

CONFIGURING ENTERPRISE CA AND ONLINE RESPONDER



Add Roles and Features Wizard



Installation progress

DESTINATION SERVER
WIN-E630K0E1QHE.server2012.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 WIN-E630K0E1QHE.server2012.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

Online Responder

Certification Authority Web Enrollment

Certificate Enrollment Policy Web Service

Certificate Enrollment Web Service

Remote Server Administration Tools

Role 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

WIN-E630K0E1QHE.server2012.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: SERVER2012\Administrator

[Change...](#)[More about AD CS Server Roles](#)

< Previous

Next >

Configure

Cancel

AD CS Configuration

Role Services

DESTINATION SERVER
WIN-E630K0E1QHE.server2012.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

AD CS Configuration

Setup Type

DESTINATION SERVER
WIN-E630K0E1QHE.server2012.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

WIN-E630K0E1QHE.server2012.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



AD CS Configuration



Private Key

DESTINATION SERVER

WIN-E630K0E1QHE.server2012.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
WIN-E630K0E1QHE.server2012.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:

RSA#Microsoft Software Key Storage Provider

Key length:

2048

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](#)

< Previous

Next >

Configure

Cancel



AD CS Configuration



CA Name

DESTINATION SERVER

WIN-E630K0E1QHE.server2012.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 name of the CA

Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA:

Distinguished name suffix:

Preview of distinguished name:

[More about CA Name](#)

< Previous

Next >

Configure

Cancel



AD CS Configuration



Validity Period

DESTINATION SERVER

WIN-E630K0E1QHE.server2012.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):

 Years

CA expiration Date: 7/3/2021 1:18:00 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
WIN-E630K0E1QHE.server2012.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
WIN-E630K0E1QHE.server2012.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

WIN-E630K0E1QHE.server2012.com

Credentials

Role Ser

Credentials

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
WIN-E630K0E1QHE.server2012.com	WIN-E630K0E1QHE.server2012.com	2/15/2017
WIN-E630K0E1QHE.server2012.com	WIN-E630K0E1QHE.server2012.com	2/15/2017

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

WIN-E630K0E1QHE.server2012.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.

^ Active Directory Certificate Services

Certification Authority

CA Type:	Enterprise Root
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA1
Key Length:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	7/3/2021 1:18:00 PM
Distinguished Name:	CN=SERVER2012CA,DC=server2012,DC=com
Certificate Database Location:	E:\Windows\system32\CertLog
Certificate Database Log Location:	E:\Windows\system32\CertLog

Certification Authority Web Enrollment

Online Responder

...

< Previous

Next >

Configure

Cancel



AD CS Configuration



Progress

DESTINATION SERVER

WIN-E630K0E1QHE.server2012.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 are being configured:

Configuring...



Active Directory Certificate Services

Certification Authority

Certification Authority Web Enrollment

Online Responder

Certificate Enrollment Policy Web Service



Results

DESTINATION SERVER

WIN-E630K0E1QHE.server2012.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

 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.

 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.

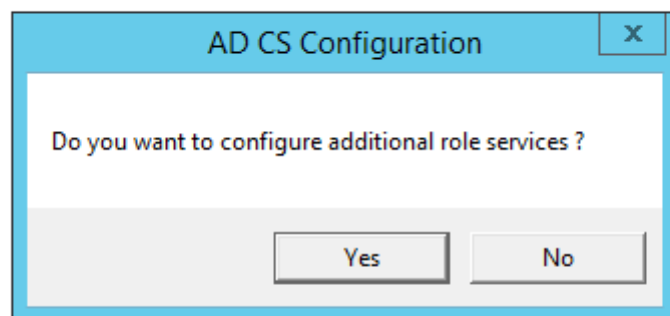
[More about CEP Configuration](#)

< Previous

Next >

Close

Cancel





Add Roles and Features Wizard



Installation progress

DESTINATION SERVER
WIN-E630K0E1QHE.server2012.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 WIN-E630K0E1QHE.server2012.com.

Active Directory Certificate Services

1 of 5 Active Directory Certificate Services role services are available to be configured on the destination server

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

Certification Authority

Online Responder

Certification Authority Web Enrollment

Certificate Enrollment Policy Web Service

Certificate Enrollment Web Service

Remote Server Administration Tools

Role 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.

