Publish Server Certificate

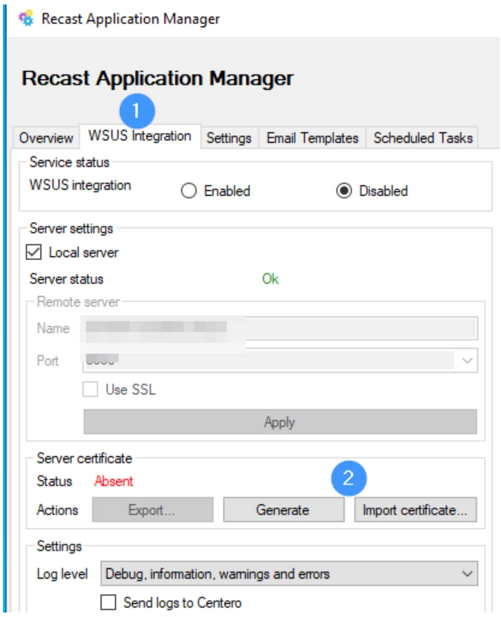
Last Modified on 08.25.23

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.



Recast Application Manager

Recast Application Manager

Service status

WSUS integration ○ Enabled ● Disabled

Server settings

☑ Local server

Server status Ok

Remote server

Name [redacted]

Port [redacted]

□ Use SSL

Server certificate

Status Absent

Settings

Log level Debug, information, warnings and errors

□ Send logs to Centero

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.

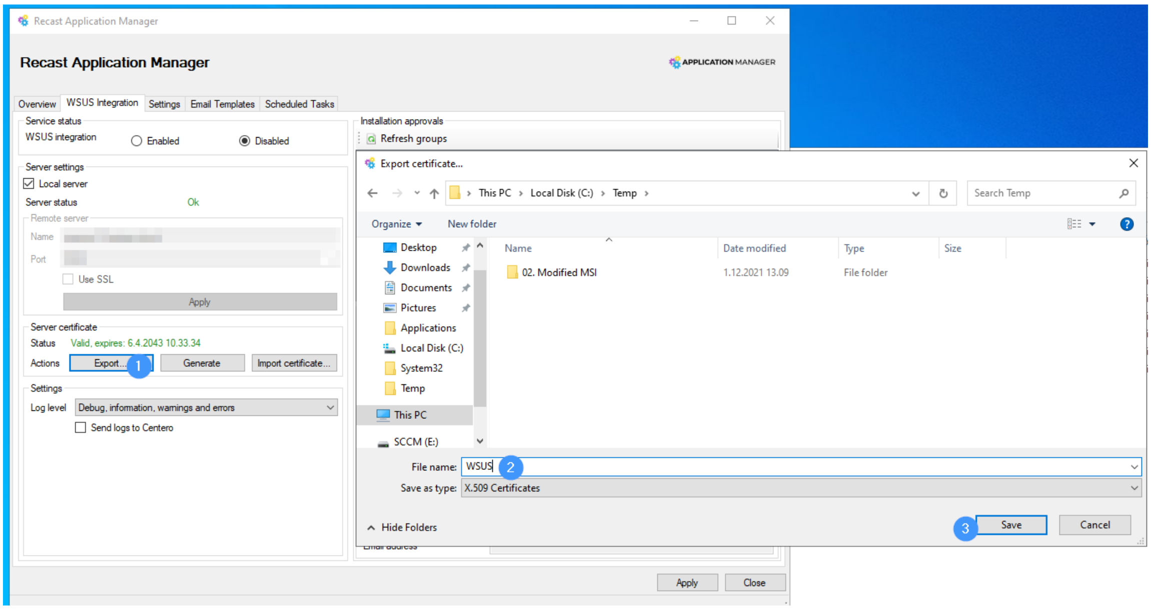
When a valid certificate exists, it must be deployed to clients in order to deploy the software updates. We recommend doing this by using a group policy object.

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.



