

Azure Active Directory **Workday-driven User Provisioning** Deployment Plan

**How to use this guide**

This step-by-step guide walks through the implementation of Workday to Active Directory User Provisioning solution in a five-step process. The links below take you to each of those steps.



**1**

**[Include](#_Stakeholders_and_Sign-off)**

[Stakeholders](#_Stakeholders_and_Sign-off)

**2**

**[Plan](#_Planning_Your_Implementation)**

[Your project](#_Planning_Your_Implementation)

**3**

**[Design](#_Designing_Your_Implementation)**

[end-to-end integration](#_Designing_Your_Implementation)

**5**

**[Manage](#_Operationalize_your_Implementation)**

[Your implementation](#_Operationalize_your_Implementation)



**4**

**[Implement](#_Implementing_Your_Solution_1)**

[Your design](#_Implementing_Your_Solution_1)

**Note:**

Throughout this document, you will see items marked as

* **Microsoft Recommends**

These are general recommendations, and you should only implement if they apply to your specific enterprise needs.

Table of Contents

Contents

[Business Value of Workday-driven User Provisioning 0](#_Toc525728695)

[Stakeholders and Sign-off 1](#_Toc525728696)

[Planning Your Implementation 2](#_Toc525728697)

[Workday-driven User Provisioning Solution Overview 2](#_Toc525728698)

[Solution Architecture 2](#_Toc525728699)

[Solution Components 3](#_Toc525728700)

[Understand Solution Capabilities 3](#_Toc525728701)

[What HR scenarios does it cover? 3](#_Toc525728702)

[Who is this user provisioning solution best suited for? 4](#_Toc525728703)

[License Considerations 4](#_Toc525728704)

[Azure AD Premium License 4](#_Toc525728705)

[Workday License 4](#_Toc525728706)

[Environment Planning 4](#_Toc525728707)

[Cloud Tenants for Azure AD and Workday 4](#_Toc525728708)

[Active Directory Test and Production instances 5](#_Toc525728709)

[On-prem servers for AAD Connect Provisioning Agent 6](#_Toc525728710)

[Security Review Planning 7](#_Toc525728711)

[Test Data Considerations 7](#_Toc525728712)

[Capture Your Identity Lifecycle Requirements – The Joiners, Movers and Leavers Process 8](#_Toc525728713)

[Workday and AD Characteristics 8](#_Toc525728714)

[Joiners Process: Identity Data and Attribute Mapping 9](#_Toc525728715)

[Movers Process: Identity Data and Attribute Mapping 10](#_Toc525728716)

[Leavers Process: Identity Data and Attribute Mapping 11](#_Toc525728717)

[Designing end-to-end integration 12](#_Toc525728718)

[Design Decision #1 – Deployment Topology 12](#_Toc525728719)

[Design Decision #2 – Select Domain Controllers to handle Provisioning Requests 13](#_Toc525728720)

[Design Decision #3 – Defining Scoping Filters 13](#_Toc525728721)

[Design Decision #4 – Determine Matching Attribute(s) 14](#_Toc525728722)

[Design Decision #5 – Configure Custom Workday Attributes 14](#_Toc525728723)

[Design Decision #6 – Determine AD Account Status 15](#_Toc525728724)

[Design Decision #7 – Workday to AD User Attribute Mapping 15](#_Toc525728725)

[Design Decision #8 – Unique Value Generation 16](#_Toc525728726)

[Design Decision #9 – AD OU Container Assignment 17](#_Toc525728727)

[Design Decision #10 – Password Delivery for new AD Accounts 17](#_Toc525728728)

[Design Decision #11 – Plan and Prepare for Initial Sync 17](#_Toc525728729)

[Implementing Your Solution 18](#_Toc525728730)

[Phase 1: Configure Workday-driven user provisioning in TEST environment 18](#_Toc525728731)

[Phase 2: User Acceptance Testing (UAT) 19](#_Toc525728732)

[Phase 3: Transitioning into production 19](#_Toc525728733)

[Phase 4: Rollback steps 19](#_Toc525728734)

[Operationalize your Implementation 20](#_Toc525728735)

[Reporting and monitoring 20](#_Toc525728736)

[Troubleshooting 21](#_Toc525728737)

[Reference Documentation 22](#_Toc525728738)

[Appendix 22](#_Toc525728739)

[Default Workday Attributes 22](#_Toc525728740)

# Business Value of Workday-driven User Provisioning

This section presents an executive summary of the business case for rolling out Workday-driven User Provisioning using the Workday to Active Directory User Provisioning solution.

Using this solution offering from Azure AD, enterprises can seamlessly manage the identity lifecycle of employees, vendors and contingent workers configuring rules that map HR business events and Joiner-Mover-Leaver processes (such as New Hire, Terminate, Transfer) to IT provisioning actions (such as Create, Enable, Disable, Delete accounts). This capability of HR-driven IT provisioning offers significant business benefits as listed below:

|  |  |
| --- | --- |
| \\MAGNUM\Projects\Microsoft\Cloud Power FY12\Design\ICONS_PNG\Increase.png | **INCREASE PRODUCTIVITY**  New hires (both employees and contingent workers) often need a common set of accounts – email, directory, file shares – that are collectively referred to as “birthright accounts”. Automating the assignment of these “birthright accounts” enables a quicker time to productivity by immediately giving new hires the tools they need to do their jobs. |
| \\MAGNUM\Projects\Microsoft\Cloud Power FY12\Design\ICONS_PNG\Confidentiality.png | **MANAGE RISK**  Secure your organization by ensuring that user identities and access to key SaaS apps are automatically updated when users transition or leave the organization. This can be implemented based on authoritative attributes such as employee status, last day of work, business unit, job location and effective dates flowing in from the HR system. |
| C:\Users\mitchellg\Desktop\Simple_Licensing.png | **ADDRESS COMPLIANCE AND GOVERNANCE**  Deploying HR-driven user provisioning creates a foundation for on-going identity governance and dramatically enhances the quality of business processes that rely on identity data. From a compliance perspective, the solution supports native audit logs for every user provisioning request performed by each application for both source and target systems. |
| \\MAGNUM\Projects\Microsoft\Cloud Power FY12\Design\ICONS_PNG\Within_Your_Reach.png | **MANAGE COST**  Reduce costs by eliminating inefficiencies and human error associated with manual provisioning. This includes maintaining custom-developed or home-grown user provisioning solutions built over time using legacy and outdated platforms. |

# Stakeholders and Sign-off

The following section serves to identify all the stakeholders that are involved in the project and need to sign off, review, or stay informed. Add stakeholders to the table below as appropriate for your organization.

