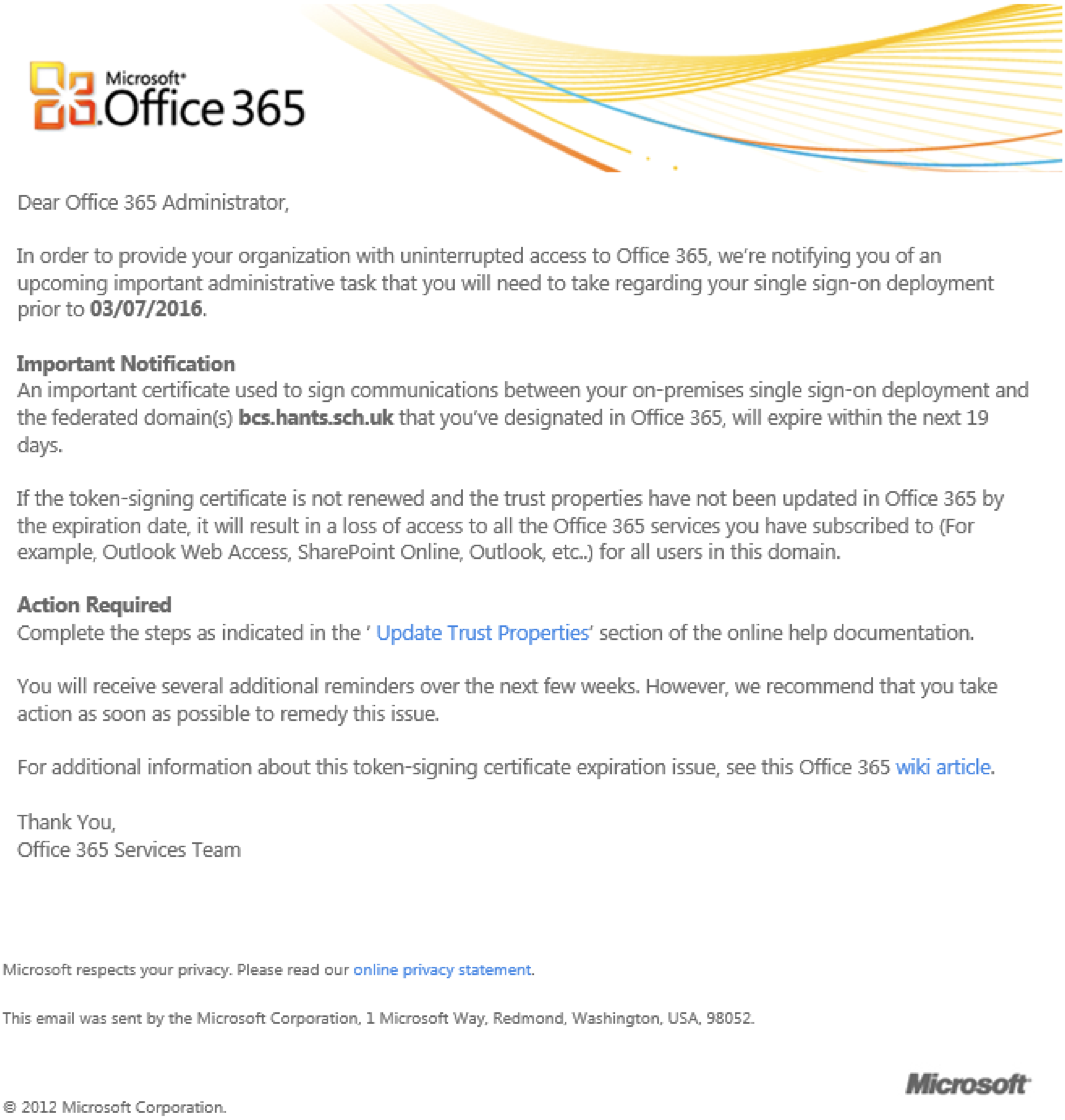
Office 365 certificate renewal

If you are an office 365 Administrator you may have received an email from Microsoft similar to the one shown below showing that your office 365 certificate is going to expire. The process to update this can be seen here (https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-o365-certs/) however there may be further steps required to ensure that your 365 system continues to function properly after renewing your certificate.



Dear Office 365 Administrator,

In order to provide your organization with uninterrupted access to Office 365, we're notifying you of an upcoming important administrative task that you will need to take regarding your single sign-on deployment prior to **03/07/2016**.

Important Notification
An important certificate used to sign communications between your on-premises single sign-on deployment and the federated domain(s) **bcs.hants.sch.uk** that you've designated in Office 365, will expire within the next 19 days.

