**How to change from AD FS authentication to Pass-Through Authentication with Seamless SSO**

First, there are still a few scenarios where AD FS is still needed or useful–such as SharePoint Hybrid Search, federation and single sign-on with third-party applications, and some certificate-based logon scenarios.

And, there are a few scenarios where pass-through authentication or password hash synchronization with seamless sso don’t work yet

* automatic alternate ID logon for Office ProPlus apps (AD FS doesn’t work in these instances, either)
* Outlook 2016 alternate ID logon (detects correct mailbox based on SMTP address, but the authentication dialox box displays the UPN)

**Preparing your environment**

First, Run the AAD Connect Network and Name Resolution Testing tool*.* It has a bunch things to help make sure your AAD Connect server can communicate with everything it needs to. If you’re already using AAD Connect successfully, you can just run it with the -OnlineEndpoints switch parameter to check your outbound connectivity.

Second, you need to make sure you have all your credentials. You’ll need:

1. Your on-premises domain admin credential for every Active Directory domain configured in AAD Connect

2. Credentials for a global admin account in your Office 365 tenant.

**Updating the configuration**

Once you have your everything ready, it’s time to run the configuration wizard to change your settings.

1. Log on to the server running Azure AD Connect.
2. Double-click / open the Azure AD Connect icon on the desktop.
3. Acknowledge the User Account Control prompt (if displayed).
4. Select the green Configure button.
5. Select Change user sign-in and click the green Next button.
6. On the Connect to Azure AD page, enter your global admin credentials and click the green Next button. I prefer to use a cloud identity credential for AAD Connect configuration changes.  
    *NOTE:  
    -If you had previously configured federation with the AAD Connect wizard, when you are presented with the User sign-in page, the Federation with AD FS radio button will already be selected.   
    -If you had previously configured AD FS outside of AAD Connect, your previous method will be selected (either Password Synchronization, Pass-through authentication, or Do not configure).   
    -If you configured AD FS federation outside of AAD Connect (like most of us have), you’ll want to stop what you’re doing and go convert your federated domains to managed (Set-MsolDomainAuthentication or Convert-MsolDomainToStandard–just a brief bit of warning: as soon as you do this, users will be unable to log in until you complete the pass-through authentication setup). Simple enough to announce a maintenance window.*
7. Select the radio button for **Pass-through authentication**, and then select the **Enable single sign-on**to enable the Seamless Single Sign-On configuration process. Click the green **Next** button to proceed.
8. Click the green **Enter credentials** button to enter a Domain Admin credentials for each of your connected domains. AAD Connect won’t save this credential (it’s only used for the configuration tasks). When you’re finished entering credentials, click the green **Next** button.
9. Confirm your choices and click the green **Configure** button.
10. Wait while the installed completes. If you are switching from Federated, the domain type will change from Federated to Managed.
11. Close the wizard. It will probably return errors.  
     You can view the log file at C:\ProgramData\AADConnect\trace-<date>.  
     *Note: As long as you see things that say “finished successfully,” you should be able to ignore any warnings.*
12. Test Pass-through authentication with Seamless SSO. The first test is opening a browser to https://portal.office.com from an outside network and making sure you don’t get redirected to your federation prompt. That in conjunction with the log file will let you know that Setup has updated the domain configuration in the tenant

**How to Deploy to your users**

I suggest you do Group Policy changes before you make the changes. Push out the changes a few weeks before making the change.

To roll out the feature to your users, you need to add the following Azure AD URL to the users’ Intranet zone settings by using Group Policy in Active Directory:

* **<https://autologon.microsoftazuread-sso.com>**
* **https://aadg.windows.net.nsatc.net**

For Edge or Internet Explore create a group policy for adding to your intranet zone settings

* **<https://autologon.microsoftazuread-sso.com>**
* **https://aadg.windows.net.nsatc.net**

Also, you need to enable an Intranet zone policy setting called **Allow updates to status bar via script** and

You may want to deploy a Group Policy Preference for this setting to disable popups.

**[HKCU\SOFTWARE\Microsoft\Office\16.0\Common\Identity\DisableADALatopWAMOverride] – REG\_DWORD “1”**

Firefox

For Firefox you can configure settings via Firefox Group Policy ADMX templates: [**https://support.mozilla.org/en-US/kb/customizing-firefox-using-group-policy**](https://support.mozilla.org/en-US/kb/customizing-firefox-using-group-policy).

You can manually do this by.

1. Launch Firefox.
2. In the URL bar, type **about:config** and press enter.
3. Click the **I accept the risk!** button.
4. In the search bar, type **network.negotiate-auth.trusted-uris** to locate the settings object to modify. Double-click it to open.
5. In the dialog box, enter **https://autologon.microsoftazuread-sso.com,https://aadg.windows.net.nsatc.net** and click OK.
6. Close and reopen Firefox for the settings to take effect.

Chrome

For Chrome you can change the settings by group policy by downloading the templates from Google here: <https://support.google.com/chrome/a/answer/187202?hl=en> and changing these settings

1. Configure the setting **Kerberos delegation server whitelist**
2. And add **https://autologon.microsoftazuread-sso.com** and **https://aadg.windows.net.nsatc.net** to the list.

Ensuring high availability

For redundancy there is a stand alone client to install on your systems.

1. Select servers that you want to install the agent on. They need to be able to communicate out to the internet on at least ports 80 and 443, though I’ve seen some requirements that give additional ports as well.
2. Download the pass-through authentication agent from here:**<http://aka.ms/getauthagent>**
3. Run the installer, and then click **Install**.
4. At the Modern Authentication dialog box, enter a global admin credential and click **Next**.
5. Click **Close** to dismiss the installer after it completes.
6. Log into https://aad.portal.azure.com with a global admin credential.
7. Select **Azure Active Directory** from the navigation blade.
8. On the Azure Active Directory blade, select **Azure AD Connect**.
9. On the Azure AD Connect blade, select the agents link next to **Pass-through authentication** to display the servers that have the pass-through authentication agent installed.
10. Verify that the servers where you have installed the pass-through authentication agent are registered and showing online. The pass-through authentication agent is installed on the server running Azure AD Connect as part of the initial configuration

For more information:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-deployment-plans>

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom>

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-quick-start#step-5-ensure-high-availability