* + SO = Sign-off on this project
  + R = Review this project and provide input
  + I = Informed of this project

|  |  |  |
| --- | --- | --- |
| Name | Role | Action |
| Enter name and email | **HR Manager**  *A representative from the HR organization who can provide inputs on existing HR business processes and worker identity + job data processing requirements.* | SO/R/I |
|  | **Workday Admin or Workday System Integrator**  *A representative from the Workday Admin team who can provide inputs related to Workday setup, Testing scenarios, HR transaction data load and review how Azure AD accesses Workday data.* | SO/R/I |
| Enter name and email | **On-premise AD Administrators**  *A representative from the AD Admin team who can provide inputs related to existing AD Account provisioning and de-provisioning lifecycle.* | SO/R/I |
| Enter name and email | **IT Support Manager / Helpdesk**  *A representative from the IT support organization who can provide inputs on the supportability of the Workday and Azure AD integration from a helpdesk perspective.* | SO/R/I |
| Enter name and email | **Identity Architect**  *A representative from the identity management team in charge of defining how the Workday and Azure AD integration aligns with the core identity management infrastructure in the customer’s organization.* | SO/R |
| Enter name and email | **Security Owner**  *A representative from the security team that can sign off that the plan will meet the security requirements of your organization.* | SO |

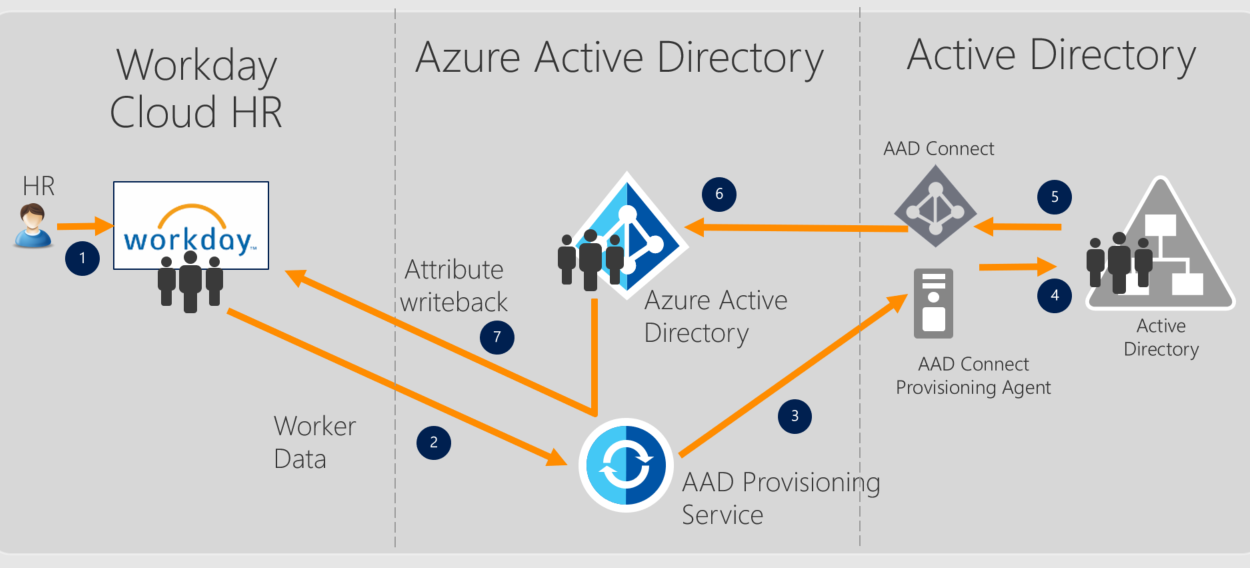
# Planning Your Implementation

## Workday-driven User Provisioning Solution Overview

### Solution Architecture

The diagram below illustrates the end-to-end user provisioning solution architecture for common hybrid environments. In this example, there are two related flows:

* **Authoritative HR Data Flow – from Workday to on-prem Active Directory:** In this flow worker events (such as New Hires, Transfers, Terminations) first occur in the cloud Workday HR tenant and then the event data flows into on-premise Active Directory through Azure AD and the Provisioning Agent. Depending on the event, it may lead to create/update/enable/disable operations in AD.
* **Email Writeback Flow – from on-prem Active Directory to Workday:** Once the account creation is complete in Active Directory, it is synced with Azure AD through AADConnect and email attribute sourced from Active Directory can be written back to Workday.



**Description of workflow:**

1. The HR team performs worker transactions (Joiners/Movers/Leavers or New Hires/Transfers/Terminations) in Workday HR module
2. The AAD Provisioning Service runs scheduled synchronizations of identities from Workday HR and identifies changes that need to be processed for sync with on-premise Active Directory.
3. The AAD Provisioning Service invokes the on-premise AAD Connect Provisioning Agent with a request payload containing AD account create/update/enable/disable operations.
4. The AAD Connect Provisioning Agent uses a service account to add/update AD Account data.
5. The AAD Connect / AD Sync engine runs delta sync to pull updates in AD.
6. The AD updates are synced with Azure Active Directory.
7. If the Workday email writeback connector is configured, it writebacks email attribute to Workday, based on the matching attribute used.

### Solution Components

The table below captures the various solution components that comprise the offering.

|  |  |  |
| --- | --- | --- |
| Integration Flow | Cloud Solution Components | On-prem Solution Components |
| Authoritative HR Data Flow – from Workday to on-prem Active Directory | * Workday Tenant * Azure AD Tenant | * AADConnect Provisioning Agent |
| Email Writeback Flow – from on-prem Active Directory to Workday | * Workday Tenant * Azure AD Tenant | * Azure AD Connect |

* **Microsoft recommends** Customers should first plan on configuring Authoritative HR data flow and then enable the email writeback flow once Workday matching attribute data is present in on-prem Active Directory.

## Understand Solution Capabilities

The [Azure Active Directory user provisioning service](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-saas-app-provisioning) integrates with the [Workday Human Resources API](https://community.workday.com/sites/default/files/file-hosting/productionapi/Human_Resources/v21.1/Get_Workers.html) in order to provision user accounts. Azure AD uses this connection to enable the following user provisioning workflows:

* **Provisioning users to Active Directory** - Synchronize selected sets of users from Workday into one or more Active Directory forests.
* **Writeback of email addresses to Workday** - The Azure AD user provisioning service can write the email addresses of Azure AD users back to Workday.

