.

ADFS

Swapping certs is a bitch. dont forget to set the TLS cert for the server in addition to the service certificate. this isnt visible in the mmc.

Change the certificate for SSL and Service-Communications using the following commands:

Set-AdfsSslCertificate –Thumbprint XXX
Set-AdfsCertificate -CertificateType "Service-Communications" –Thumbprint XXX

Restart the adfs service.

If you havent given permissions to the new certificates private key to the service account, do that too.

If using a windows WAP, you likely broke the trust too. fix it by running Install-webapplicationproxy

```
$FScredential = Get-CredentialInstall-WebApplicationProxy -FederationServiceName
"FS01.Contoso.com" -FederationServiceTrustCredential $FScredential -CertificateThumbprint
"0a1b2c3d0a1b2c3d0a1b2c3d0a1b2c3d0a1b2c3d"
```

use a user account with admin on the ADFS box, and the certificate used should be the one you intend to present to clients. you can get the thumbprint with:

```
Get-ChildItem -Path cert: -Recurse | select Subject, FriendlyName, Thumbprint | Format-List
```

https://docs.microsoft.com/en-us/powershell/module/webapplicationproxy/install-webapplicationproxy?view=windowsserver2022-ps

---

Revision #2
Created 26 January 2022 03:51:05 by Nolan
Updated 26 January 2022 03:59:47 by Nolan