

Enable Remote access from intranet with TLS-SSL certificate (Advanced)

Last updated by | Veena Pachauri | Mar 8, 2023 at 11:10 PM PST

Enable Remote access from intranet with TLS/SSL certificate (Advanced)

For an detailed overview of the SSL/TLS Strong encryption technology please go [here](#).

Certificate could be a general TLS certificate for a Web Server under the following requirements:

- The certificate must be a publicly trusted X509 v3 certificate. We recommend that you use certificates that are issued by a public partner certification authority (CA).
- Each integration runtime node must trust this certificate.
- We recommend Subject Alternative Name (SAN) certificates because all the fully qualified domain names (FQDN) of integration runtime nodes are required to be secured by this certificate. (WCF TLS/SSL validate only check last DNS Name in SAN was fixed in .NET Framework 4.6.1. Refer to Mitigation: X509CertificateClaimSet.FindClaims Method | Microsoft Docs)
- Wildcard certificates (*) is not supported.
- The certificate must have private key (like PFX format).
- The certificate can use any key size supported by Windows Server 2012 R2 for TLS/SSL certificates.
- We only support CSP (Cryptographic Service Provider) certificate so far. Certificates that use CNG keys (Key Storage Provider) aren't supported.

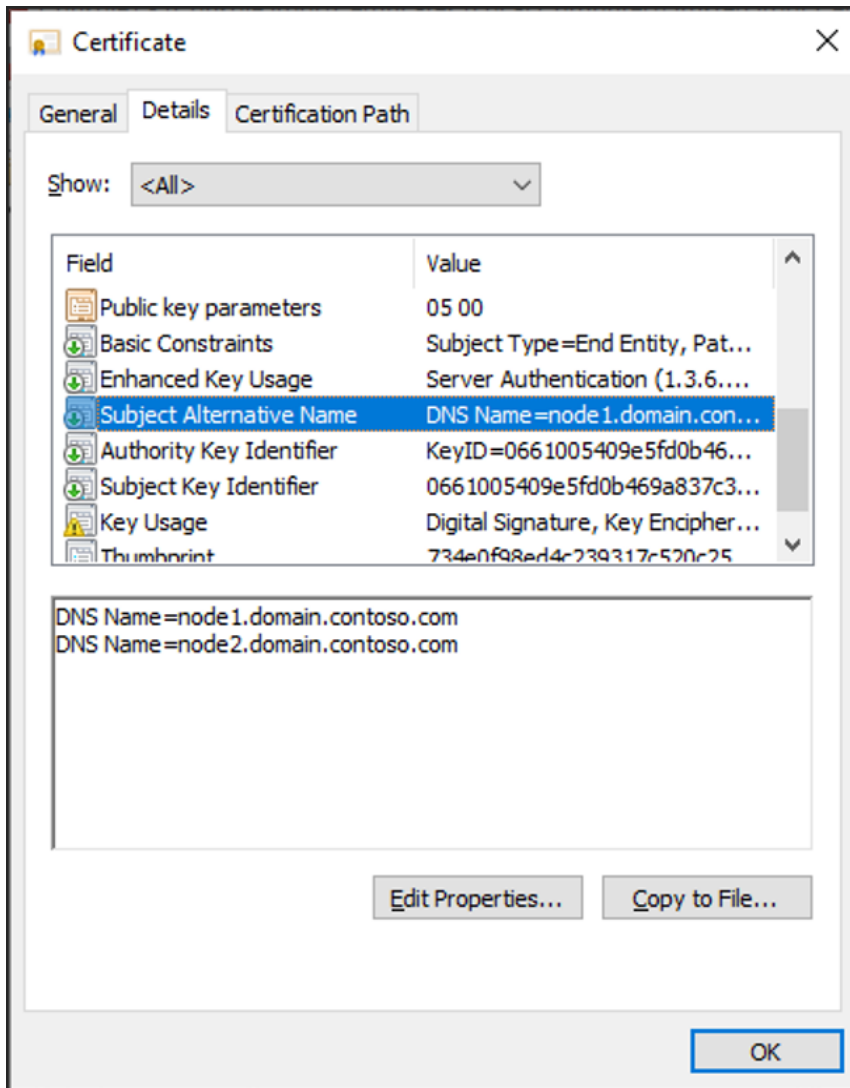
Step-by-step instructions:

1. Run below PowerShell command on all machines to get their FQDNs

```
[System.Net.Dns]::GetHostByName("localhost").HostName
```

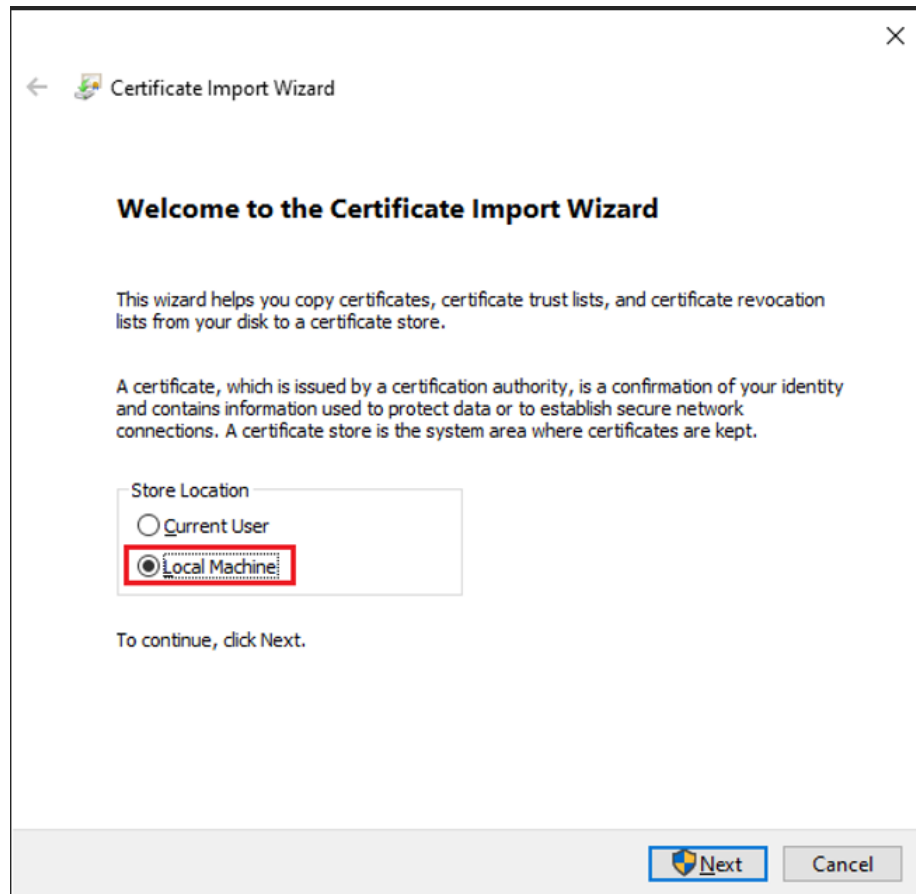
For example, the FQDNs are [node1.domain.contoso.com](#) and [node2.domain.contoso.com](#).

2. Generate a certificate with the FQDNs of all machines in Subject Alternative Name



3. Install the certificate on all nodes to Local Machine -> Personal so that it can be selected on Integration Runtime configuration manager.

1. Click on the certificate and install it.



2. Select Local Machine and enter the password.
3. Select Place all certificates in the following store. Click Browse. Select Personal.
4. Select Finish to install the certificate.

4. Enable Remote access from intranet

During Self-hosted Integration Runtime node registration:

- Select Enable remote access from intranet and select Next.