### What HR scenarios does it cover?

The Workday user provisioning workflows supported by the Azure AD user provisioning service enable automation of the following human resources and identity lifecycle management scenarios:

* **Hiring new employees** - When a new employee is added to Workday, a user account is automatically created in Active Directory, Azure Active Directory, and optionally Office 365 and [other SaaS applications supported by Azure AD](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-saas-app-provisioning), with write-back of the email address to Workday.
* **Employee attribute and profile updates** - When an employee record is updated in Workday (such as their name, title, or manager), their user account will be automatically updated in Active Directory, Azure Active Directory, and optionally Office 365 and [other SaaS applications supported by Azure AD](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-saas-app-provisioning).
* **Employee terminations** - When an employee is terminated in Workday, their user account is automatically disabled in Active Directory, Azure Active Directory, and optionally Office 365 and [other SaaS applications supported by Azure AD](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-saas-app-provisioning).
* **Employee re-hires** - When an employee is rehired in Workday, their old account can be automatically reactivated or re-provisioned (depending on your preference) to Active Directory, Azure Active Directory, and optionally Office 365 and [other SaaS applications supported by Azure AD](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-saas-app-provisioning).

### Who is this user provisioning solution best suited for?

This Workday user provisioning solution is presently in public preview, and is ideally suited for:

* Organizations that desire a pre-built, cloud-based solution for Workday user provisioning
* Organizations that require direct user provisioning from Workday to Active Directory
* Organizations that require users to be provisioned using data obtained from the Workday HCM module (see [Get\_Workers](https://community.workday.com/sites/default/files/file-hosting/productionapi/Human_Resources/v21.1/Get_Workers.html))
* Organizations that require joining, moving, and leaving users to be synced to one or more Active Directory Forests, Domains, and OUs based only on change information detected in the Workday HCM module (see [Get\_Workers](https://community.workday.com/sites/default/files/file-hosting/productionapi/Human_Resources/v21.1/Get_Workers.html))
* Organizations using Office 365 for email

## License Considerations

### Azure AD Premium License

You will need [Azure AD Premium License](https://azure.microsoft.com/pricing/details/active-directory/) to configure the Workday to AD User Provisioning integration.

If you have an existing Enterprise Mobility and Security (EMS) subscription with Microsoft, you may already have Azure AD Premium.

**Enterprise Mobility and Security (EMS) subscriptions:**

* EMS E3 includes P1
* EMS E5 includes P2.

If you have an existing Enterprise Agreement or Server and Cloud Enrollment, you may already have Azure Premium. Check the details of your agreement.

### Workday License

You will also need the appropriate Workday license to meet your business needs. Improper number of licenses owned in the application may lead to errors during the provisioning/updating of a user.

## Environment Planning

### Cloud Tenants for Azure AD and Workday

Integrating HR business processes and identity workflows from Workday to Active Directory involves considerable amount of data validation, data transformation and end-to-end testing before deploying the solution into production.

* **Microsoft recommends** maintaining a clean separation between production and test environments and setting up a separate “TEST/POC Environment” with non-production Azure AD and Workday tenants. Workday test tenants are also referred to “implementation/deployment” tenants and these are separate from “production tenants”.

The Workday to AD User Provisioning solution requires configuring a Workday System Integration account with appropriate permissions to query Workday worker information. Refer to the [tutorial](https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/workday-inbound-tutorial#configure-a-system-integration-user-in-workday) for steps to create this system integration account. You will also need Azure AD Global Admin credentials to configure the Provisioning Agent and Provisioning App.

Use the Worksheet Workday and Azure AD Tenant Info to capture details of the Azure AD and Workday Cloud Tenants. This information will be used to configure the Workday to AD User Provisioning App at the time of the implementation.

Worksheet : Workday and Azure AD Tenant Info

|  |  |  |  |
| --- | --- | --- | --- |
| Configuration Parameter | Parameter Value | | Usage / Recommendation |
|  | **Non-Production** | **Production** |  |
| Workday Admin Portal URL | <Enter Value Here> | <Enter Value Here> | Use this URL to access the Workday Admin Portal to lookup user information directly in Workday |
| Workday Admin User ID | <Enter Value Here> | <Enter Value Here> | Use this ID to access Workday Admin Portal |
| Workday Admin Password |  |  | We recommend storing Workday Admin Password in a secure password vault. |
| Workday Web Services (WWS) Endpoint URL | <Enter Value Here> | <Enter Value Here> | This URL will be used to configure the Provisioning App in Azure AD Portal |
| WWS Integration Account ID | <Enter Value Here> | <Enter Value Here> | This refers to the Workday System Integration Account. |
| WWS Integration Account Password |  |  | We recommend storing the WWS Integration Account Password in a secure password vault. |
| Azure AD Admin Portal | <Enter Value Here> | <Enter Value Here> | Azure Admin Portal URL |
| Azure Global Admin User ID | <Enter Value Here> | <Enter Value Here> | This ID and Password will be used for Provisioning Agent Registration and configuring the Provisioning App. |
| Azure Global Admin Password | <Enter Value Here> | <Enter Value Here> |

### Active Directory Test and Production instances

Integrating HR business processes and identity workflows from Workday to Active Directory involves considerable amount of data validation, data transformation and end-to-end testing before deploying the solution into production.

* **For large deployments with more than 10K users, Microsoft recommends** setting up a separate TEST/POC Active Directory and pairing it to work with the non-production Azure AD and Workday tenants. This setup when coupled with periodic production data refresh strategies also assists in reproduction and troubleshooting of production defects.

If setting up a separate TEST/POC Active Directory is not feasible, you may create a separate TEST OU container in your production AD with appropriate delegated permissions for read and write to the specific OU.

Use the Worksheet Active Directory Info to capture Active Directory details. If you have more than one AD domains to integrate, create a copy of this Worksheet. This information will be used to configure the Workday to AD User Provisioning Agent at the time of the implementation.

