



Partner FAQ: AuthPoint | Unify Identity Management with Microsoft Entra ID Synchronization (DDS) Configuration Changes.

Overview

Identity is the control plane for modern security, but fragmented user and group management across tools creates friction and risk. To address this, WatchGuard is moving forward with Directories and Domain Services (DDS) as the identity hub in WatchGuard Cloud, starting with Microsoft Entra ID synchronization.

On **January 15, 2026**, WatchGuard will introduce **changes in how Entra ID users and groups are managed across WatchGuard Cloud services**, including AuthPoint. This FAQ explains what is changing, who is impacted, and where to find the official guidance and resources to complete the required configuration updates.

At a glance

- **Who is impacted:** Partners who synchronize identities from Microsoft Entra ID for AuthPoint and/or use Entra ID users and groups.
- **What is changing:** Entra ID users and groups are managed through WatchGuard Cloud DDS so identity data can be used consistently across services.
- **What you need to do:** Follow the published [step-by-step guide](#) and implementation paths ([new](#) vs. [conversion](#)) to apply the required configuration updates for impacted tenant(s), then validate expected results.
- **Recommended approach for MSPs:** Use a phased rollout (start with a low-risk tenant, validate, then expand).

Before you start (quick checklist)

- **Identify** which account(s) / tenant(s) currently use Entra ID with AuthPoint.
- **Confirm** you have the required WatchGuard Cloud administrative access for **Configure > Directories and Domain Services**.
- **Prepare** Microsoft Entra ID application registration details (Domain Name, Application (client) ID, Client Secret).
- **Plan** a maintenance window and communication plan if you manage multiple tenants.
- Have the **validation** checklist ready (users, groups, memberships, and downstream policy behavior).

FAQ

About the change

Q: What is changing?

A: On **January 15, 2026**, WatchGuard is releasing an update that enhances synchronization of Microsoft Entra ID users and groups through WatchGuard Cloud Directories and Domain Services (DDS), enabling more consistent identity use across AuthPoint. **This release introduces changes in how Entra ID users and groups are managed across WatchGuard Cloud services.** As part of this process, **all existing AuthPoint Entra ID external identity configurations must be migrated to Directories and Domain Services** in WatchGuard Cloud. [Learn more](#)



Q: Why is WatchGuard moving Entra ID user management to DDS?

A: DDS is designed to act as a centralized identity foundation in WatchGuard Cloud. Connecting Entra ID to DDS helps reduce identity silos and supports more consistent identity inputs across services.

Q: What is DDS (Directories and Domain Services)?

A: DDS is designed to act as a central repository for users, groups, and devices for WatchGuard Cloud services. It provides shared identity data that multiple services can consume.

Q: What does "single source of truth" mean here?

A: Entra ID remains the authoritative source for user and group data; DDS helps reflect Entra ID identity information in WatchGuard Cloud so services that consume identities can stay aligned.

Q: How does this relate to the WatchGuard Cloud Directory?

A: WatchGuard Cloud Directory is an authentication domain for users and groups hosted in WatchGuard Cloud. DDS is the broader capability area for managing authentication domains and directory integrations, including Entra ID.

Q: What benefits should partners expect?

A: Partners can expect these benefits:

- **Less manual work:** reduced repetitive identity administration by reflecting Entra ID adds/removals/group changes through DDS.
- **Better policy consistency:** use the same Entra ID groups for identity-driven decisions across AuthPoint.
- **Stronger posture:** consistent enforcement of **MFA** and **Zero Trust policies** across services (where applicable).

Impact and required actions

Q: Who does this change impact?

A: Partners are impacted if they **currently use Microsoft Entra ID** for identity **synchronization** with **AuthPoint and/or** rely on **Entra ID users and groups**.

Q: What do partners need to do? Will this impact existing tenants or existing configurations?

