Technical Note

Admin By Request
ZERO TRUST PLATFORM

Product Platform: **All platforms**
Product Version: **All versions**
Document Date: **15 November 2024**
Document Version: **2.0**
Classification: **Public**

Synchronizing Clients with the Portal

Introduction

Admin By Request (ABR) clients synchronize with the portal to ensure they have the latest settings and policies. This synchronization process happens periodically and can also be triggered manually.

The following explanation is based on common questions and scenarios.

NOTE
The term "Entra ID" is used here rather than the older "Azure AD (AAD)" term.

Periodic Synchronization

By default, ABR clients synchronize with the portal **every four hours**, subject to internet connectivity. This regular synchronization ensures that any changes in ABR portal configuration are reflected/applied to each endpoint.

Another purpose of synchronization is to ensure that Active Directory (AD) or Entra ID group memberships, settings, and policies are applied to the clients in a timely manner. While the AD Connector is **On** (portal: **Settings > Tenant Settings > Groups > ENTRA ID / AZURE AD > Enable Connector**), Entra ID groups are "looked-up" by the ABR client when one of the following happens:

1. The user logs on to the endpoint device.
2. Once every 4 hours if the ABR client is idle.
3. If a user clicks **About Admin By Request** via the tray icon or menu bar (see "Manual Synchronization" on the next page)

Note that group modifications made on the Entra ID platform can take *between 30 seconds to 1 hour*. This is how the Entra ID platform works and is determined by Microsoft - Admin By Request has no control over this interval. Refer also to "Factors Affecting Synchronization Timing" on the next page.

Manual Synchronization

Users can manually trigger a synchronization to ensure that the latest portal settings and policies are immediately applied to the ABR client. This can be useful when changes need to be reflected quickly, such as during testing prior to roll-out, or when a user is added to or removed from an AD/Entra ID group that affects their permissions.

To trigger synchronization:

- Simply log on to the ABR client (i.e. the endpoint device).
- For Windows endpoints, click the *ABR icon in the tool tray* on the device and select **About Admin By Request**. This action triggers the *About* screen and also initiates an immediate synchronization with the portal.
- For macOS and Linux endpoints, click the *ABR menu bar icon* on the device and select **About Admin By Request**. This action triggers the *About* screen and also initiates an immediate synchronization with the portal.

Scripted Synchronization

On macOS endpoints, synchronization can be triggered by running command:

```
open -g -n /Applications/Admin\ By\ Request.app --args -refresh
```

On Linux endpoints, synchronization can be triggered by running command:

```
abr settings --reload
```

Factors Affecting Synchronization Timing

While the default synchronization interval is four hours, the actual time it takes for changes to be reflected can vary. This variability can be due to the time it takes for changes to propagate through AD/Entra ID and be recognized by the ABR client. Factors such as network latency, AD replication schedules, and Entra ID synchronization cycles can all influence this timing.

IMPORTANT

User/device group memberships are handled by Entra ID; ABR clients are in Microsoft's hands when it comes to propagation time.

In many cases (as indicated by customer tickets on this subject) we see customer screen grabs from Entra ID showing that users or devices are members of group XYZ and asking why the portal has not yet picked them up.

However, in these cases, the portal does not know the endpoint state. The actual time that synchronization with Entra ID/Intune "kicks in" on an endpoint can vary and depends on many factors. Note also that, with on-premise AD configuration, endpoints need to have a "line of sight" to the PDC (Primary Domain Controller). It's important to be aware of this, especially when users work remotely (i.e. off site) and are using VPN or similar to reach the corporate network.

Handling Hybrid Environments

In hybrid environments where devices may be joined to both on-prem AD and Entra ID, ABR provides a **Hybrid preference** setting. This setting allows administrators to specify whether the ABR client should prioritize synchronizing with AD or Entra ID. This is crucial for environments where different sub-settings are based on either AD or Entra ID groups.

If the environment is a hybrid setup, i.e. it's connected to both on-prem AD and Entra ID, then it very much depends on what the AD Connector hybrid preference is set to. If set to **Prefer Active Directory**, then AD groups will be the ones used to match sub-settings. If set to **Prefer Entra ID**, then Entra ID groups will be used instead.

Issues can arise if *different group names* are used for on-prem and Entra ID groups, or if group members are not synchronized properly between them.

Common Issues and Solutions

If synchronization issues arise, such as changes not being reflected in the ABR portal or incorrect group memberships, the first thing to check is the Connectivity panel in the user interface, accessed via **About Admin By Request > Connectivity**. If cloud connectivity status is failing, then the ABR client won't be able to synchronize with the portal.

To investigate this, or to look at other areas if connectivity is OK:

- Ensure that the ABR client is up to date. Upgrading to the latest version can resolve synchronization issues.
- Verify that the AD/Entra ID groups are correctly configured and that the client has network connectivity to the appropriate directory services.
- Use the `whoami /groups` command on Windows to verify group memberships directly on the client machine (see note below).
- For hybrid environments, ensure that the ABR portal is configured to correctly handle AD and Entra ID group memberships, according to the selected preference.

> The `whoami /groups` command shows *only* on-prem AD groups. There are other options to show Entra ID groups:
>
> - Use the Remote Server Administration Tools (RSAT) PowerShell module to look up a user's groups. In particular, the cmdlets **Get-ADUser** and **Get-ADGroup**.
>   For more information on the RSAT PowerShell module, refer to https://learn.microsoft.com/en-us/powershell/module/activedirectory/?view=windowsserver2022-ps.
> - Users can view their assigned groups by going to their Microsoft 365 account page. This can be accessed (in Microsoft 365) by going to **Settings > Accounts > Your info > Accounts : Manage my accounts > My Groups**.
> - IT Admins and tech savvy users can login with an admin account on the device to look up the following registry subkey via the Registry Editor: **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\CloudActiveSync\ADSICache\**.

For more information, including answers to questions and/or further assistance, please contact your account manager or get in touch via our contact page.