Worksheet : Active Directory Info

|  |  |  |  |
| --- | --- | --- | --- |
| Configuration Parameter | Parameter Value | | Usage / Recommendation |
|  | **Non-Production** | **Production** |  |
| AD Domain Name (FQDN) | <Enter Value Here> | <Enter Value Here> | Capture the fully qualified domain name (e.g. corp.contoso.com) |
| AD Service Account ID | <Enter Value Here> | <Enter Value Here> | Use this ID to configure the Provisioning Agent. This ID must have read and write access to the containers that will store Workday Identity data. |
| AD Service Account Password |  |  | We recommend storing AD Service Account Password in a secure password vault. |
| AD Container DN | <Enter Value Here> | <Enter Value Here> | The default AD Container in which to create AD accounts for new users fetched from Workday. |

### On-prem servers for AAD Connect Provisioning Agent

The Workday to AD User Provisioning solution requires deploying one or more Provisioning Agents on servers running Windows 2012 R2 or Windows Server 2016 with minimum of 4 GB RAM. If you already have Azure AD Connect running on a Windows 2012 R2 server or Windows Server 2016, you may choose to run the Provisioning Agent on the same server.

* **In production environments, Microsoft recommends** that you have a minimum of 3 Provisioning Agents configured with your Azure AD tenant for high availability.

Use the Worksheet Provisioning Agent Installation Checklist to prepare for the deployment of the Provisioning Agent.

Worksheet : Provisioning Agent Installation Checklist

| # | Deployment Aspect | (Y/N) | Microsoft Recommendation |
| --- | --- | --- | --- |
| 1 | Have you identified Windows 2012 R2 or 2016 server(s) to install the Provisioning Agent? |  | If answer = N, please procure the necessary servers to install the Provisioning Agent. |
| 2 | Can the Provisioning Agent connect to your on-prem Active Directory from the Windows server host where you plan to install it? |  | If answer = N, please ensure that the Provisioning Agent is installed on a server host that can communicate with your on-prem AD. |
| 3 | Do you allow port 80/443/8080 outbound communication from the Windows server host where you plan to install the Provisioning Agent? |  | If answer = N, please ensure that firewall rules are configured to allow outbound 80/443/8080 communication to Azure AD tenant.   * If your firewall enforces rules according to the originating users, open these ports for traffic from Windows services that run as a network service. * If your firewall or proxy allows DNS whitelisting, whitelist connections to \*.msappproxy.net and \*.servicebus.windows.net. * For certificate validation, unblock the following URLs: mscrl.microsoft.com:80, crl.microsoft.com:80, ocsp.msocsp.com:80, and www.microsoft.com:80. |

### Security Review Planning

It is common for a security review to be required as part of a deployment of a new service. If a security review is required or has not yet been conducted, please review the many Azure AD [whitepapers](https://www.microsoft.com/download/details.aspx?id=36391) that will provides an overview for the identity as a service.

## Test Data Considerations

The quality of the Workday to AD User Provisioning solution largely depends on the quality of the test data available in the TEST/POC environment which is used during the early phases of solution design, validation and testing.

* **Microsoft recommends** creating a test environment that mirrors production with respect to user data quality and integrity to avoid surprises when the solution is rolled out into production. More specifically, ensure that there is consistency between test and production environments when it comes to Workday schema, AD schema, AD Hierarchy and customizations in Workday and AD.
* **Microsoft recommends** using techniques such as data redaction and data scrubbing when refreshing the test environment with production data to remove/mask sensitive PII (Personally Identifiable Information) data to comply with privacy and security standards.

## Capture Your Identity Lifecycle Requirements – The Joiners, Movers and Leavers Process

This section provides guidelines, worksheets and templates to capture your identity lifecycle management requirements in a format that will bring clarity to the design and implementation stages of the deployment. These guidelines, worksheets and templates can be used by System Integrators / Consultants / SMEs to work with various stakeholders during the requirements gathering stage to capture what the industry calls the Joiners-Movers-Leavers (JML) process.

### Workday and AD Characteristics

Before diving into the details of the Joiners-Movers-Leavers process, use Worksheet 4: Workday and AD Characteristics to capture aspects of the Workday and AD deployment that will impact the solution deployment topology.

Worksheet : Workday and AD Characteristics

| # | Question | Response |
| --- | --- | --- |
| 1 | How many AD domains do you plan to integrate with Workday HR? |  |
| 2 | If you have multiple AD domains, are these AD domains contiguous or [disjoint](https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/disjoint-namespace)? Disjoint namespaces can occur if your organization has gone through mergers or acquisitions in the past. |  |
| 3 | How many domain controllers are part of your AD topology? |  |
| 4 | Do you want a specific set of domain controllers to handle read and write requests arising out of this integration? |  |
| 5 | If the answer to question #4 is “Yes”, please specify the domain controller names and the geography in which they are located? |  |
| 6 | In which geography is your Workday tenant? |  |
| 7 | What is the size of your Workday tenant (including both active and inactive users)? |  |
| 8 | How many production Workday tenants do you plan to integration with on-prem AD? |  |

**Note:**  You will use the response captured above to make the following design decisions:

* [Design Decision #1 – Deployment Topology](#_Design_Decision_#1)
* [Design Decision #2 – Select Domain Controllers to handle Provisioning Requests](#_Design_Decision_#2)
* [Design Decision #11 – Plan and Prepare for Initial Sync](#_Design_Decision_#4)

### Joiners Process: Identity Data and Attribute Mapping

The Joiners Process (aka User on-boarding process) is initiated by one of the following business processes configured in Workday:

* Hire Employee
* Contract Contingent Worker

… and ends after successfully provisioning the necessary attributes in Active Directory for new account creation.

Use Worksheet 5: Joiners Business Process to capture various characteristics of the Joiners Process in your organization and how it is currently implemented for AD Account Creation.