If the token-signing certificate is not renewed and the trust properties have not been updated in Office 365 by the expiration date, it will result in a loss of access to all the Office 365 services you have subscribed to (For example, Outlook Web Access, SharePoint Online, Outlook, etc..) for all users in this domain.

Action Required
Complete the steps as indicated in the ' Update Trust Properties' section of the online help documentation.

You will receive several additional reminders over the next few weeks. However, we recommend that you take action as soon as possible to remedy this issue.

For additional information about this token-signing certificate expiration issue, see this Office 365 wiki article.

Thank You,
Office 365 Services Team

Microsoft respects your privacy. Please read our online privacy statement.

This email was sent by the Microsoft Corporation, 1 Microsoft Way, Redmond, Washington, USA, 98052.

Symptom – My certificate is updated and email is flowing but I cannot access my global address list or set up new outlook profiles. Accompanied by event viewer error 342 Source: ADFS stating Token validation failed - invalid credentials on mailboxes.

Likely cause – your certificate has updated but the ADFS service account does not have read access to it.

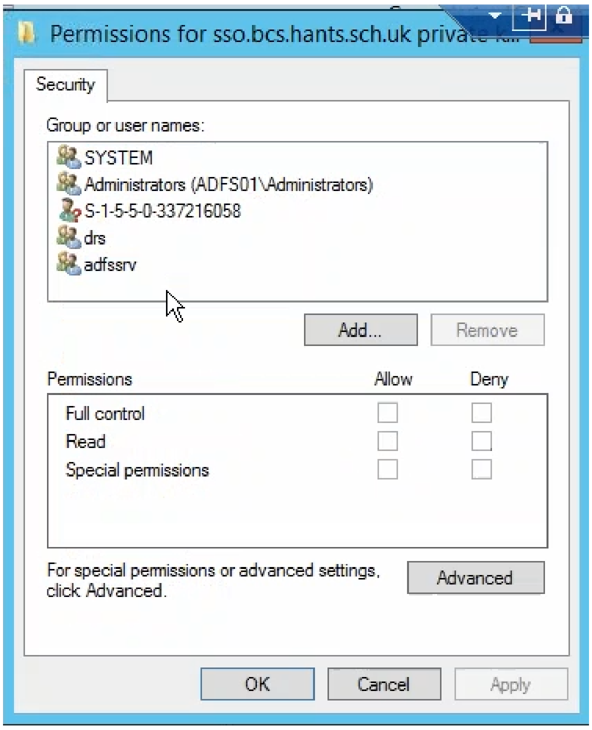
Solution – Set the permissions on the new certificate so that the account running your ADFS service has read or higher access. To do so follow these steps

Step 1 – Identify which account the ADFS service is running under, do this by right clicking the properties of the active directory federation services service in services.msc and selecting properties and under the log on tab it will show you under 'this account'.

Step 2 – Open MMC and add the certificates snap in with the local computer account.

Step 3 – Under personal right click the new certificate and select manage private keys

Step 4 – Grant the ADFS service account you identified earlier read access or higher permissions



Permissions for sso.bcs.hants.sch.uk private k...

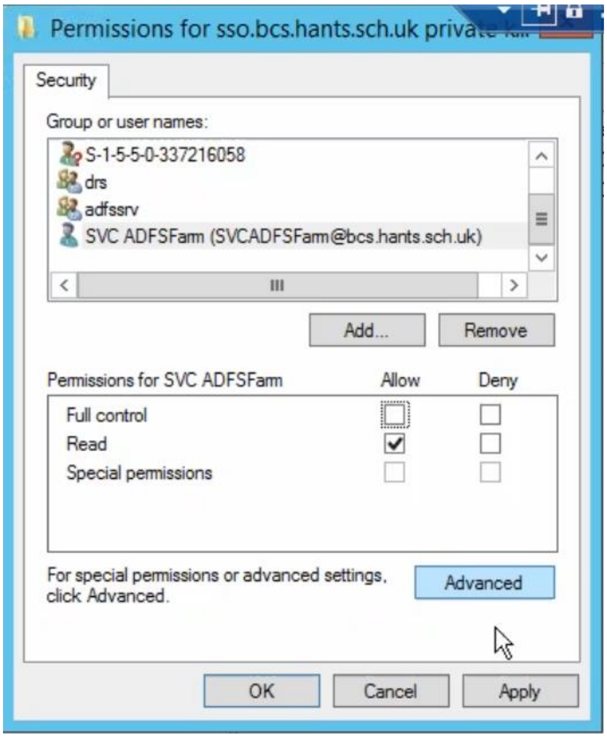
Security

Group or user names:

- SYSTEM
- Administrators (ADFS01\Administrators)
- S-1-5-5-0-337216058
- drs
- adfssrv

Permissions	Allow	Deny
Full control	□	□
Read	□	□
Special permissions	□	□

For special permissions or advanced settings, click Advanced.



