

ⓘ We're no longer updating this content regularly. Check the [Microsoft Product Lifecycle](#) for information about how this product, service, technology, or API is supported.

Recommended Version

✕

 Filter by title

⋮ / [AD CS Certificate Request \(Enrollment\) Processing](#) /

⊕ ⋮

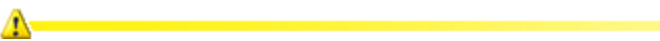
# Event ID 53 — AD CS Certificate Request (Enrollment) Processing

Article • 08/26/2009

## In this article


- [Event Details](#)
- [Resolve](#)
- [Verify](#)
- [Related Management Information](#)

Applies To: Windows Server 2008 R2



One of the primary functions of a certification authority (CA) is to evaluate certificate requests from clients and, if predefined criteria are met, issue certificates to those clients. In order for certificate enrollment to succeed, a number of elements must be in place before the request is submitted, including a CA with a valid CA certificate; properly configured certificate templates, client accounts, and certificate requests; and a way for the client to submit the request to the CA, have the request validated, and install the issued certificate.

## Event Details

 Expand table

Product:	Windows Operating System
ID:	53
Source:	Microsoft-Windows-CertificationAuthority
Version:	6.1
Symbolic Name:	MSG_DN_CERT_DENIED_WITH_INFO
Message:	Active Directory Certificate Services denied request %1 because %2. The request was for %3. Additional information: %4

## Resolve

### Remove conditions that prevent a certificate request from being approved

Problems in chain building are a common cause for certificate requests to fail. Use the following procedure to validate the certificate chain for the certification authority (CA) and fix any problems that are identified:

- Confirm user account information in Active Directory Domain Services (AD DS).

- Confirm certificate template information.
- Confirm the certificate chain for the CA.
- Check the most recent certificate revocation lists (CRLs).
- Publish a new CRL.

If this does not resolve the problem, check and resolve issues in the following areas:

- The failed requests queue for the CA
- AD DS connectivity

Signatures that are required to complete the certificate request might not be available. If this is the case:

- Enable additional users with registration authority certificates to sign certificate requests.
- Modify the certificate template to require fewer registration authority signatures.
- Submit the certificate request again.

## Confirm user account information in AD DS

To perform this procedure, you must have membership in **Domain Admins**, or you must have been delegated the appropriate authority.

To confirm user account information:

1. On the domain controller, click **Start**, point to **Administrative Tools**, and click **Active Directory Users and Computers**.
2. In the console tree, select the domain and user group in which the user's account should be located.
3. If the user account exists, right-click the account, click **Properties**, and confirm that the user has a properly configured Domain Name System (DNS) name.

## Confirm certificate template information

To perform this procedure, you must have Manage CA permission, or you must have been delegated the appropriate authority.

To confirm certificate template information:

1. On the computer hosting the CA, click **Start**, type **certtmpl.msc** and press ENTER.
2. Right-click the certificate template that you are troubleshooting, and confirm that the user or group has permissions to enroll for a certificate based on this template.

## Confirm the certificate chain for the CA

To validate the chain for the CA:

1. Click **Start**, type **mmc**, and then press ENTER.
2. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
3. On the **File** menu, click **Add/Remove Snap-in**, click **Certificates**, and then click **Add**.
4. Click **Computer account**, and click **Next**.
5. Select the computer hosting the CA, click **Finish**, and then click **OK**.
6. Select each CA certificate in the certificate chain, and click **View Certificate**.
7. Click the **Details** tab, and click **Copy to File** to start the Certificate Export Wizard. Save each certificate with a .cer extension.
8. Open a command prompt and run the following command on each CA certificate: **certutil -urlfetch -verify <CAcert.cer>** and then press ENTER. Replace **<CAcert.cer>** with the name of a CA certificate file that you saved in step 7.
9. Use the same command with a certificate file for an end-entity (user or computer) certificate issued by the CA to confirm CRLs for the CA itself as well as its

chain.

10. Resolve any problems identified in the command line output.

## Generate and publish new CRLs

If the command line output indicates that a CRL for a CA has expired, generate new base and delta CRLs on the CA and copy them to the required locations. You may need to restart an offline CA to do this.

On the CA, check the current published CRL. By default, the CA creates CRLs in the folder %windir%\System32\CertSrv\CertEnroll. If the CRLs currently in this location have expired or are invalid, you can use the following procedure to publish a new CRL.

To publish a new CRL by using the Certification Authority snap-in:

1. On the computer hosting the CA, click **Start**, point to **Administrative Tools**, and click **Certification Authority**.
2. Select the CA, and expand the folders below the CA name.
3. Right-click the **Revoked Certificates** folder.
4. Click **All Tasks**, and then click **Publish**.

You can also generate and publish CRLs from a command prompt.

To publish a CRL by using the Certutil command-line tool:

1. On the computer hosting the CA, click **Start**, type **cmd** and press ENTER..
2. Type **certutil -CRL** and press ENTER.\*\* \*\*

If a CRL is identified as unavailable but a valid CRL exists in the local directory on the CA, confirm that the CA can connect to the CRL distribution point, and then use the preceding steps to generate and publish CRLs again.

CRLs can be published manually to Active Directory Domain Services (AD DS) by using the following command:

```
certutil -dspublish"<crlname.crl>" ldap:///CN=<CA name>,CN=<CA hostname>,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=<contoso>,DC=<com>?certificateRevocationList?base?objectClass=cRLDistributionPoint
```

Replace \*crlname.crl \*with the name of your CRL file, <CA name> and <CA hostname> with your CA name and the name of the host on which that CA runs, and <contoso> and <\*com> \*with the namespace of your Active Directory domain.