Worksheet : Joiners Business Process

| # | Question | Response | Where is this information used? |
| --- | --- | --- | --- |
| 1 | Is Workday used to on-board both Employees and Contingent Workers? |  | To make [Design Decision #3 – Defining Scoping Filters](#_Design_Decision_#3) |
| 2 | Do you plan to use the Azure AD Workday-driven User Provisioning solution to manage both Employees and Contingent Workers? |  | To make [Design Decision #3 – Defining Scoping Filters](#_Design_Decision_#3) |
| 3 | Do you plan to rollout Workday-driven User Provisioning solution only for a subset of the Workday users? (For e.g. Employees only, Workers belonging to a certain business unit or location.) |  | To make [Design Decision #3 – Defining Scoping Filters](#_Design_Decision_#3) |
| 4 | On an average, how many new employees and/or contingent workers do you add per month? |  | Use this information to plan operational aspects around [reporting and monitoring](#_Reporting_and_monitoring) the solution |
| 5 | What is the unique ID in Workday that is used to identify each user? |  | To make [Design Decision #4 – Determine Matching Attribute(s)](#_Design_Decision_#4) |
| 6 | Do you plan to propagate custom attributes from Workday to AD? |  | To make [Design Decision #5 – Configure Custom Workday Attributes](#_Design_Decision_#5) |
| 7 | From an identity lifecycle perspective, how do you handle re-hires? Do rehires retain their old employee ID? |  | To make [Design Decision #4 – Determine Matching Attribute(s)](#_Design_Decision_#4) and [Design Decision #6 – Determine AD Account Status](#_Design_Decision_#6) |
| 8 | Do you process future-dated hires and created AD accounts for them in advance? |  |
| 9 | From an identity lifecycle perspective, how do you handle Employee to Contingent Worker conversion? |  |
| 10 | From an identity lifecycle perspective, how do you handle Contingent Worker to Employee conversion? |  |
| 11 | Do converted users retain their old AD account or do they get new ones? |  |
| 12 | Is the AD account creation process manual, automated or partially automated? Please describe the process or provide a reference to the documentation. |  | To make [Design Decision #7 –Attribute Mapping for Account Creation](#_Design_Decision_#7) |
| 13 | How do you generate unique attribute values for AD attributes such as CN, samAccountName and UPN? |  | To make [Design Decision #8 – Unique Value Generation](#_Design_Decision_#8) |
| 14 | What is the business logic for deciding the AD OU container to assign to a new user account? |  | To make [Design Decision #9 – AD OU Container Assignment](#_Design_Decision_#9) |
| 15 | How do you set and deliver temporary password of new user accounts? |  | To make [Design Decision #10 – Password delivery for new AD Accounts](#_Design_Decision_#10) |

### Movers Process: Identity Data and Attribute Mapping

The Movers Process (e.g. User transfer, Job Change, Location Change, Manager Change, Business Unit Change) is initiated by one of the following changes in Workday:

* Preferred Name Change
* Manager ID Change
* Primary Work Mobile Phone Change
* Supervisory Organization Change
* Worker Type Change
* Job Title Change

… and ends after successfully provisioning the necessary attributes in Active Directory for the user’s existing account.

Use Worksheet 6: Movers Business Process to capture various characteristics of the Movers Process in your organization and how it is currently implemented for AD Account updates.

Worksheet : Movers Business Process

| # | Question | Response | Where is this information used? |
| --- | --- | --- | --- |
| 1 | What attributes would you like to process whenever a “Movers” operation takes place in Workday? |  | To make [Design Decision #7 – Workday to AD User Attribute Mapping](#_Design_Decision_#7) |
| 2 | Do you perform any specific attribute validations at the time of user updates? If yes, please provide details. |  | To make [Design Decision #7 – Workday to AD User Attribute Mapping](#_Design_Decision_#7) |
| 3 | Should Supervisory Organization change move the user from one OU to another in AD? |  | To make [Design Decision #9 – AD OU Container Assignment](#_Design_Decision_#9) |

### Leavers Process: Identity Data and Attribute Mapping

The Leavers Process (aka User off-boarding) is initiated by one of the following business processes in Workday:

* Terminate Employee
* Rescind Hire/Contract
* End Contingent Worker Contract

… and ends after successfully de-provisioning or disabling the user’s account in Active Directory.

Use Worksheet 7: Leavers Business Process to capture various characteristics of the Leavers Process in your organization and how it is currently implemented for AD Account status changes and deletions.

Worksheet : Leavers Business Process

| # | Question | Response | Where is this information used? |
| --- | --- | --- | --- |
| 1 | Are terminations handled differently for Employees and Contingent Workers in AD? |  | To make [Design Decision #7 – Workday to AD User Attribute Mapping](#_Design_Decision_#7) and [Design Decision #6 – Determine AD Account Status](#_Design_Decision_#6) |
| 2 | How do you process the “Rescind” operation in AD? This needs to be handled if future dated hires are created in AD as part of the Joiner Process. |  | To make [Design Decision #6 – Determine AD Account Status](#_Design_Decision_#6) |
| 3 | What effective dates are considered for processing User Termination? |  | To make [Design Decision #7 – Workday to AD User Attribute Mapping](#_Design_Decision_#7) and [Design Decision #6 – Determine AD Account Status](#_Design_Decision_#6) |
| 4 | How do employee and contingent worker conversions impact existing AD accounts? |  | To make [Design Decision #7 – Workday to AD User Attribute Mapping](#_Design_Decision_#7) and [Design Decision #6 – Determine AD Account Status](#_Design_Decision_#6) |
| 5 | Do you disable AD accounts for users who are on extended leave? |  | To make [Design Decision #6 – Determine AD Account Status](#_Design_Decision_#6) |

# Designing end-to-end integration

This section will assist you in designing the Workday-driven User Provisioning solution in your environment that best meets your business needs.

## Design Decision #1 – Deployment Topology

The Workday-driven User Provisioning solution has 4 key components:

* Workday tenant
* Azure AD Provisioning App (aka Run Profile)
* Provisioning Agent
* On-prem Active Directory

The deployment topology could vary depending on the number of Workday tenants and on-prem Active Directory domains that you plan to integrate. Use the responses from Worksheet 4: Workday and AD Characteristics to arrive at a decision.

The table below summarizes the options available for commonly encountered Workday and AD combinations within enterprises.

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | # of Provisioning Agent Groups to configure | # of Provisioning App instances to configure | Deployment Topology description |
| 1 WD, 1 AD Domain | 1 | 1 | This is the simplest deployment topology wherein users from a single Workday tenant are mapped to a single AD domain. |
| 1 WD, “N” AD Domains with contiguous namespace | 1 | N | In this topology, a single Provisioning Agent group can serve multiple AD domains provided they are part of the same contiguous namespace. The only variance is the need to configure one Provisioning App instance / Run Profile per AD domain. |
| 1 WD, “N” AD Domains with disjoint namespace | N | N | In this topology, you will need one Provisioning Agent group and one Run Profile per disjoint namespace. |
| N WD, 1 AD Domain | 1 | N | If you plan to integrate multiple Workday instances with the same Active Directory domain, then you need to plan on configuring a separate Provisioning App / Run Profile per Workday instance. |

## Design Decision #2 – Select Domain Controllers to handle Provisioning Requests

During the on-prem Provisioning Agent installation, you will be provided an option to specify Domain Controllers that should handle provisioning requests. Use the responses from Worksheet 4: Workday and AD Characteristics to arrive at a decision considering aspects such as geographical affinity and proximity of the Provisioning Agent to the Domain Controller.