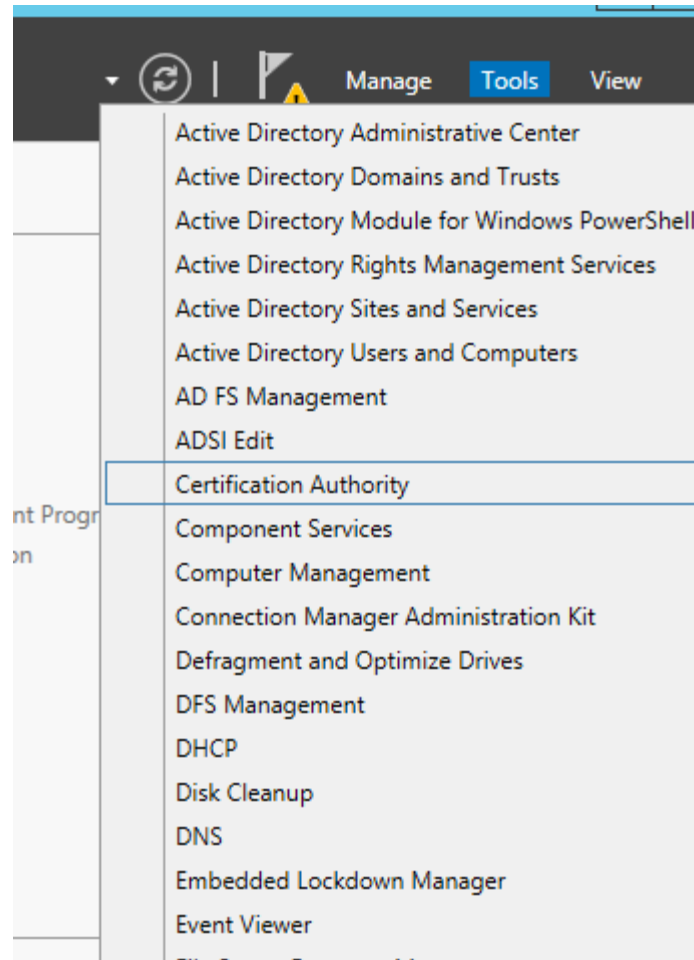
[Export configuration settings](#)

