Freshservice Azure AD Sync Configuration Guide

This guide outlines the steps to configure Azure Active Directory (AAD) synchronization with Freshservice. Integrating with Azure AD supports ITIL principles by enabling accurate identity management, automation of user provisioning, and improved security controls.

# Purpose

To streamline user and group management in Freshservice by leveraging Azure AD as the source of truth. This ensures consistency in roles, department mapping, and permission settings based on ITIL-aligned identity practices.

# Pre-Requisites

• Azure AD Admin access

• Freshservice Admin access

• SCIM provisioning available in Azure AD Premium P1 or higher

• List of groups or OUs to sync

# Step-by-Step Configuration

## 1. Enable SCIM in Freshservice

• Log in to Freshservice as an admin.

• Go to Admin > Account Settings > SCIM Settings.

• Enable SCIM and copy the Tenant URL and Bearer Token for Azure configuration.

## 2. Set up Freshservice as an Enterprise App in Azure AD

• In the Azure Portal, navigate to Azure Active Directory > Enterprise Applications.

• Click '+ New Application', then select 'Create your own application'.

• Name the app (e.g., Freshservice SCIM), then choose 'Integrate any other application'.

• Under 'Provisioning', select 'Automatic'.

## 3. Configure SCIM Provisioning in Azure AD

• Paste the Freshservice SCIM Tenant URL and Bearer Token into the respective fields.

• Click 'Test Connection' to validate.

• Under 'Mappings', configure the attribute mappings (email, department, job title, etc.).

• Save and start provisioning.

## 4. Define Group Sync Rules

• From the app page in Azure AD, go to 'Users and Groups'.

• Assign the groups or users that need access to Freshservice.

• Only members of these groups will be provisioned to Freshservice.

## 5. Verify Sync in Freshservice

• After a successful sync, verify that users appear under Admin > Users.

• Check that their department, roles, and email addresses are accurate.

• Assign Freshservice roles if not already automated via mapping.

# Best Practices

• Use group-based role mapping for automation and scalability.

• Periodically audit sync logs in Azure to ensure no failures.

• Align department mapping in Freshservice with HR or organizational data structures.

• Apply role-based access control (RBAC) per ITIL standards.

# Post-Sync Checklist

☐ SCIM successfully enabled and tested

☐ User attributes and roles are syncing as expected

☐ Unused test users removed from Freshservice

☐ Group membership rules documented

This integration reduces manual overhead, improves data consistency, and supports ITIL service transition by establishing a reliable foundation for user-based automation.