* **Microsoft recommends** setting this configuration if you have several geographically distributed domain controllers. Installing the Provisioning Agent in close proximity to the selected domain controller improves the reliability and performance of the end-to-end solution.

## Design Decision #3 – Defining Scoping Filters

When [configuring attribute mappings](https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/workday-inbound-tutorial#part-2-configure-attribute-mappings) in the Workday to AD User Provisioning app, you can set the **Source Object Scope** field to select which sets of users in Workday should be in scope for provisioning to AD, by defining a set of attribute-based filters. The default scope is “all users in Workday”.

Depending on your requirements, captured in Worksheet 5: Joiners Business Process you can design the scoping filter to only provision a subset of the Workday user population.

Example filters:

* Example: Scope to users with Worker IDs between 1000000 and 2000000
  + Attribute: WorkerID
  + Operator: REGEX Match
  + Value: (1[0-9][0-9][0-9][0-9][0-9][0-9])
* Example: Only employees and not contingent workers
  + Attribute: EmployeeID
  + Operator: IS NOT NULL

Use the Worksheet 8: Workday Scoping Filter to capture the scoping filters that will be used in your deployment

Worksheet : Workday Scoping Filter

| # | Scoping Filter Attribute | Operator | Attribute Value |
| --- | --- | --- | --- |
| 1 | WorkerID | REGEX Match | <Value> |
| 2 | Company | EQUALTO | <Value> |

## Design Decision #4 – Determine Matching Attribute(s)

When [configuring attribute mappings](https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/workday-inbound-tutorial#part-2-configure-attribute-mappings) in the Workday to AD User Provisioning app, you need to specify which attribute or attributes in Workday will be used to match with accounts presents in Active Directory. By default, the Workday *WorkerID* attribute is mapped to Active Directory *cn* attribute and this is set as the matching attribute pair.

Depending on your requirements, captured in Worksheet 5: Joiners Business Process you can set a different matching attribute pair. For e.g. *WorkerID* to *employeeID* attribute.

You can also set multiple matching attributes and assign a matching precedence. When there are multiple matching attributes, they are evaluated in the order based on matching precedence. As soon as a match is found, no further matching attributes are evaluated.

Use the Worksheet 9: Workday to AD Matching Attribute(s) to capture the matching attribute pair(s) that will be used in your deployment.

Worksheet : Workday to AD Matching Attribute(s)

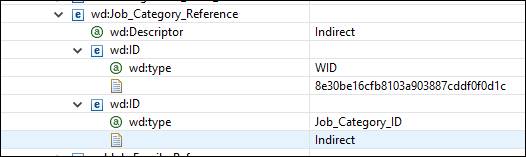
| # | Workday Attribute | AD Attribute | Matching Precedence | Matching Condition |
| --- | --- | --- | --- | --- |
| 1 | WorkerID | employeeID | 1 | Always |
| 2 | ContingentWorkerID | employeeID | 2 | Only during object creation |
|  |  |  |  |  |

## Design Decision #5 – Configure Custom Workday Attributes

The default list of Workday attributes shipped with the connector is documented in the Appendix section: [Default Workday attributes](#_Default_Workday_Attributes).

In addition to the default list, the Workday-driven User Provisioning solution supports configuring custom Workday attributes specific to your deployment. To include custom attributes from Workday, identify the XPath expression for the Workday Attribute and include it in the attribute mappings.

Example: To include “Job\_Category\_ID” in your attribute mappings, browse through the XML document in Workday Studio and build the XPath expression.



In this case, to pull the “indirect” value of the Job\_Category\_Reference element, use the XPath expression: /job\_Category\_Reference/wd:ID[@wd:type="Job\_Category\_ID"]/text()

Use the Worksheet 10: Custom Workday Attributes to capture the custom Workday attributes that will be used in your deployment. For details instructions around setting custom attributes, please refer to the [tutorial](https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/workday-inbound-tutorial#customizing-the-list-of-workday-user-attributes).

Worksheet : Custom Workday Attributes

| # | Workday Attribute | XPath Expression |
| --- | --- | --- |
| 1 | CountryReferenceTwoLetter | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/  wd:Business\_Site\_Summary\_Data/wd:Address\_Data/  wd:Country\_Reference/wd:ID[@wd:type='ISO\_3166-1\_Alpha-2\_Code']/text() |
| 2 |  |  |

## Design Decision #6 – Determine AD Account Status

By default, the Workday to AD User Provisioning connector uses the “Worker Status Data-> Active” field to determine whether to enable or disable the AD Account. This “not” of this value is assigned to a Boolean attribute “accountDisabled”.

Depending on your requirements, you may customize the mapping logic so that the AD Account is enabled or disabled based on a combination of data points. You can use [Azure AD expressions](https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/functions-for-customizing-application-data) to build custom business logic.

## Design Decision #7 – Workday to AD User Attribute Mapping

The Workday to AD User Provisioning Connector ships with default Workday to AD attribute mapping. Depending on the requirements captured in the Worksheet 5: Joiners Business Process and Worksheet 6: Movers Business Process, you can modify the attribute mappings that meets your integration goals.

Use the Worksheet 11: AD Account Creation Attribute Mapping to capture the attribute mapping to use at the time of AD Account Creation.

Worksheet : AD Account Creation Attribute Mapping

|  |  |  |  |
| --- | --- | --- | --- |
| Workday Attribute | Active Directory Attribute | Expression (if any) | Special Processing Remarks |
| WorkerID | employeeID |  |  |
| LastName, FirstName | cn | Use Join() function |  |
| UserId | sAMAccountName | Use SelectUniqueValue() function | Handle UniqueID Generation |
| !Active | accountDisabled |  |  |
| AddressLineData | streetAddress |  |  |
| CountryReference | country |  |  |
| CountryRegionReference | state |  |  |
| EmployeeID | employeeID |  | Only during object creation |
| EmployeeID | employeeNumber |  |  |
| Fax | facsimileTelephoneNumber |  |  |
| FirstName | givenName |  |  |
| JobFamilyID | department |  |  |
| LastName | sn |  |  |
| LocalReference | preferredLanguage |  |  |
| ManagerReference | manager |  |  |
| Mobile | mobile |  |  |
| Municipality | l |  |  |
| PostalCode | postalCode |  |  |
| PreferredNameData | displayName |  |  |
| Telephone | telephone |  |  |
| Title | title |  |  |
| WorkspaceReference | physicalDeliveryOfficeName |  |  |
| Populate based on the value of Municipality attribute | parentDistinguishedName | Use Switch() expression |  |
|  |  |  |  |

## Design Decision #8 – Unique Value Generation

Depending on the requirements captured in the Worksheet 5: Joiners Business Process you may need to generate unique values when setting attributes like CN, samAccountName and UPN that have uniqueness constraints.