A: This release changes how Entra ID users and groups are managed across WatchGuard Cloud services. All AuthPoint accounts with an existing Azure AD/Entra ID external identity must migrate the external identity to Directories and Domain Services. This migration is designed to be straightforward and can be completed from the **Configure > AuthPoint > External Identities** page. After the migration is complete, make sure that authentication works for your users.

Q: What happens if we do not take action right away?

A: There is no required deadline for the rollout at this time. If you leave your current configuration as is, it should continue to work until you are ready to migrate. That said, we **strongly recommend** planning the migration as soon as practical so you can take advantage of the DDS-based synchronization improvements and ensure your configuration stays aligned with the latest supported approach. If a hard migration date is introduced in the future, WatchGuard will share a follow-up announcement in advance.



Q: Does this change affect Zero Trust Policies configuration?

A: Your existing Zero Trust Policies do not change as part of this update. However, if you previously synchronized Entra ID users into AuthPoint and used a manually created AuthPoint group for policy targeting, that extra AuthPoint group may no longer be necessary after moving to the DDS-based configuration. After the update, review your policies to confirm they target the intended Entra ID groups and that access outcomes remain as expected.

Roles, permissions, and prerequisites

Q: Who should make this change?

A: A technical administrator who has (1) the required administrative access in WatchGuard Cloud for Directories and Domain Services, and (2) Entra ID administrative access to register an application and grant required permissions.

Q: Do I need to install an agent to sync Entra ID users and groups?

A: No agents are required. WatchGuard Cloud communicates directly with Entra ID to sync users and groups.

Q: Where do I configure Entra ID in WatchGuard Cloud?

A: In WatchGuard Cloud, go to **Configure > Directories and Domain Services (Authentication Domains)**.

Q: How do I add an Entra ID authentication domain in WatchGuard Cloud?

A: Follow these steps in order: first, use the [Add an Authentication Domain to WatchGuard Cloud](#) help topic to create your **Entra ID authentication domain**. Next, use the [Configure a directory sync](#) help topic to synchronize Entra ID users and groups into **DDS**. Finally, follow the [Set up an external identity with a group sync](#) help topic so AuthPoint can consume those synchronized users and groups.

How the pieces fit together (high level)

1. **WGC / DDS:** Add Entra ID authentication domain → enable directory sync
2. **AuthPoint:** Set up or migrate external identity to use the DDS-based approach → validate MFA/auth flows

Implementation paths (new vs. conversion)

We provide two demos to match common implementation scenarios. Choose the path that best matches your tenant:

Scenario	Use this when	What to follow
New configuration	You are setting up Entra ID synchronization via DDS for the first time in a tenant.	New configuration Demo
Convert existing configuration	You have an existing Entra ID-related configuration and need to transition to the DDS-based approach.	Convert existing configuration Demo

***Note:** If you are not sure which path applies, start with the [step-by-step guide](#) and review the decision points in the conversion demo.

Validation and rollback

Q: What should we validate after we apply the update?

A: At minimum, validate that:

1. The correct users and groups are present
2. Group memberships match expectations
3. AuthPoint behavior that depends on those users and groups works as intended.

Note: For MSPs, repeat validation for each tenant as you roll out the change.

Q: What information should I capture if I need support?

A: Be ready to provide the tenant/account name, the authentication domain name, timestamps, relevant screenshots, and any error messages. If the issue is related to Entra ID app registration, capture the app registration details used (without sharing sensitive or confidential information).

Resources & Support

- [Add a New Entra ID External Identity to AuthPoint or Migrate an Existing Entra ID External Identity to DDS](#)
- [Add an Authentication Domain to WatchGuard Cloud](#)
- Implementation path demos:
 - [New configuration](#)
 - [Convert existing configuration](#)
- Training video: [Sync Users from Entra ID](#)
- [AuthPoint Release Notes](#)

If you have questions or need help planning the update (especially across multiple tenants), please contact your WatchGuard Account Manager or Sales Representative.