The ultimate in-depth reference

Hundreds of timesaving solutions

Supremely well-organized, packed with expert advice

Microsoft

Microsoft 365 Administration Inside OUT

Third Edition

Aaron Guilmette • Darryl Kegg • Ed Fisher

Microsoft

Microsoft 365 Administration Inside Out, Third Edition

Aaron Guilmette
Darryl Kegg
Ed Fisher

FIGURE 10-15 Selecting a service account

Finally, clicking the Specify Custom Sync Groups checkbox allows you to specify alternate group names for the four groups that delegate rights to the AAD Connect implementation.

These four groups shown above can be domain groups if you are installing AAD Connect on a domain joined server (as pictured in Figure 10-16) or group names that are local to the AAD Connect server. However, in either case, if you specify custom sync groups, they need to be created before the installation. Failure to create the groups before installation causes the installer to fail, and an entry is logged in the Application Event log, indicating the group could not be found.

FIGURE 10-16 Specify Custom Sync Groups

If no custom sync groups are provided, the installer will automatically create the following four groups, which are used to secure AAD Connect and are granted the permissions shown in Table 10-1.

Table 10-1 AAD Connect default application groups

GROUP NAME	PERMISSIONS
`ADSyncAdmins`	Full rights to the AAD Connect tool.
`ADSyncOperators`	Able to view operations run history; cannot view connectors or objects. Able to view sync rules but unable to edit or delete.
`ADSyncBrowse`	No access to the Sync service console and cannot view Synchronization rules.
`ADSyncPasswordSet`	No access to the Sync service console and cannot view Synchronization rules.

The only populated group at the time of installation is the ADSyncAdmins group. The user account used to perform the AAD Connect installation will be placed into this group automatically when the installation completes.

Import synchronization settings

One of the newer features of AAD Connect is the option to import synchronization settings from an existing AAD Connect installation. (This was added in Version 2.0.3.0 in July of 2021.)

This new feature is exceptionally handy when setting up an AAD Connect server in Staging Mode when you have a significant number of rule customizations or organizational unit selections on your existing AAD Connect production server.

In past versions, you were typically forced to use PowerShell to re-create rules; depending on the granularity of the organizational unit selection process, OU selection was an exercise that might take hours. This newer feature will import everything except passwords to the new server, requiring that you enter only the passwords during the installation and nothing else.

Each time a change is made to the AAD Connect configuration using the AAD Connect Wizard, a file named `Applied-SynchronizationPolicy-xxxx.JSON` is automatically exported to `%ProgramData%\AADConnect`. (In this example, `xxxx` represents a timestamp.)

This file can then be used as part of the AAD Connect installation by checking the box and supplying the path to the appropriate JSON file.

Inside Out

AAD Connect JSON export

The AAD Connect Wizard automatically exports a JSON configuration file each time the installation is changed. However, any changes made via the Synchronization Rules Editor, the Synchronization Service Manager, or by using PowerShell would not be included.

When changes are made without the use of the Wizard, it is necessary to run the AAD Connect Wizard and select the View or Export Current Configuration option to save a new JSON file with the updated configuration.

Selecting your authentication method

Another critical milestone when installing and configuring AAD Connect is selecting the authentication method your users will use to access Microsoft 365. There are several options available during the installation of the AAD Connect tool in Custom mode on the User Sign-In page.

While selecting an authentication method is important to the overall design and deployment of Microsoft 365 and your directory synchronization, you can run the configuration Wizard on the desktop at any time to change these settings. As a result, you might want to simply choose Do Not Configure and bypass the authentication configuration steps during initial installation and return to change them later.

Password synchronization

Selecting Password Synchronization on the User Sign-In dialog shown in Figure 10-17 configures the AAD Connect tool to automatically synchronize user passwords from on-premises Active Directory to Azure Active Directory. This synchronization process occurs independently of the regularly scheduled 30-minute synchronization cycle used by the AAD Connect server to synchronize on-premises Active Directory object properties (such as the name, email address, and so on). That means password changes in on-premises Active Directory are replicated to Microsoft 365 every 1–2 minutes.