To cater to such requirements, use the Azure AD function SelectUniqueValues.

Here is a brief synopsis of this function:

**SelectUniqueValue()** - Requires a minimum of two arguments, which are expressions representing values that will be checked for uniqueness in the target app. The first unique value found will be the one returned. If all the values already exist in the target, the entry will get escrowed and the reason gets logged in the audit logs. There is no upper bound to the number of arguments that can be provided.

Considerations:

1. This is a top-level function, it cannot be nested.
2. This function is only for entry creations.

Example usage in an expression:

SelectUniqueValue(

    Join("@", NormalizeDiacritics(Join(".",  [FirstName], [LastName])), "contoso.com"),

    Join("2@", NormalizeDiacritics(Join(".",  [FirstName], [LastName])), "contoso.com"),

   Join("3@", NormalizeDiacritics(Join(".",  [FirstName], [LastName])), "contoso.com"),

)

## Design Decision #9 – AD OU Container Assignment

It is common requirement to place AD user accounts into containers based on business units, locations and department. You can configure the business logic for OU assignment as part of the attribute mapping using the Azure AD [Switch()](https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/functions-for-customizing-application-data#switch) function and mapping it to the AD attribute *parentDistinguishedName*.

Example:

Switch([Municipality], "OU=Standard Users,OU=Users,OU=Default,OU=Locations,DC=contoso,DC=com", "Dallas", "OU=Standard Users,OU=Users,OU=Dallas,OU=Locations,DC=contoso,DC=com", "Austin", "OU=Standard Users,OU=Users,OU=Austin,OU=Locations,DC=contoso,DC=com", "Seattle", "OU=Standard Users,OU=Users,OU=Seattle,OU=Locations,DC=contoso,DC=com", “London", "OU=Standard Users,OU=Users,OU=London,OU=Locations,DC=contoso,DC=com")

## Design Decision #10 – Password Delivery for new AD Accounts

One of the final steps involved in new AD account provisioning is the delivery of the temporary password assigned to the user’s AD account. Many enterprises still use the traditional approach of delivering the temporary password to the user’s manager, who then hands over the password to the new hire/contingent worker. This process has an inherent security flaw and it could be used to launch insider attacks.

As part of the hiring process, HR teams usually run a background check and vet the mobile number of the new hire. With the Workday to AD User Provisioning integration, you can build on top of this fact and rollout a self-service password reset capability for the user on Day 1. This is accomplished by flowing the “Mobile Number” attribute of the new hire from Workday to AD and then from AD to Azure AD using AAD Connect. Once the “Mobile Number” is present in Azure AD, you can enable the [Self-Service Password Reset (SSPR)](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-authenticationdata) for the user’s account, so that on Day 1, she can use the registered and verified mobile number for authentication.

## Design Decision #11 – Plan and Prepare for Initial Sync

When the Azure AD provisioning service runs for the first time, it performs an initial sync against the Workday to create a snapshot of all user objects in Workday.

The time taken for initial syncs are directly dependent on how many users are present in the source system. Initial syncs for Workday tenants with over 100,000 users can take a long time.

* **For large Workday tenants (> 30,000 users), Microsoft recommends** running the initial sync in progressive stages and launching the full sync only after validating that the correct attributes are set in Active Directory for different user provisioning scenarios.
* Run the first initial sync only for a limited set of users by setting the [scoping filter](#_Design_Decision_#3).
* Verify AD account provisioning and attribute values set for the users selected for the first run. If the result meets your expectation, expand the scoping filter to progressively include more users and verify the results for the second run.
* Once you are satisfied with the results of the initial sync for test users, you can launch the full sync.

# Implementing Your Solution

This section is used to guide you through the implementation and testing of your Workday-driven User Provisioning solution using the end-to-end design captured in the previous section. This workflow is divided into four phases.

## Phase 1: Configure Workday-driven user provisioning in TEST environment

* **Microsoft recommends** that the initial configuration of Workday-driven User Provisioning should be done on a test environment with a small subset of users before scaling it to all users in production.

1. Refer to the Workday specific integration [tutorial](https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/workday-inbound-tutorial) to configure the provisioning agent and the user provisioning connector. Use the design and planning worksheets to complete the configuration.
2. Use the attribute mapping design decision worksheets from the previous section to customize your desired user attribute mappings for Workday to Active Directory per the [instructions here](https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/workday-inbound-tutorial#part-2-configure-attribute-mappings).
3. If the data values between your source and target systems are incompatible, you can [configure expressions for attribute mappings](https://docs.microsoft.com/azure/active-directory/active-directory-saas-writing-expressions-for-attribute-mappings) that will convert your users data into formats that are more acceptable for AD.
4. Configure the desired users that you would like to provision from Workday to AD using [scoping filters](https://docs.microsoft.com/azure/active-directory/active-directory-saas-scoping-filters).
5. Run the initial sync to load Workday data into AD.

## Phase 2: User Acceptance Testing (UAT)

Once you have configured Workday-driven User Provisioning, you will need to run test cases to verify whether this solution meets your organization’s requirements. These test cases should reflect your Business Use Cases. Use the table below to document your test scenarios along with the expected and actual results:

|  |  |  |
| --- | --- | --- |
| Scenarios | Expected Results | Actual Results |
| *e.g. New Employee Hire in Workday* | *e.g. User Account is provisioned in AD. User can log into AD-domain applications and perform the desired actions.* |  |
| *e.g. User is terminated in Workday* | *e.g. User Account is disabled in AD. User cannot log into any enterprise applications protected by AD.* |  |
| *e.g. User Supervisory Organization is updated in Workday* | *e.g. User Account moves from one OU to another OU in AD.* |  |
|  |  |  |

Use the results above to determine how to transition your Workday-driven User Provisioning implementation into production based on your established timelines. Feel free to extend the above table as needed.

## Phase 3: Transitioning into production

Once your testing is complete and successful, move your Workday-driven User Provisioning implementation into production by repeating all the steps in Phase 1 to Phase 3 in your production environment.