Permissions for sso.bcs.hants.sch.uk private k...

Security

Group or user names:

- S-1-5-5-0-337216058
- drs
- adfssrv
- SVC ADFSFarm (SVCADFSFarm@bcs.hants.sch.uk)

Permissions for SVC ADFSFarm	Allow	Deny
Full control	□	□
Read	☑	□
Special permissions	□	□

For special permissions or advanced settings, click Advanced.

Step 5 – Restart the ADFS service

Symptom – No mail is flowing and outlook cannot connect.

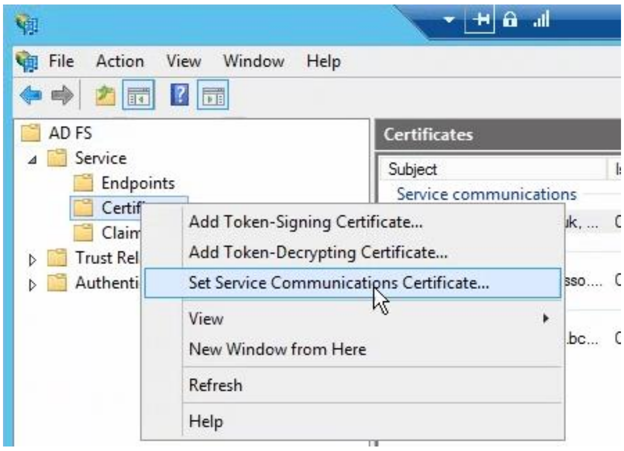
Likely Cause – The new ADFS certificate has not been set as the service communications certificate

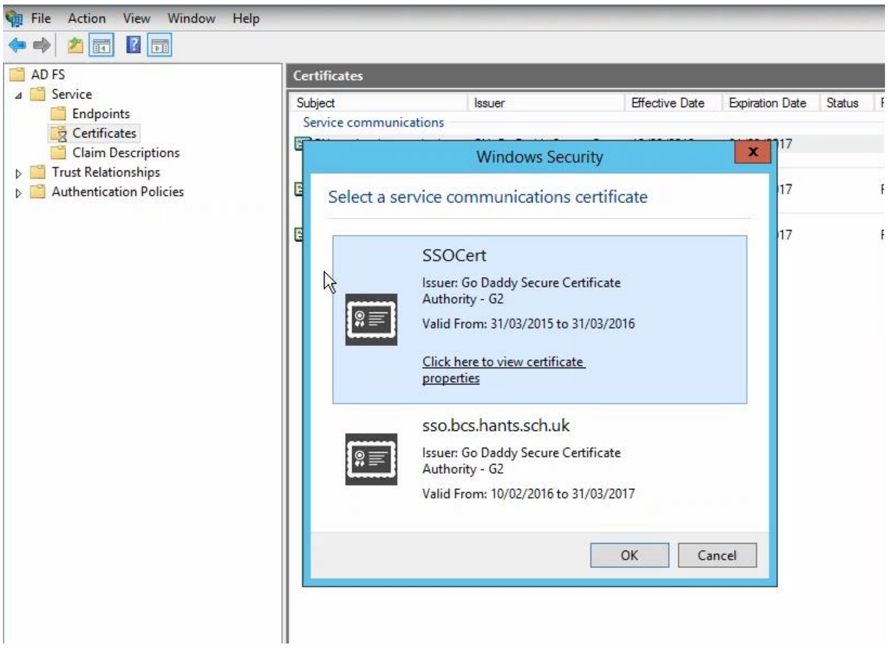
Solution - You will need to set the new non expired certificate as the ADFS services communications certificate from within the ADFS control panel located in Administrative tools. Follow these steps to do so

Step 1 – Open Administrative tools on your ADFS server and launch ‘ADFS’

Step 2 – Expand service and right click on certificates

Step 3 – Click Set service communications certificate and pick the new one





Windows Security

Select a service communications certificate

SSOCert
Issuer: Go Daddy Secure Certificate Authority - G2
Valid From: 31/03/2015 to 31/03/2016
Click here to view certificate properties