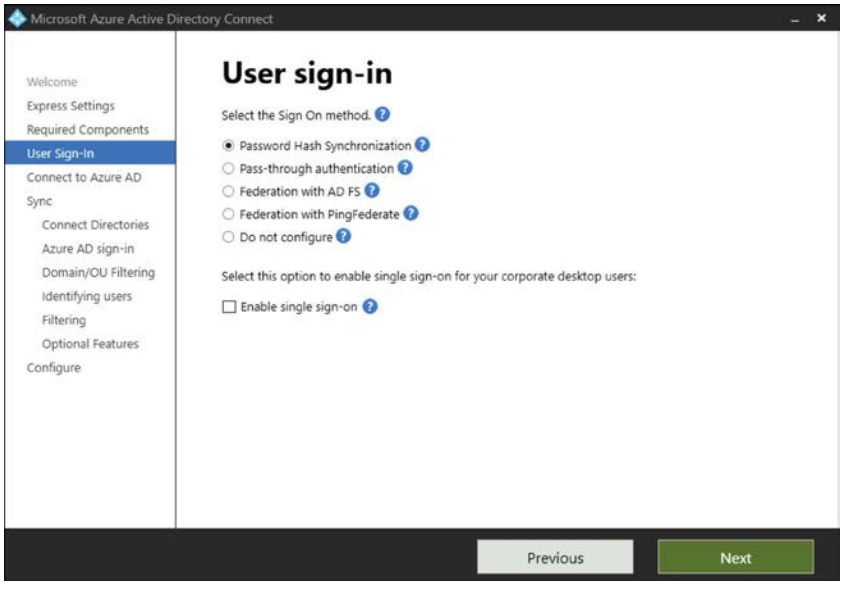

FIGURE 10-17 The User Sign-In dialog

NOTE

Password encryption

Passwords synchronized to Microsoft 365 are not transmitted in cleartext. Instead, the user's password hash is encrypted a second time using an MD5 key and an additional cipher. The result is a hash-of-a-hash or salted-hash and is transmitted via an encrypted HTTPS session between the AAD Connect server and Microsoft 365.

The user authentication, hash expansion, and decryption take place in Azure Active Directory, not the on-premises Active Directory.

Scope

When you enable the password synchronization feature as part of the AAD Connect installation, there is an initial synchronization of all passwords to Microsoft 365 for any users configured within the scope of the solution.

In an Express mode configuration, **all** user objects are automatically within the scope of the solution. However, when performing a Custom installation, the organizational unit selection and any group filtering you enabled defines the users who fall within the configuration scope and which passwords will be initially synchronized.

Permissions

When password synchronization is automatically enabled as part of an Express mode installation, the service account (such as `MSOL_xxxxxxx`) generated in on-premises Active Directory is automatically delegated the Replicating Directory Changes and Replicating Directory Changes All permissions at the forest's top level.

However, when performing a Custom installation, there is no automatic account creation; therefore, no rights are delegated automatically. The service account you create for the Active Directory Forest connector will need to have the rights manually delegated to the top level of each domain in the forest.

Inside Out

Password policies

It is important to note that when using password synchronization, the cloud account password is set to never expire. This means that an expired password in on-premises Active Directory that remains unchanged is still valid in Microsoft 365 and can be used to log in to the tenant.

Pass-through authentication

Pass-through authentication (see Figure 10-18) is an alternative to password synchronization if your company policies prohibit the transmission of passwords, even in an encrypted format via the public Internet. Instead of syncing user passwords to the cloud and relying on Microsoft 365 to process logins, pass-through authentication allows for authentication requests to be processed by on-premises Active Directory infrastructure without the need to transmit passwords or deploy identity providers like Microsoft's AD FS.