Microsoft Integration Runtime Configuration Manager



New Integration Runtime (Self-hosted) Node

Integration Runtime (Self-hosted) node name:

DAVIZEN-DEV



Below is the list of Integration Runtime (Self-hosted) Nodes:

SHIR-Demo

DAVIZEN-DEV : Current New Node

☒ Enable remote access from intranet

Next

Cancel

- Set the TCP Port (8060 by default). Make sure the port is open on firewall.
- Click Select. In the pop-up window, choose the right certificate and select Finish.

Microsoft Integration Runtime Configuration Manager



Remote access from intranet

Tcp Port: 8060

TLS/SSL Certifica...

Select

Remove

☐ Enable remote access without TLS/SSL certificate

Windows Security

Select Certificate

Select a certificate to bind to the SSL port.



*.davizen-test.com

Issuer: *.davizen-test.com

Valid From: 5/26/2021 to 5/26/2022

[Click here to view certificate properties](#)

[More choices](#)

OK

Cancel

Finish

Cancel

Note:
- The data
- For untrus
[Cert Require](#)

always encrypted using HTTPS.
Node communication channel. [TLS/SSL](#)

After Self-hosted Integration Runtime node is registered:

Please note that self-hosted Integration Runtime can change the remote access settings only when it has single node, which is by design. Otherwise, the radio button cannot be checked.

The screenshot shows the 'Microsoft Integration Runtime Configuration Manager' window. The 'Settings' tab is selected, and the 'Remote access from intranet' section is active. The text explains that remote access is used for setting/encrypting linked services and enabling node-node communication. Three radio buttons are present: 'Disable', 'Enable without TLS/SSL certificate (Basic)', and 'Enable with TLS/SSL certificate (Advanced)'. The 'Advanced' option is selected and highlighted with a red box. Below the radio buttons, there is a 'TLS/SSL Certificate' field with 'contoso.com' entered, a 'Select' button, and a 'Remove' button. A 'Tcp Port' field shows '8060'. A 'Note' section states that data transfer is encrypted using HTTPS and recommends adding a TLS/SSL certificate for untrusted networks, with a link to 'TLS/SSL Cert Requirements'. At the bottom right are 'OK' and 'Close' buttons. A status bar at the very bottom shows a green checkmark and the text 'Connected to the cloud service (Data Factory V2)'.

Microsoft Integration Runtime Configuration Manager

Home Settings Diagnostics Update Help

Remote access from intranet

Remote access from intranet is used for

1. Setting/Encrypting Linked Service/Credential from within your Intranet environment.
2. For enabling Node-node communication during High Availability and Scalability setup (2+ nodes).

☐ Disable

☐ Enable without TLS/SSL certificate (Basic)

☒ Enable with TLS/SSL certificate (Advanced)

TLS/SSL Certificate:

Tcp Port:

Note:

- The data transfer between Integration Runtime (Self-hosted) node and the Cloud data stores is always encrypted using HTTPS.
- For untrusted network, we recommend adding a TLS/SSL certificate (advanced) to secure Node-Node communication channel. [TLS/SSL Cert Requirements](#)

✓ Connected to the cloud service (Data Factory V2)

1. Self-hosted Integration Runtime Configuration Manager -> Settings -> Remote access from intranet. Click Change.
2. Choose Enable with TLS/SSL certificate (Advanced).

3. Click Select. In the pop-up window, choose the right certificate and select OK.

The screenshot shows the 'Microsoft Integration Runtime Configuration Manager' window. The 'Settings' tab is selected. Under the 'Remote access from intranet' section, the following options are visible:

- Remote access from intranet is used for:
 1. Setting/Encrypting Linked Service/Credential from within your Intranet environment.
 2. For enabling Node-node communication during High Availability and Scalability setup (2+ nodes).
- Radio button options:
 - ☐ Disable
 - ☐ Enable without TLS/SSL certificate (Basic)
 - ☒ Enable with TLS/SSL certificate (Advanced)
- TLS/SSL Certificate:
- Tcp Port:
- Note:
 - The data transfer between Integration Runtime (Self-hosted) node and the Cloud data stores is always encrypted using HTTPS.
 - For untrusted network, we recommend adding a TLS/SSL certificate (advanced) to secure Node-Node communication channel. [TLS/SSL Cert Requirements](#)
-

At the bottom of the window, a status bar shows a green checkmark and the text 'Connected to the cloud service (Data Factory V2)'.