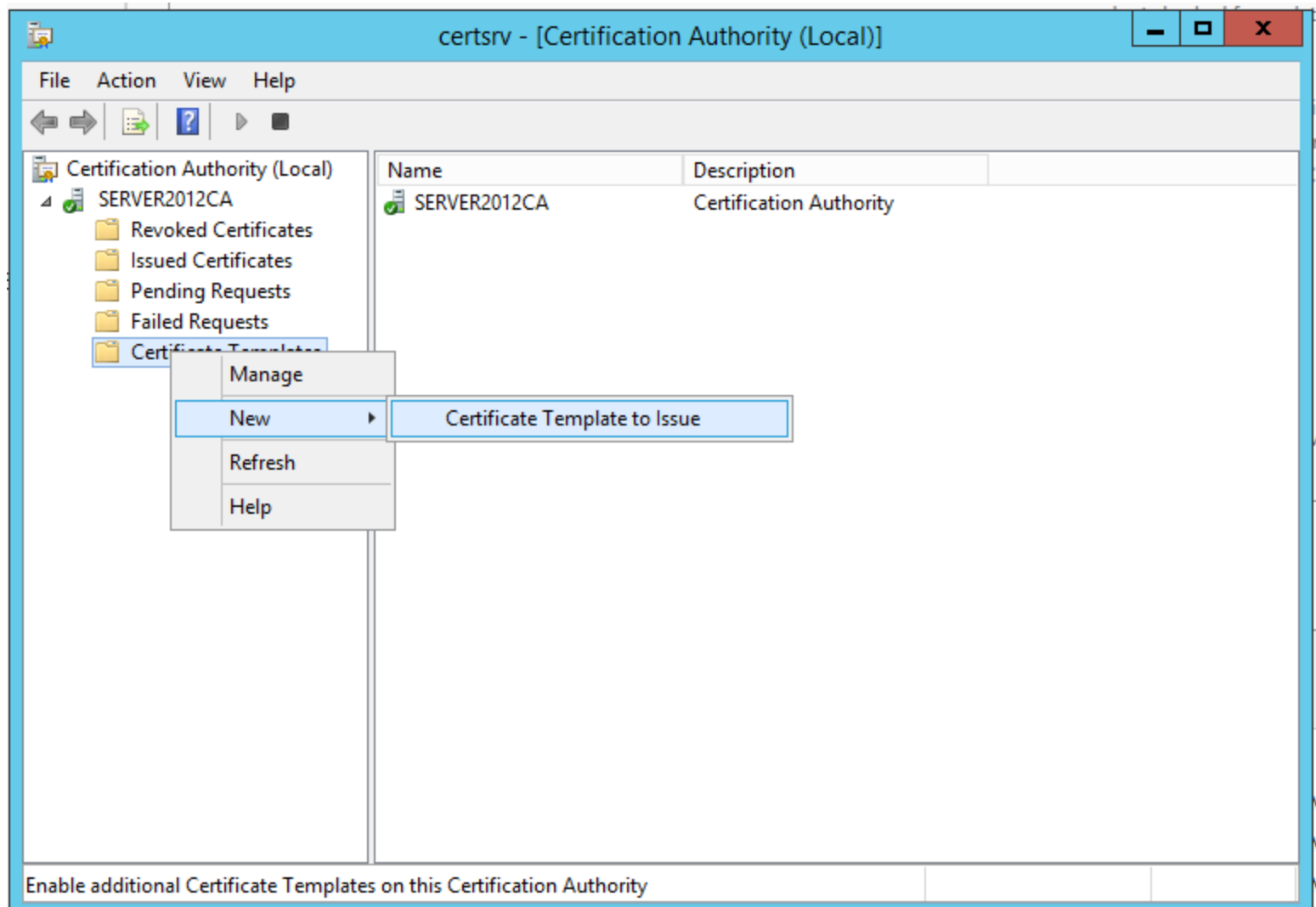
< Previous

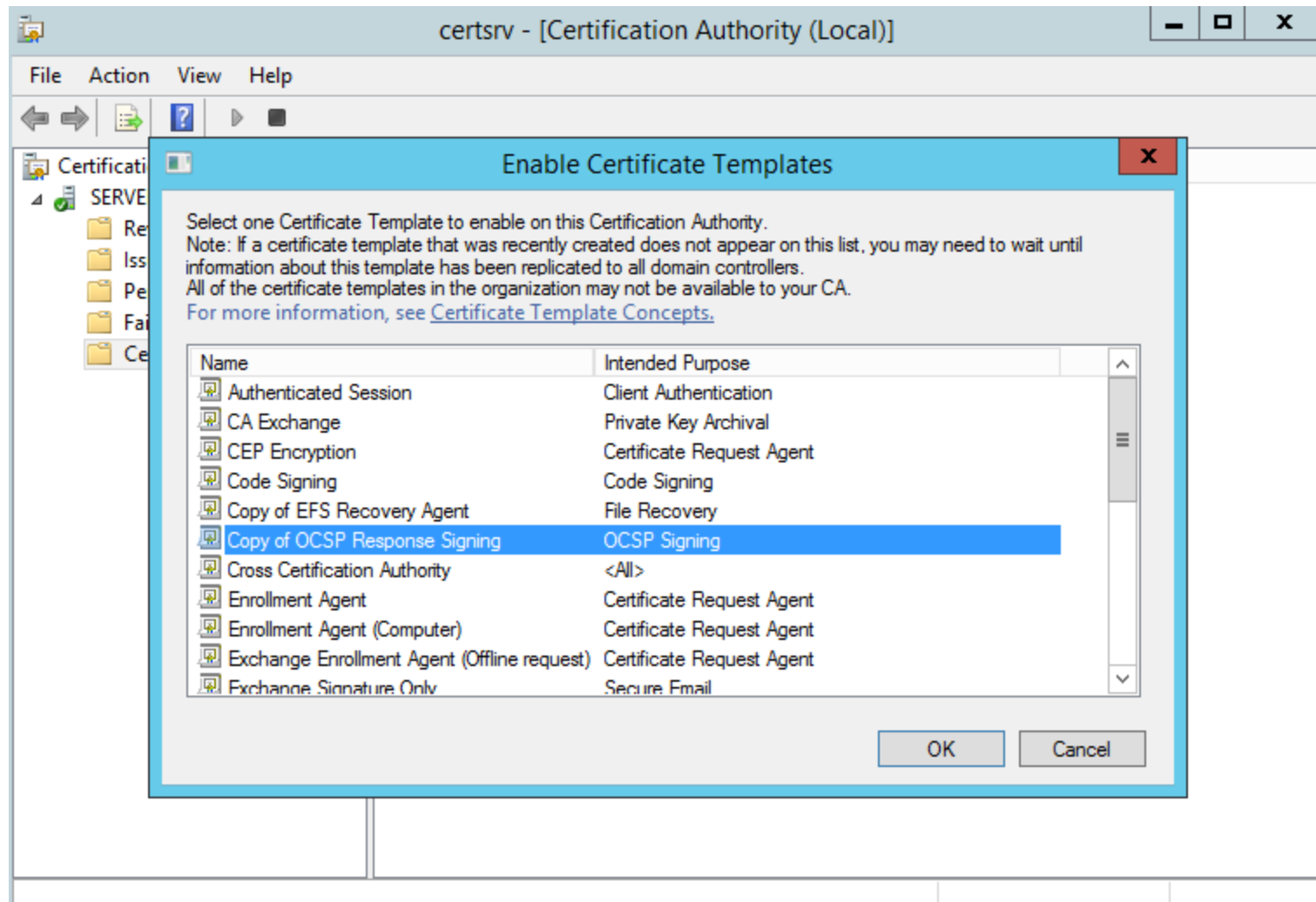
Next >

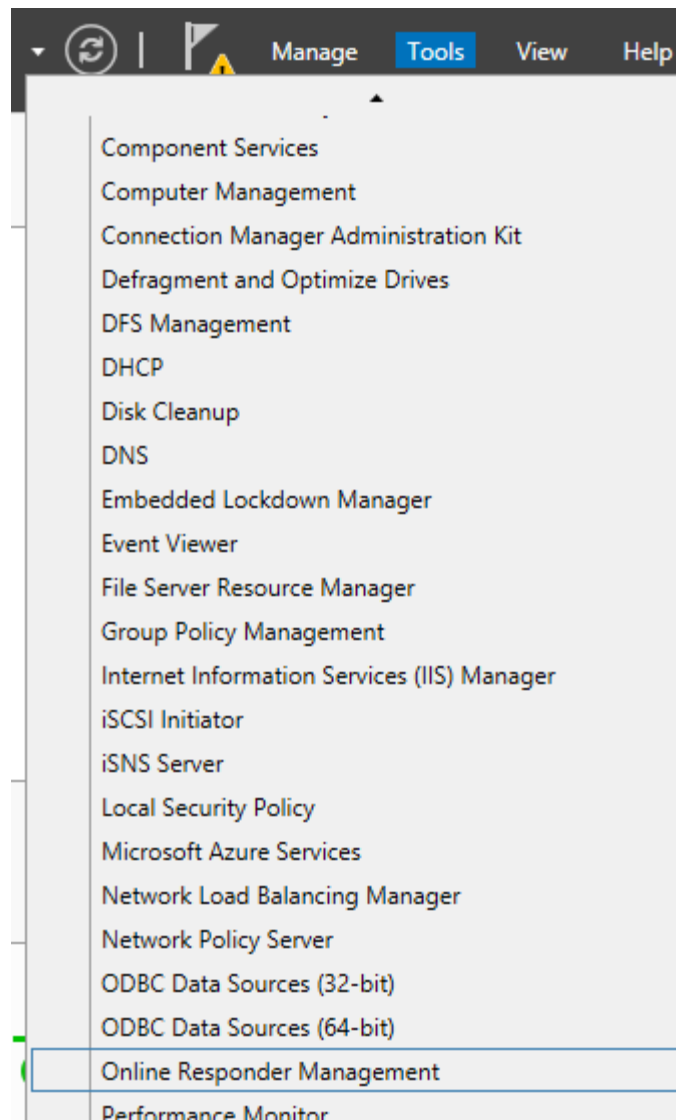
Close

Cancel









ocsp - [Online Responder: WIN-E630K0E1QHE.server2012.com]

File Action View Help

Online Responder: WIN-E630K0E1QHE

Revocation Configuration

Array Configuration

Online Responder Configuration

Configure and manage one or more certificate revocation responders.

Add Revocation Configuration

Refresh

Help

OVERVIEW

The Online Responder Management snap-in helps you configure and manage online certificate status protocol (OCSP) responders with one or more certification authorities.

Use this tool to:

- Manage certificate revocation configurations for an Online Responder Array.
- Monitor the operating status of each member of an Online Responder Array.
- Manage Online Responder Array members.

Revocation Configuration Status

The Status pane identifies Online Responder configurations that are working properly or that may need administrator attention. To get more information, select the Array members.

Note: You may need to click Refresh if recent configuration changes or other administrative actions are not represented here.

[For more information, see Verifying that a revocation configuration is functioning properly.](#)

There are currently no configured revocation configurations available. Use the revocation configuration node to add a revocation configuration.

