

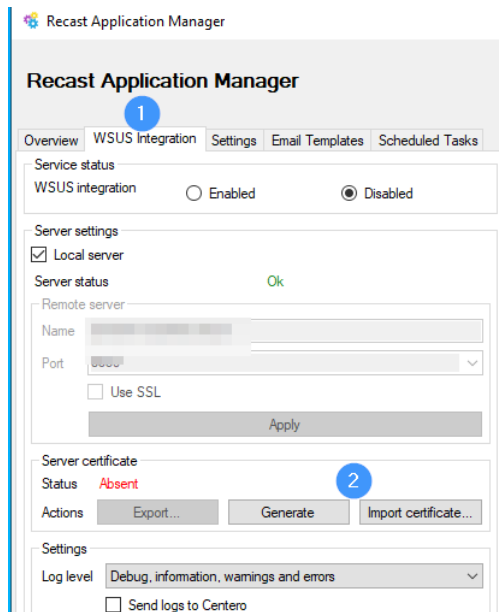
Publish Server Certificate

Last Modified on 2026-06-08

In order to deploy third-party updates via WSUS, the server and clients must have the same self-signed certificate. Client devices are able to install AM-deployed applications as soon as the certificate is installed.

To generate a certificate or import one:

1. Launch Application Manager and go to the **WSUS integration** tab.
2. Click **Generate** to create a new self-signed certificate, or **Import certificate** to use an existing certificate.



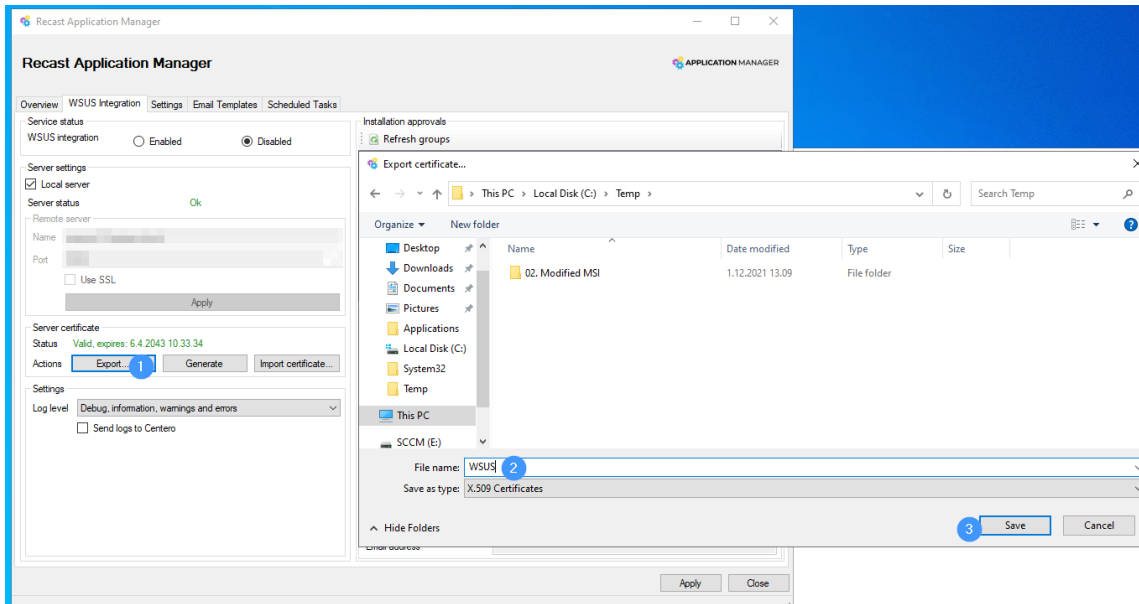
3. Select **OK** if there is no existing certificate. If you are changing an existing certificate, Application Manager will confirm the replacement. Click **Yes** if you would like to replace an existing certificate.

When a valid certificate exists, it must be deployed to clients in order to deploy the software updates. We recommend doing this by using a group policy object.

