >

Close

Cancel