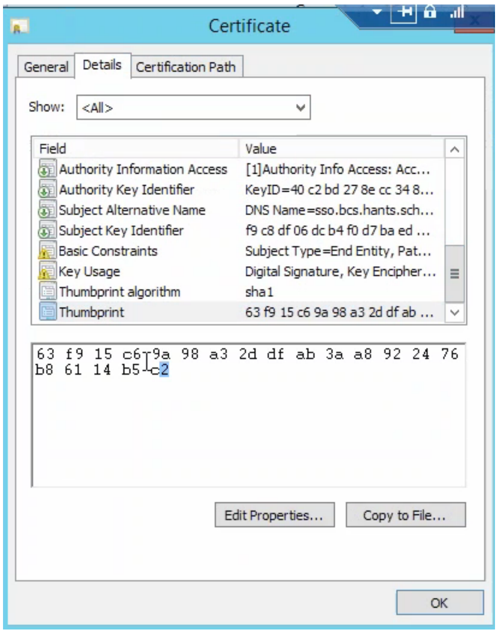
sso.bcs.hants.sch.uk
Issuer: Go Daddy Secure Certificate Authority - G2
Valid From: 10/02/2016 to 31/03/2017

Symptom – my organisations ADFS Sign in page has an expired certificate

Likely cause – you need to update the bindings via powershell for HTTPS for AD FS and the device registration service

Solution – You will need your new valid certificates thumbnail and access to powershell on the ADFS server (Microsoft ref https://technet.microsoft.com/en-us/library/dn479374(v=wps.630).aspx). Perform the following steps:

Step 1 – Ensure that a valid new certificate has been imported to the personal store on the ADFS server and grab the certificates thumbprint (this can be found in the details pane of the certificate when opened)



Show: <All>

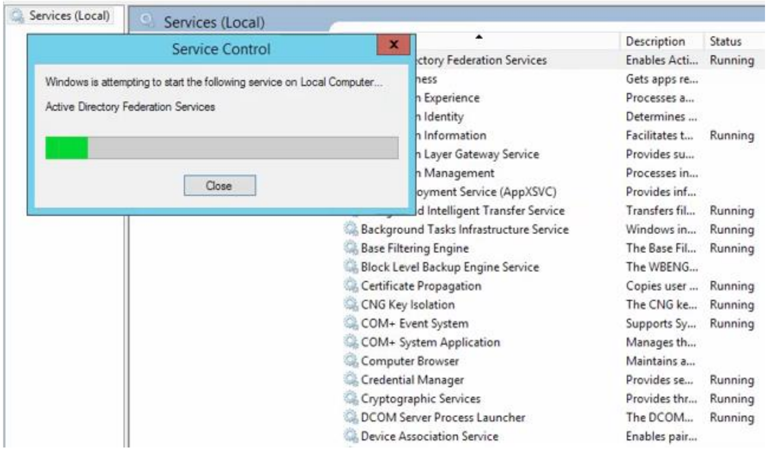
Field	Value
Authority Information Access	[1]Authority Info Access: Acc...
Authority Key Identifier	KeyID=40 c2 bd 27 8e cc 34 8...
Subject Alternative Name	DNS Name=sso.bcs.hants.sch...
Subject Key Identifier	f9 c8 df 06 dc b4 f0 d7 ba ed ...
Basic Constraints	Subject Type=End Entity, Pat...
Key Usage	Digital Signature, Key Encipher...
Thumbprint algorithm	sha1
Thumbprint	63 f9 15 c6 9a 98 a3 2d df ab ...

```
63 f9 15 c6 9a 98 a3 2d df ab 3a a8 92 24 76
b8 61 14 b5 c2
```

Step 2 – Copy it to a text file and remove the spaces, you will need this in the next step

Step 3 – Open powershell and enter the command Set-AdfsSslCertificate – Thumbprint *YOUR THUMBPRINT* For example: Set-adfssslcertificate -Thumbprint 63f915c69a98a32ddfab3aa8922476b86114b5c2

Step 4 – Press enter and then restart your ADFS service, once restarted the ADFS login web page should now use the new certificate for its bindings



Windows is attempting to start the following service on Local Computer...

Active Directory Federation Services

	Description	Status
ctory Federation Services	Enables Acti...	Running
ness	Gets apps re...	
n Experience	Processes a...	
n Identity	Determines ...	
n Information	Facilitates t...	Running
n Layer Gateway Service	Provides su...	
n Management	Processes in...	
oyment Service (AppXSVC)	Provides inf...	
d Intelligent Transfer Service	Transfers fil...	Running
Background Tasks Infrastructure Service	Windows in...	Running
Base Filtering Engine	The Base Fil...	Running
Block Level Backup Engine Service	The WBENG...	
Certificate Propagation	Copies user ...	Running
CNG Key Isolation	The CNG ke...	Running
COM+ Event System	Supports Sy...	Running
COM+ System Application	Manages th...	
Computer Browser	Maintains a...	
Credential Manager	Provides se...	Running
Cryptographic Services	Provides thr...	Running
DCOM Server Process Launcher	The DCOM...	Running
Device Association Service	Enables pair...	