WSUS integration ○ Enabled ● Disabled

☑ Local server

Server status Ok

□ Use SSL

Status Valid, expires: 6.4.2043 10.33.34

Log level Debug, information, warnings and errors

□ Send logs to Centero

02. Modified MSI 1.12.2021 13.09 File folder

File name: WSUS

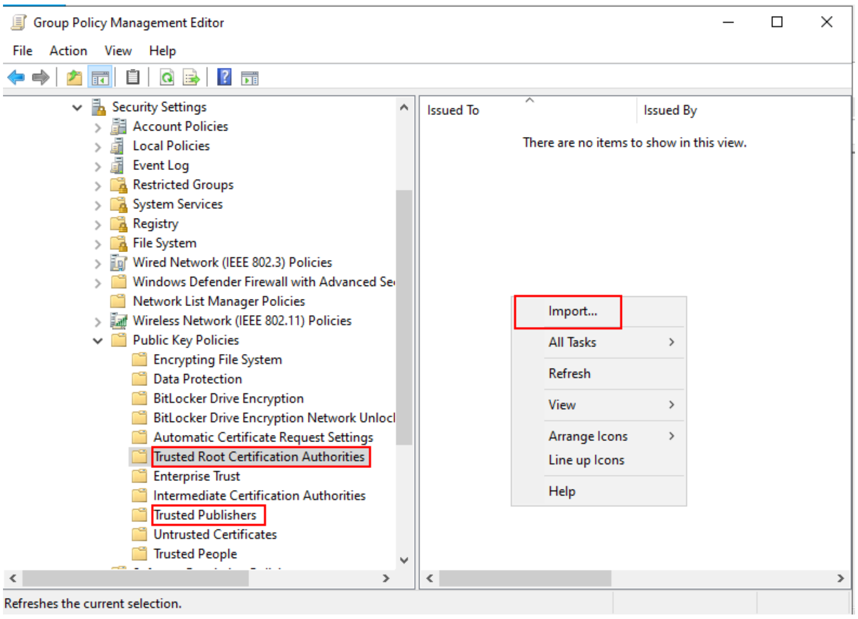
Save as type: X.509 Certificates

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**.



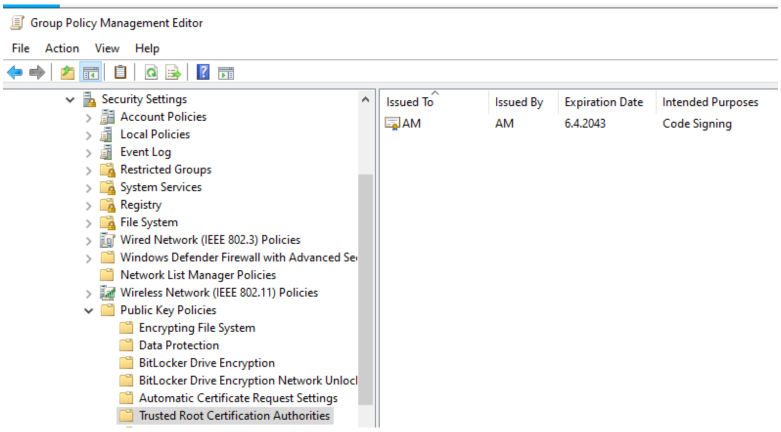
Group Policy Management Editor
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Se
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Encrypting File System
Data Protection
BitLocker Drive Encryption
BitLocker Drive Encryption Network Unlocl
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Trusted People
Issued To
Issued By
Import...
All Tasks
Refresh
View
Arrange Icons
Line up Icons
Help

There are no items to show in this view.

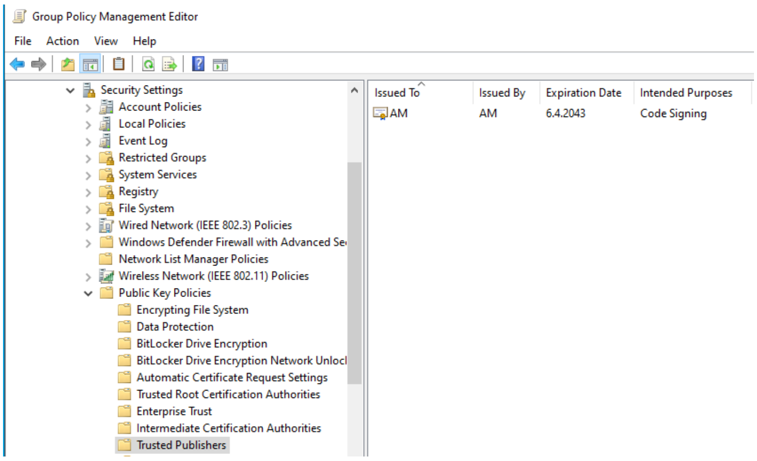
Refreshes the current selection.

4. Follow the prompts and find the certificate.

End Result


Group Policy Management Editor
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Se
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Encrypting File System
Data Protection
BitLocker Drive Encryption
BitLocker Drive Encryption Network Unlocl
Automatic Certificate Request Settings
Trusted Root Certification Authorities

Issued To	Issued By	Expiration Date	Intended Purposes
AM	AM	6.4.2043	Code Signing


Group Policy Management Editor
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Se
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Encrypting File System
Data Protection
BitLocker Drive Encryption
BitLocker Drive Encryption Network Unlocl
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers

Issued To	Issued By	Expiration Date	Intended Purposes
AM	AM	6.4.2043	Code Signing

5. Deploy the Group Policy Object.