To export an existing certificate:

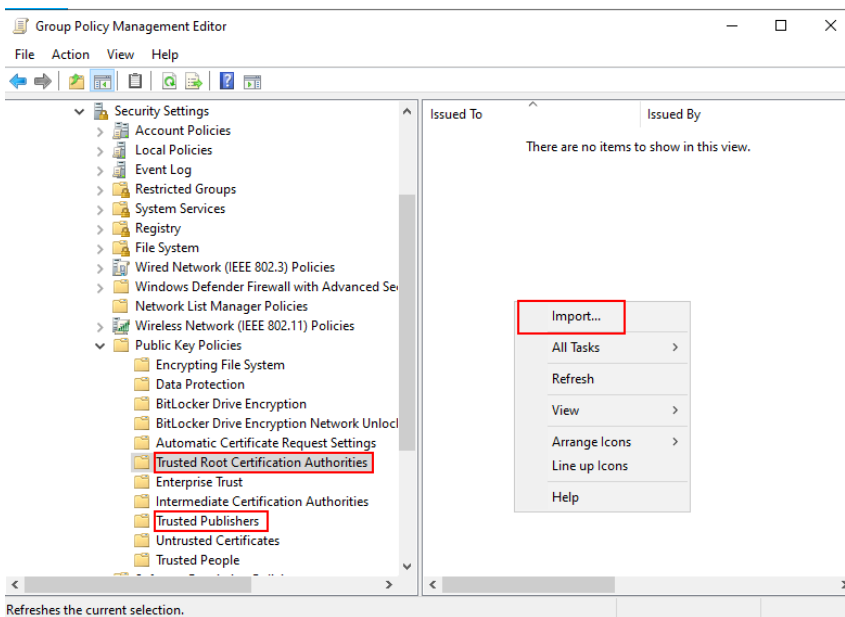
1. Click **Export**.
2. Enter the filename.
3. **Save** the certificate to a location where you can access it with a group policy object (GPO) management tool.

Recast



To set up the group policy object:

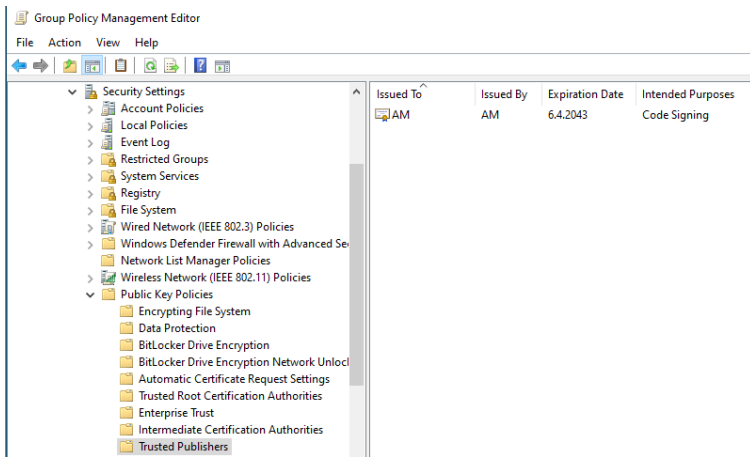
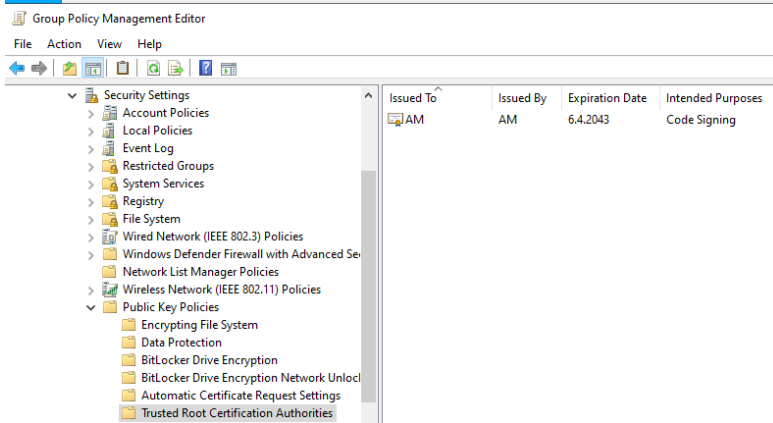
1. Open **Group Policy Management** (gpmc.msc). Create a new GPO or edit an existing one.
2. Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.
3. Import the certificate to the **Trusted Root Certification Authorities** and **Trusted Publishers** folders by right-clicking the empty space in the right-hand pane and selecting **Import**.



4. Follow the prompts and find the certificate.

End Result

Recast



5. Deploy the Group Policy Object.