## Confirm configured CRL distribution points

Check all configured CRL distribution points to confirm that publication was successful and that new CRLs are available on the network.

To perform this procedure, you must have Manage CA permission, or you must have been delegated the appropriate authority.

To check the configured CRL distribution points by using the Certification Authority snap-in:

1. On the computer hosting the CA, click **Start**, point to **Administrative Tools**, and click **Certification Authority**.
2. Right-click the name of the CA, and click **Properties**.
3. Click the **Extensions** tab.
4. Review the configured CRL distribution points and confirm that the names are valid.

To check the configured CRL distribution point URLs by using Certutil:

1. Open a command prompt window on the CA.
2. Type **certutil -getreg ca\crlpublicationurls** and press ENTER.

- 3. Review the configured CRL distribution points and confirm that the names are valid.

## Check the failed requests queue on the CA

To perform this procedure, you must have Manage CA permission, or you must have been delegated the appropriate authority.

To check the failed requests queue on the CA by using the Certification Authority snap-in:

- 1. On the computer hosting the CA, click **Start**, point to **Administrative Tools**, and click **Certification Authority**.
- 2. Click **Failed Requests**.
- 3. Look for failed requests that were submitted at or near the time of the event, and check columns such as the **Request Disposition Message**, **Request Status Code**, and **Requester Name** for additional diagnostic information.

To check failed requests by using Certutil:

- 1. On the computer hosting the CA, click **Start**, type **cmd** and press ENTER.
- 2. Type **certutil -view LogFail** and press ENTER.
- 3. Type **certutil -view -restrict requestID="<nnn>"** and press ENTER. Replace *nnn* with the Request ID of one of the failed requests in the output of the LogFail command.

## Confirm AD DS connectivity

To confirm an Active Directory Certificate Services (AD CS) connection to AD DS:

- 1. On the CA, open a command prompt window.
- 2. Type **ping <server\_FQDN>**, where *server\_FQDN* is the fully qualified domain name (FQDN) of the domain controller (for example, server1.contoso.com), and then press ENTER.
- 3. If the ping was successful, you will receive a reply similar to the following:

Reply from IP\_address: bytes=32 time=3ms TTL=59

Reply from IP\_address: bytes=32 time=20ms TTL=59

Reply from IP\_address: bytes=32 time=3ms TTL=59

Reply from IP\_address: bytes=32 time=6ms TTL=59 3

- 4. At the command prompt, type **ping <IP\_address>**, where *IP\_address* is the IP address of the domain controller, and then press ENTER.
- 5. If you can successfully connect to the domain controller by IP address but not by FQDN, this indicates a possible issue with Domain Name System (DNS) host name resolution. If you cannot successfully connect to the domain controller by IP address, this indicates a possible issue with network connectivity, firewall configuration, or Internet Protocol security (IPsec) configuration.

## Issue additional registration authority certificates

To perform this procedure, you must be a member of local **Administrators** on the computer hosting the CA, or you must have been delegated the appropriate authority.

To issue additional registration authority certificates:

- 1. On the computer hosting the CA, click **Start**, type **certtmpl.msc**, and then press ENTER.
- 2. In the details pane, right-click the registration authority certificate template, and then click **Properties**.

- On the **Security** tab, add the names of the users or groups to whom you want to issue registration authority certificates.
- In **Group or user names**, click one of the new objects, and then, on **Permissions for*ObjectName***, under the **Allow** column, select the **Read** and **Enroll** check boxes.
- Repeat the previous step for each new object, and click **OK**.
- Click **Start**, point to **Administrative Tools**, and click **Certification Authority**.
- Double-click the name of the CA.
- Right-click the **Certificate Templates** container, click **New**, and then click **Certificate Template to Issue**.
- Select the certificate template, and click **OK**.

## Modify certificate template signature requirements

To perform this procedure, you must have Manage CA permission, or you must have been delegated the appropriate authority.

To modify certificate template signature requirements:

- On the computer hosting the CA, click **Start**, type **certtmpl.msc**, and then press ENTER.
- In the details pane, right-click the certificate template that you want to change, and then click **Properties**.
- Click the **Issuance Requirements** tab.
- Under **This number of authorized signatures**, enter the number of registration authority signatures you want to use.
- Repeat the previous step for each new object, and click **OK**.
- Click **Start**, point to **Administrative Tools**, and click **Certification Authority**.
- Double-click the name of the CA.
- Right-click the **Certificate Templates** container, click **New**, and then click **Certificate Template to Issue**.
- Select the certificate template, and click **OK**.

## Verify

To perform this procedure, you must have permission to request a certificate.

To confirm that certificate request processing is working properly:

- Click **Start**, type **certmgr.msc**, and then press ENTER.
- If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
- In the console tree, double-click **Personal**, and then click **Certificates**.
- On the **Action** menu, point to **All Tasks**, and click **Request New Certificate** to start the Certificate Enrollment wizard.
- Use the wizard to create and submit a certificate request for any type of certificate that is available.
- Under **Certificate Installation Results**, confirm that the enrollment completes successfully and no errors are reported. You can also click **Details** to view additional information about the certificate.

## Related Management Information

[AD CS Certificate Request \(Enrollment\) Processing](#)

[Active Directory Certificate Services](#)

