Renewing Microsoft Federation Gateway Certificates

# Overview

This document describes how to go about renewing the self-signed Microsoft Federation Gateway Certificates.

# Remove the Exchange Federation Certificate

On the internal Hub Transport server, run the following from an Exchange Management Shell:

* List all Federation certificates:
  + $Servers = Get-ExchangeServer; $Servers | foreach {Get-ExchangeCertificate -Server $\_ | Where {$\_.Services -match 'Federation'}} | Format-List Identity,Thumbprint,Services,Subject
* Make a note of the thumbprint, and then run:
  + Remove-exchangecertificate -thumbprint <thumbprint>
* Confirm that there are no more Federation certificates:
  + $Servers = Get-ExchangeServer; $Servers | foreach {Get-ExchangeCertificate -Server $\_ | Where {$\_.Services -match 'Federation'}} | Format-List Identity,Thumbprint,Services,Subject

# Create a new Exchange Federation Certificate

On the internal Hub Transport server, run the following from an Exchange Management Shell:

* $ski = [System.Guid]::NewGuid().ToString(“N”)
* New-ExchangeCertificate -FriendlyName “Microsoft Federation Gateway” -DomainName <yourdomain> -Services Federation -KeySize 2048 -PrivateKeyExportable $true -SubjectKeyIdentifier $ski

# Create a new Federation Trust

On the internal Hub Transport server, run the following from an Exchange Management Shell:

* Make a note of the thumbprint, and then run:
  + Set-FederationTrust -Identity "Microsoft Federation Gateway" -Thumbprint <thumbprint> -RefreshMetaData
* Publish the new federation certificate:
  + Set-FederationTrust -Identity "Microsoft Federation Gateway" -PublishFederationCertificate
* List the federation trusts:
  + Get-FederationTrust | Format-List \*priv\*
* Refresh the metadata:
  + Set-FederationTrust -Identity "Microsoft Federation Gateway" -Thumbprint <thumbprint> -RefreshMetaData
* Set the federated organisation identifier:
  + Set-FederatedOrganizationIdentifier -DelegationFederationTrust "Microsoft Federation Gateway" -AccountNamespace <yourdomain> -Enabled $trust

# Configure Auth Config

On the internal Hub Transport server, run the following from an Exchange Management Shell:

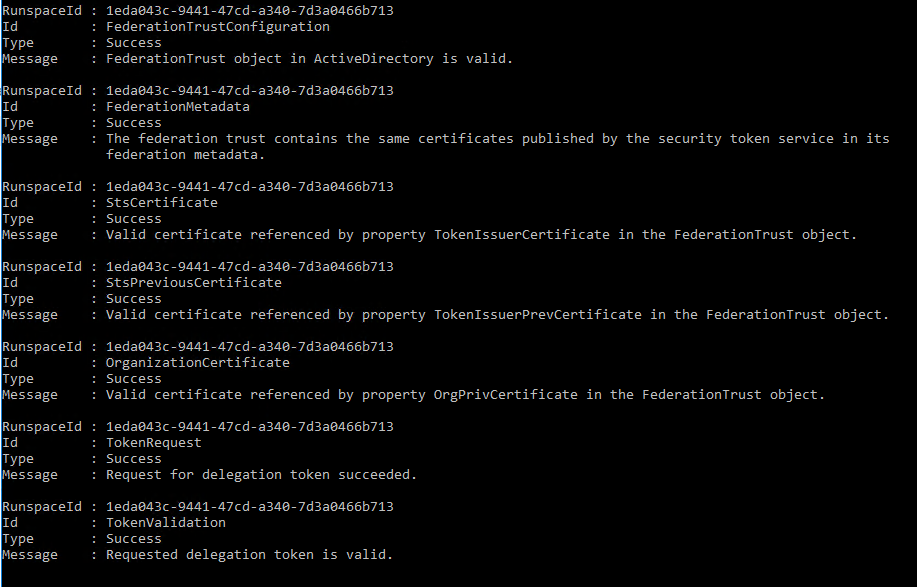
* $a=get-date
* Set-AuthConfig -NewCertificateThumbprint <thumbprint> –NewCertificateEffectiveDate $a
* Click accept to continue even though the certificate effective date is not 48 hours into the future
* Set-AuthConfig –PublishCertificate
* Make sure that you remove any potential reference to the previous certificate (which might not exist anymore) by running:
  + Set-AuthConfig -ClearPreviousCertificate
* Run iisreset from an elevated command prompt (do this on all Internal Hub Transport servers)

# Test Federation

On the internal Hub Transport server, run the following from an Exchange Management Shell:

* Test-FederationTrust -UserIdentity <smtp-address>

All six steps should complete successfully:



**Note – it is normal for the last step to fail. This is due to the different time zone which the MFG (Microsoft Federation Gateway) is in. The test should pass when run again after 7 hours.**

# Renew Federated Domain Proof

It will be necessary to renew the domain proof for each federated domain. To do this, a new TXT record must be created in the public DNS of the federated domain.

Retrieve the new domain proof record:

* Get-FederatedDomainProof
  + Enter the name for the primary federated domain: <yourdomain>
* Make a note of the DNS record and add a new TXT record in the public DNS with that value
* Perform the above for all federated domains
* Log in to the EAC (Exchange Admin Centre), click *Organisation*, then *Modify*
* Click the *Update* button and ensure that the status says *Succeeded* for each federated domain
* If there are any failures, ensure that the domain proof DNS TXT record contains the correct value in public DNS