Verify the remote access settings in Self-hosted Integration Runtime Configuration Manager.

Microsoft Integration Runtime Configuration Manager

Home Settings Diagnostics Update Help

Remote access from intranet ⓘ

Status: Enabled

Port: 8060 Ssl Encrypted

Change

HTTP Proxy ⓘ

Current Proxy: No proxy

Change

✓ Connected to the cloud service (Data Factory V2)

Microsoft Integration Runtime Configuration Manager

Home Settings Diagnostics Update Help

Remote access from intranet

Remote access from intranet is used for

1. Setting/Encrypting Linked Service/Credential from within your Intranet environment.
2. For enabling Node-node communication during High Availability and Scalability setup (2+ nodes).

☐ Disable

☐ Enable without TLS/SSL certificate (Basic)

☒ Enable with TLS/SSL certificate (Advanced)

TLS/SSL Certificate:

Tcp Port:

Note:

- The data transfer between Integration Runtime (Self-hosted) node and the Cloud data stores is always encrypted using HTTPS.
- For untrusted network, we recommend adding a TLS/SSL certificate (advanced) to secure Node-Node communication channel. [TLS/SSL Cert Requirements](#)

✓ Connected to the cloud service (Data Factory V2)

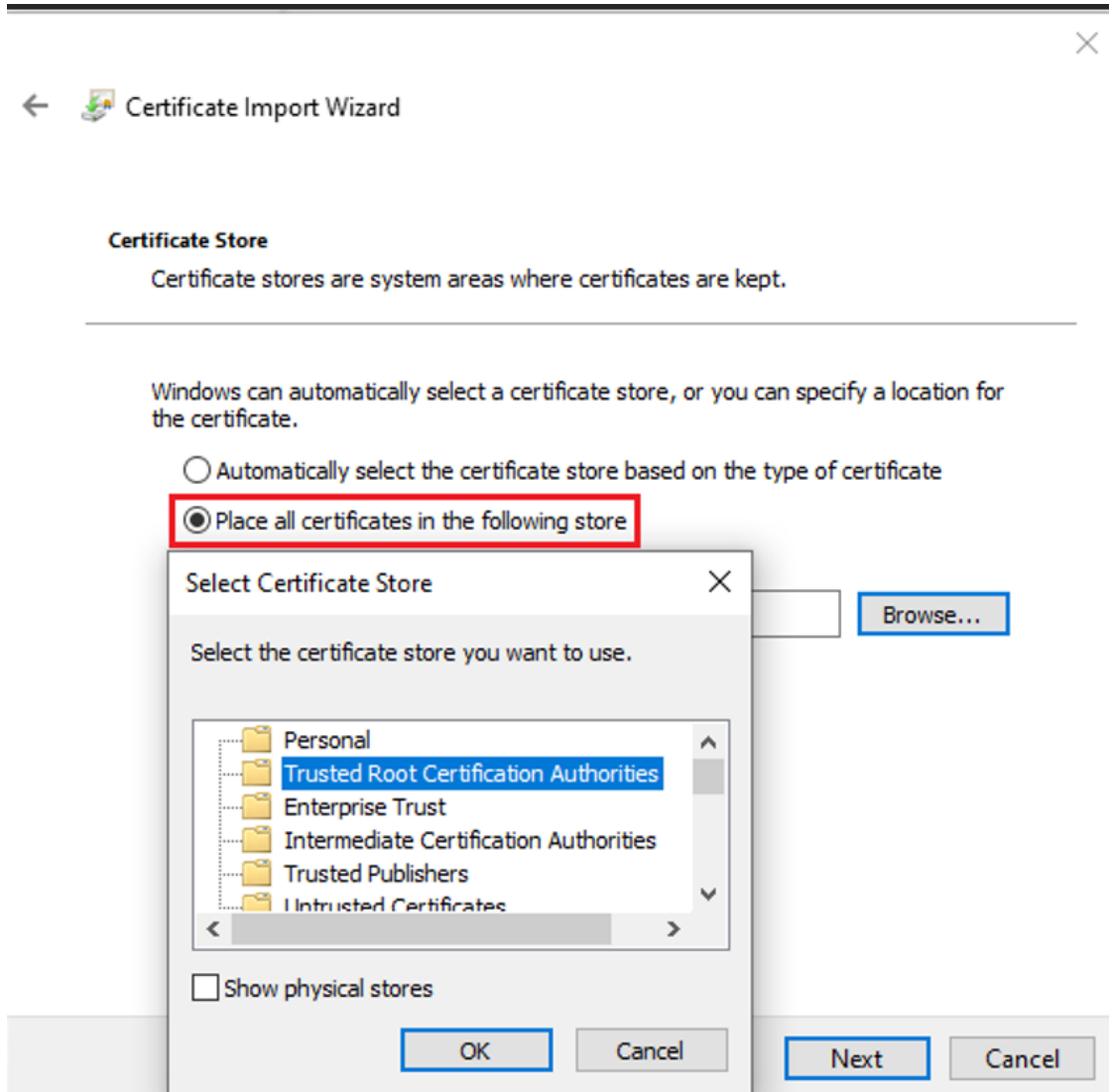
5. Using self-signed certificate

Generate and export self-signed certificate (this step can be skipped if you already have the certificate):

1. Generate self-signed certificate via PowerShell (with elevated privileges): `New-SelfSignedCertificate -DnsName contoso.com , node1.domain.contoso.com , node2.domain.contoso.com -Provider "Microsoft Enhanced RSA and AES Cryptographic Provider" -CertStoreLocation cert:\LocalMachine\My`
2. To export the generated certificate with a private key to a password protected PFX file, you will need its thumbprint. It can be copied from the results of `New-SelfSignedCertificate` command. For example, it is `CEB5B4372AA7BF877E56BCE27542F9F0A1AD197F`.
3. Export the generated certificate with private key via PowerShell (with elevated privileges): `$CertPassword = ConvertTo-SecureString -String "Password" -Force -AsPlainText Export-PfxCertificate -Cert cert:\LocalMachine\My\CEB5B4372AA7BF877E56BCE27542F9F0A1AD197F -FilePath C:\self-signedcertificate.pfx -Password $CertPassword`
4. You have exported the certificate with private key to `C:\self-signedcertificate.pfx`.

Install the certificate on all nodes to: **Local Machine** -> **Trusted Root Certification Authorities** store:

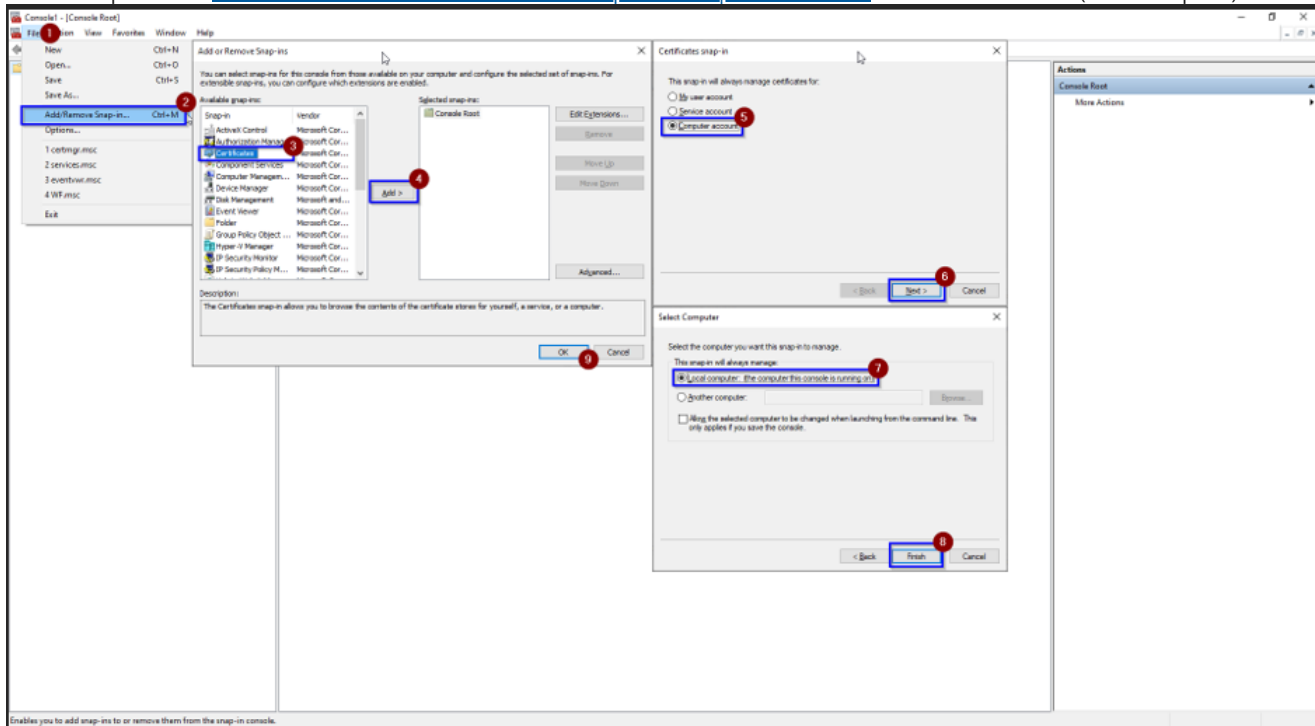
1. Click on the certificate and install it.
2. Select Local Machine and enter the password.
3. Select Place all certificates in the following store. Click Browse. Select Trusted Root Certification Authorities.
4. Select Finish to install the certificate.



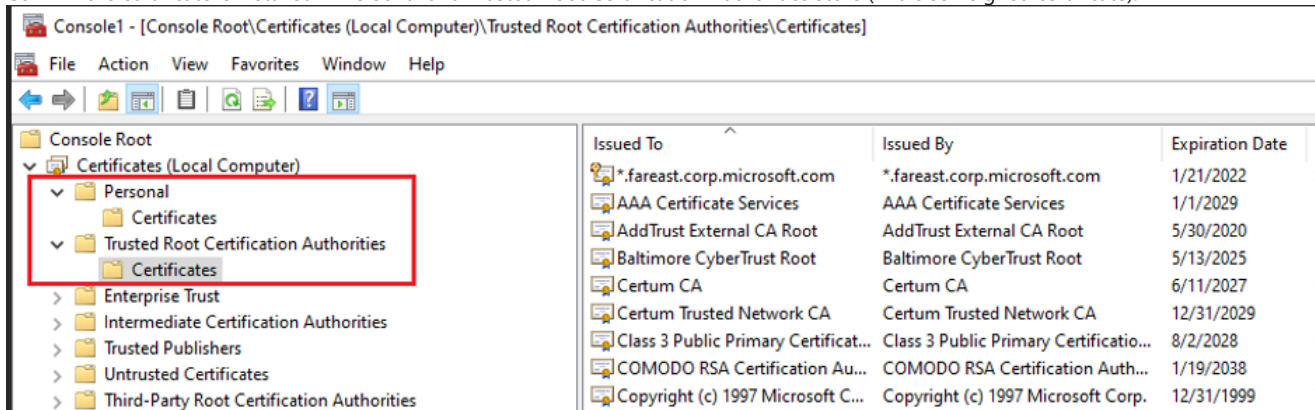
6. Trouble shooting

Verify the certificate exists in the target store:

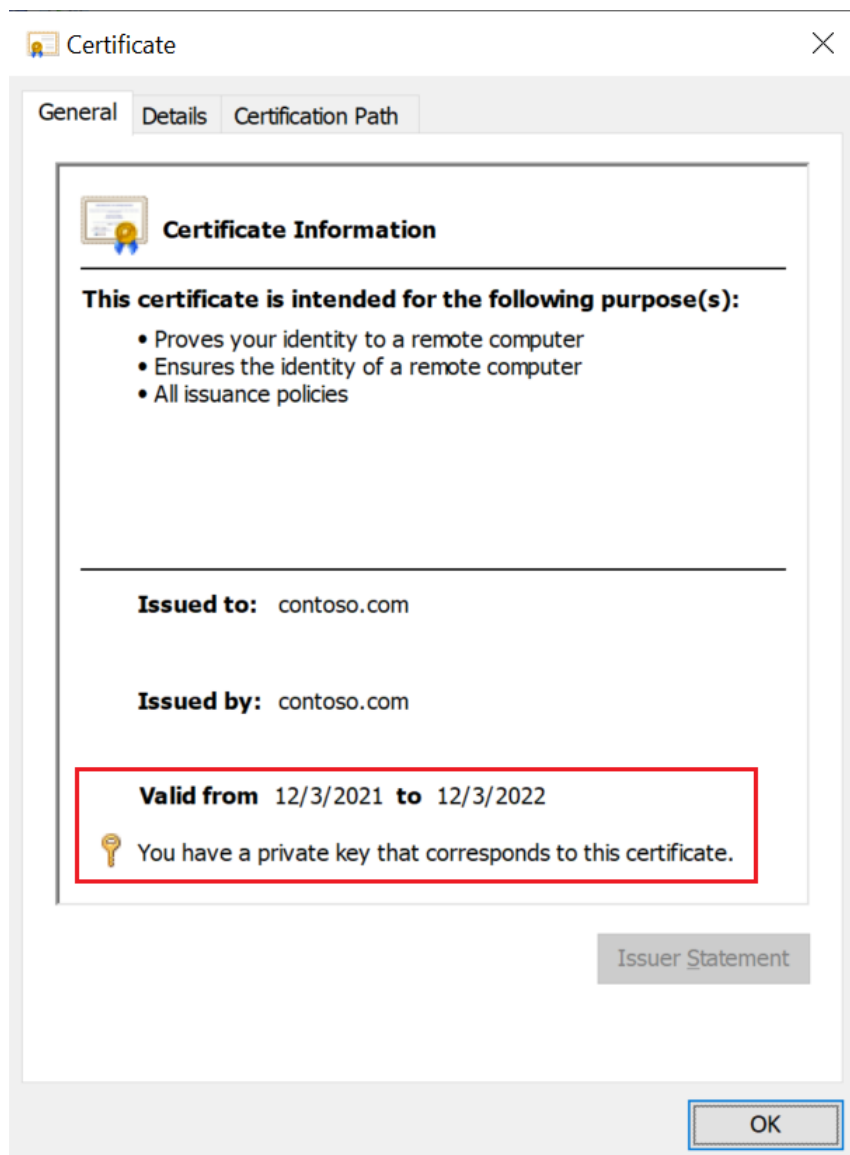
1. Follow this procedure [How to: View certificates with the MMC snap-in - WCF | Microsoft Docs](#) to view Certificates (Local Computer) in the MMC snap-in.



2. Confirm the certificate is installed in Personal and Trusted Root Certification Authorities store (If it is self-signed certificate):



Verify the certificate has private key and isn't expired:



Make sure the Service account for Self-hosted integration runtime (default account is NT SERVICE\DIAHostService) has read permission to the private keys of certificate.

1. Right click on the certificate -> All Tasks -> Manage Private Keys.
2. If no, grant the permission, Apply and save.

Updating a certificate in a cluster:

The process to renew certificate is not much different from adding the new one.

1. Follow steps 1 ~ 3 to install the new certificate all nodes. If it is self-signed certificate, need additional step [#5](#) to trust it.
2. Follow step 4.2 [After Self-hosted Integration Runtime node is registered](#) to update the certificate on all nodes (select the new one).