Add Revocation Configuration



Getting started with adding a revocation configuration

Getting started with addi...

Name the Revocation Co...

Select CA Certificate Loca...

Choose CA Certificate

Select Signing Certificate

Revocation Provider

Welcome to the Add Revocation Configuration Wizard. This wizard helps you add a revocation configuration to your Online Responder Array. To complete this task, you need to:

1. Specify a name for the new revocation configuration
2. Select a CA certificate to associate with the revocation configuration
3. Select a signing certificate to sign Online Responder responses
4. Configure the revocation provider that will process revocation status requests

< Previous

Next >

Finish

Cancel



Online Responder Configuration

Use this s

Overview

The Online Re
certification a

Use this tool to

- Manage cer

- Monitor the

Message On

Revocation C

The Status pa
information, s

Note: You ma

[For more info](#)

There are cur

Add Revocation Configuration

?

X

Name the Revocation Configuration

Getting started with addi...

Name the Revocation Co...

Select CA Certificate Loca...

Choose CA Certificate

Select Signing Certificate

Revocation Provider

The Revocation Configuration name is used to help you identify this revocation configuration. It is recommended to use a name that can identify the CA you would like to associate with this Revocation Configuration.

Name:

< Previous

Next >

Finish

Cancel

Add Revocation Configuration



Select CA Certificate Location

Getting started with addi...

Name the Revocation Co...

Select CA Certificate Loca...

Choose CA Certificate

Select Signing Certificate

Revocation Provider

Specify the location of the CA certificate that you want to associate with this revocation configuration.

- ☒ Select a certificate for an Existing enterprise CA
Select this option if your CA certificate is available in Active Directory or on the CA computer
- ☐ Select a certificate from the Local certificate store
Select this option if the CA certificate is available in a certificate store on the local computer
- ☐ Import certificate from a File
Select this option if the CA certificate has been saved as a file

< Previous

Next >

Finish

Cancel

Add Revocation Configuration



Choose CA Certificate

Getting started with addi...

Name the Revocation Co...

Select CA Certificate Loca...

Choose CA Certificate

Select Signing Certificate

Revocation Provider

In order to check the status of a certificate, a revocation configuration for the Online Responder must identify the CA that issued the certificate.
You can identify this CA by selecting a CA certificate published in Active Directory or by locating a CA computer.

☒ Browse CA certificates published in Active Directory

Browse...

☐ Browse for a CA by Computer name

Browse...

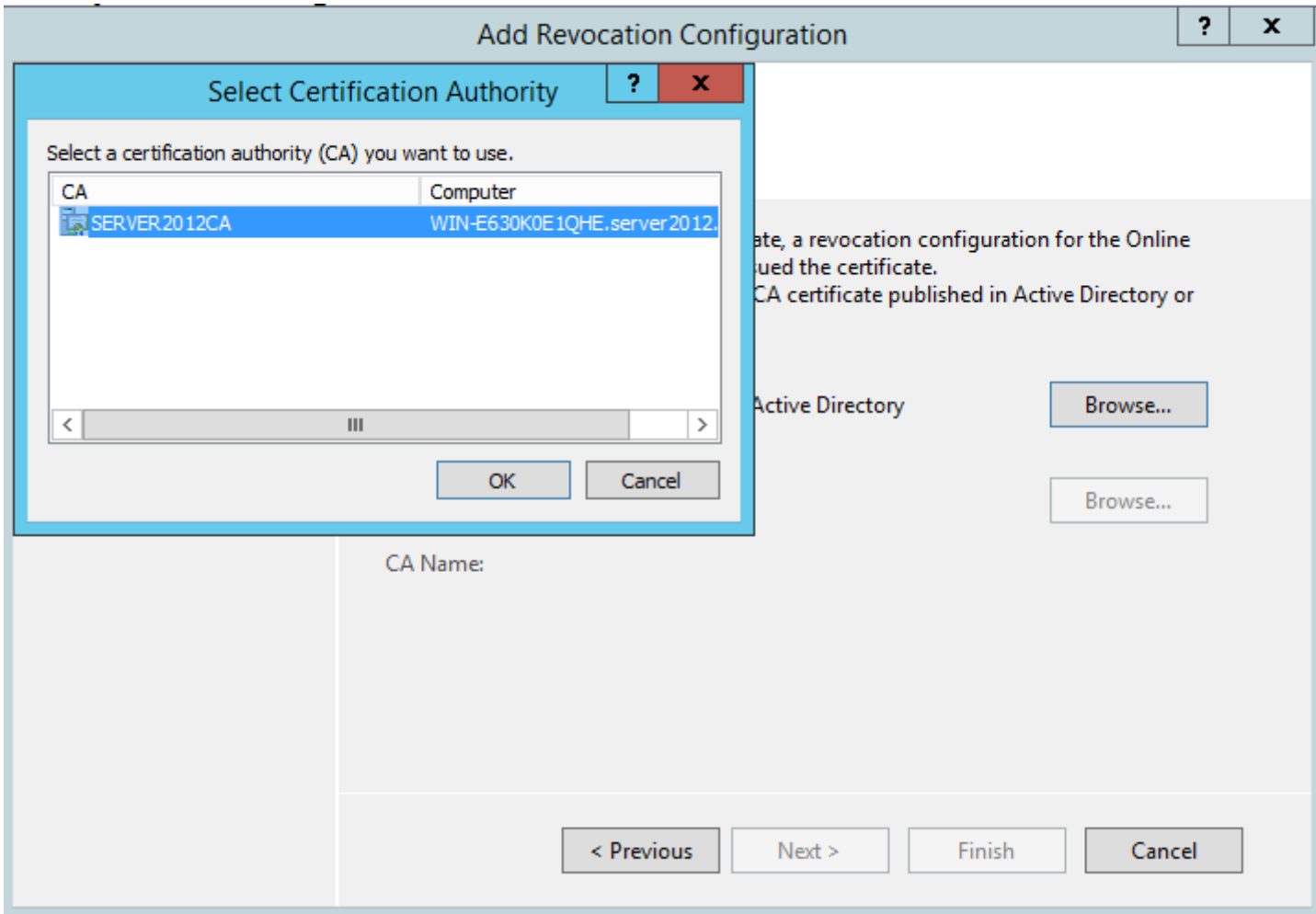
CA Name:

< Previous

Next >

Finish

Cancel



Add Revocation Configuration



Choose CA Certificate

Getting started with addi...

Name the Revocation Co...

Select CA Certificate Loca...

Choose CA Certificate

Select Signing Certificate

Revocation Provider

In order to check the status of a certificate, a revocation configuration for the Online Responder must identify the CA that issued the certificate. You can identify this CA by selecting a CA certificate published in Active Directory or by locating a CA computer.

☒ Browse CA certificates published in Active Directory

Browse...

☐ Browse for a CA by Computer name

Browse...

[CA Name: SERVER2012CA](#)

< Previous

Next >

Finish

Cancel

Add Revocation Configuration



Select Signing Certificate

Getting started with addi...

Name the Revocation Co...

Select CA Certificate Loca...

Choose CA Certificate

Select Signing Certificate

Revocation Provider

Revocation information is signed before it is sent to a client. The Online Responder can select a signing certificate automatically, or you can manually select a signing certificate for each Online Responder.

☒ Automatically select a signing certificate

☒ Auto-Enroll for an OCSP signing certificate

Certification authority: WIN-E630K0E1QHE.server2012.com\SERVER2012CA

Browse...

Certificate Template: Copy of OCSP Response Signing

☐ Manually select a signing certificate

Note: You will need to specify a signing certificate for each member in the Online Responder Array.

☐ Use the CA certificate for the revocation configuration

< Previous

Next >

Finish

Cancel

Online Responder Configuration

Use this

Add Revocation Configuration



Revocation Provider

Getting started with addi...

Name the Revocation Co...

Select CA Certificate Loca...

Choose CA Certificate

Select Signing Certificate

Revocation Provider

A revocation provider is the component of an Online Responder that processes certificate status requests.
To view and edit the properties of the revocation provider, click the Provider button.

Provider...

< Previous

Next >

Finish

Cancel



Online Responder Configuration

Use this snap-in to configure and manage one or more certificate revocation responders.

Overview

The Online Responder Management snap-in helps you configure and manage online certificate status protocol (OCSP) responders with one or more certification authorities.

Use this tool to:

- Manage certificate revocation configurations for an Online Responder Array.
- Monitor the operating status of each member of an Online Responder Array.
- Manage Online Responder Array members.

Revocation Configuration Status

The Status pane identifies Online Responder configurations that are working properly or that may need administrator attention. To get more information, select the Array members.

Note: You may need to click Refresh if recent configuration changes or other administrative actions are not represented here.

[For more information, see Verifying that a revocation configuration is functioning properly.](#)



Server2012CA

Working