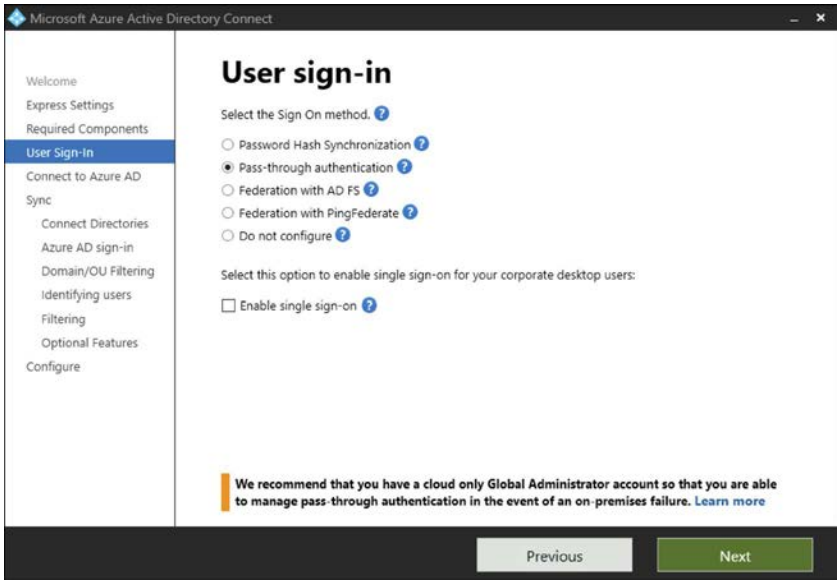

FIGURE 10-18 Selecting Pass-Through Authentication

Overview

The implementation of pass-through authentication requires the deployment of a processing agent added to the AAD Connect server automatically when the option is selected, which operates using outbound-only communication. The agent can be deployed on more than one server for high-availability, provided the server is domain joined to the domain where the users being authenticated reside and the server is running Windows Server 2012R2 or later.

Pass-through authentication behaves similarly to Microsoft's AD FS. However, instead of redirecting authentication requests back to an on-premises server, the request is placed in an Azure queue and picked up via a regularly scheduled process initiated by the processing agent running on-premises. The processing agent sends the request to an Active Directory domain controller, where the domain controller processes it, and the results are returned to the processing agent to be sent back to Azure. Upon receipt, Azure issues a token to the user so they can access Microsoft 365 services.

Requirements

While Azure AD pass-through authentication eliminates the need to synchronize passwords to Microsoft 365 and simplifies the authentication process compared to the implementation of Microsoft AD FS or other identity providers, pass-through authentication has several key requirements that must be met to ensure it will operate properly.

The AAD Connect server and the underlying pass-through processing agent must be installed and domain-joined to the forest where the authentication requests will be directed. All servers running the processing agent must also be Windows Server 2012R2 or later.

Pass-through authentication is supported in a multi-forest configuration, though a forest trust is required.

The `UserPrincipalName` value used for synchronization to Microsoft 365 must be the value from the `UserPrincipalName` attribute in on-premises Active Directory and must be a routable UPN suffix. Alternate Login ID is not supported with pass-through authentication.

The AAD Connect server and any servers running the processing agent must be able to reach Azure Active Directory on several additional TCP/IP ports and should not be located behind a proxy server or network devices that perform SSL inspection or URL filtering.

> NOTE
>
> **The list of pre-requisites for pass-through authentication can be found at *https://aka.ms/ptaprereqs*.**

Checking the radio button for pass-through authentication will deploy the processing agent as part of the AAD Connect Custom installation. Any additional installations of the processing agent will require the download of the processing agent at *https://aka.ms/ptagent*.

Federation with AD FS and Ping

The AAD Connect Wizard provides a method for installing the AD FS components as part of the normal installation process. Selecting the Federation With AD FS option on the User Sign-In page will add several additional pages to the installation wizard that will allow you to install the AD FS and Web Application Proxy Server roles in your organization. See Figure 10-19.

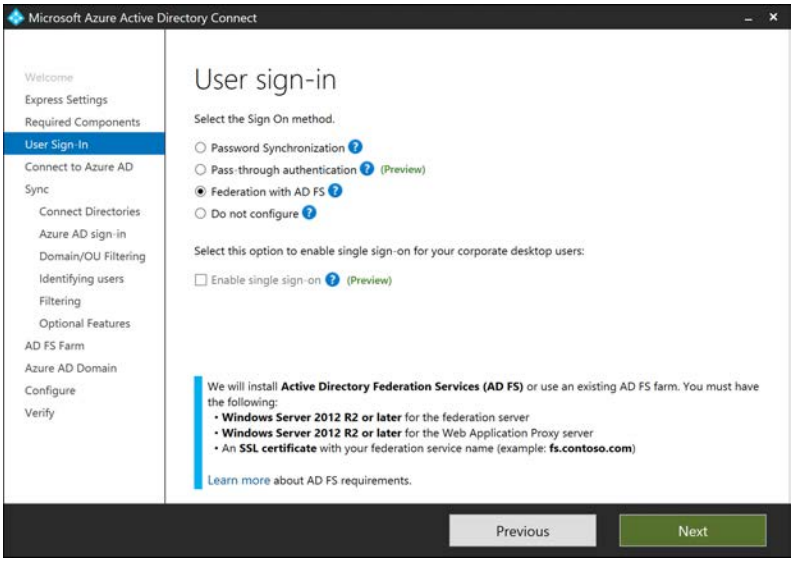

FIGURE 10-19 Federation With AD FS