## Phase 4: Rollback steps

If the automatic user provisioning implementation fails to work as desired in the production environment, the following rollback steps below can assist you in reverting back to a previous known good state:

* 1. Review the [provisioning summary report](https://docs.microsoft.com/azure/active-directory/active-directory-saas-provisioning-reporting#getting-provisioning-reports-from-the-azure-management-portal) and [provisioning audit logs](https://docs.microsoft.com/azure/active-directory/active-directory-saas-provisioning-reporting#provisioning-audit-logs) to determine what the incorrect operations were performed on the affected users and/or groups.
  2. The last known good state of the users affected can be determined through the provisioning audit logs or by reviewing the AD logs.
  3. Work with the AD Admin to update the users affected directly in AD using the last known good state values.

# Operationalize your Implementation

This section will guide you in best practices to maintain the Workday-driven User Provisioning solution that has been deployed.

## Reporting and monitoring

Azure AD can provide additional insights into your organization’s user provisioning usage and operational health through audit logs and reports. The table below lists the provisioning reports and logs available along with the insights that they provide:

| Report Type | Insights | Location |
| --- | --- | --- |
| Provisioning summary report | * The total number of users that have been synchronized and are currently in scope for provisioning. * The last time the synchronization was run which typically occur every 20-40 minutes, after a full synchronization has completed. * Determine if an initial full synchronization has been completed. * Whether or not the provisioning process has been placed in quarantine, and what the reason for the quarantine status is. | * Azure management portal |
| Provisioning audit logs | * Import events - recorded each time the Azure AD provisioning service retrieves information about an individual user or group. * Synchronization rule events - report on the results of the attribute mapping rules and any configured scoping filters, after user data has been imported. * Export events - recorded each time the Azure AD provisioning service writes a user account to a target system (in this case AD). These events record all user attributes and their values that were written by the Azure AD provisioning service at the time of the event. If there was an error while writing the user account or group object to the target system, it will be displayed here. * Process escrow - occur when the provisioning service encounters a failure while attempting an operation and begins to retry the operation on a back-off interval of time. An "escrow" event is recorded each time a provisioning operation was retired. | * Azure management portal * Audit API |
| Provisioning Digest Report | * You can deploy the PowerShell script at this location to generate daily digest reports around user provisioning. Here are the features of this PowerShell script:   + Reads all user account provisioning events from the Azure AD graph for a specified time period, and emits a digest report.   + The digest report is written to a text file on the host system, and can also be sent over email using an Office365 email account   + This script can be scheduled to run at any desired time interval using the Windows Task Scheduler | * [GitHub](https://github.com/asmalser-msft/AAD-User-Provisioning-Digest-Report) |

To learn more about how to navigate the user provisioning reports and audit logs, refer to the [tutorial here](https://docs.microsoft.com/azure/active-directory/active-directory-saas-provisioning-reporting).

* **Microsoft recommends** that you assume ownership of and consume these reports on a regular basis based on your organization’s requirements. Azure AD retains most audit data for 30 days.

## Troubleshooting

To learn more about common issues that affect automatic user provisioning and how to resolve them, refer to the [troubleshooting documentation here](https://docs.microsoft.com/azure/active-directory/active-directory-application-provisioning-content-map). The table below documents additional user provisioning issues that should be considered:

|  |  |  |
| --- | --- | --- |
| Issue | Possible Cause | Recommended Steps |
| User provisioning stopped working despite configuration not being changed since last known good state. | The admin account password for your application in the **Admin Credentials** section may have been changed and/or expired. | * Verify if you are indeed failing on incorrect credentials by reviewing the provisioning audit logs. * Update your admin account password in your application. |
| You have updated the admin account password for your application in the **Admin Credentials** section but have not yet updated the **Security Token**. | * Verify if you are indeed failing on incorrect credentials by reviewing the provisioning audit logs. * Update your Security Token in the Azure AD portal for your application. |

## Reference Documentation

1. [Debug SAML-based SSO](https://docs.microsoft.com/azure/active-directory/develop/active-directory-saml-debugging)
2. [Customizing claim issued in SAML token](https://docs.microsoft.com/azure/active-directory/develop/active-directory-saml-claims-customization)
3. [Single Sign-on SAML protocol](https://docs.microsoft.com/azure/active-directory/develop/active-directory-single-sign-on-protocol-reference)
4. [Single Sign-Out SAML protocol](https://docs.microsoft.com/azure/active-directory/develop/active-directory-single-sign-out-protocol-reference)
5. [Azure AD B2B](https://docs.microsoft.com/azure/active-directory/active-directory-b2b-what-is-azure-ad-b2b) (for external users such as partners and vendors)
6. [Azure AD Conditional Access](https://docs.microsoft.com/azure/active-directory/active-directory-conditional-access-azure-portal)
7. [Azure Identity Protection](https://docs.microsoft.com/azure/active-directory/active-directory-identityprotection)
8. [SSO access](https://docs.microsoft.com/azure/active-directory/active-directory-appssoaccess-whatis)
9. [MFA Conditional Access for SaaS](https://docs.microsoft.com/azure/active-directory/active-directory-playbook-building-blocks#mfa-conditional-access-for-saas-applications)
10. [Configure Token Lifetimes](https://docs.microsoft.com/azure/active-directory/active-directory-configurable-token-lifetimes)
11. [Claim mapping for Apps via PowerShell](https://docs.microsoft.com/azure/active-directory/active-directory-claims-mapping)
12. [Overview of Azure AD automatic user provisioning](https://docs.microsoft.com/azure/active-directory/active-directory-saas-app-provisioning)
13. [Application specific integration tutorials for user provisioning](https://docs.microsoft.com/azure/active-directory/active-directory-saas-tutorial-list)
14. [Azure AD BYOA SCIM user provisioning](https://docs.microsoft.com/azure/active-directory/active-directory-scim-provisioning)

# Appendix

## Default Workday Attributes

Given below is the list of default Workday attributes that are supported by the connector. You can update the XPath Expression for your deployment.

| Attribute Name | Workday XPath Expression |
| --- | --- |
| Active | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Active/text() |
| AddressLine2Data | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Business\_Site\_Summary\_Data/wd:Address\_Data/wd:Address\_Line\_Data[@wd:Type='ADDRESS\_LINE\_2']/text() |
| AddressLine3Data | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Business\_Site\_Summary\_Data/wd:Address\_Data/wd:Address\_Line\_Data[@wd:Type='ADDRESS\_LINE\_3']/text() |
| AddressLine4Data | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Business\_Site\_Summary\_Data/wd:Address\_Data/wd:Address\_Line\_Data[@wd:Type='ADDRESS\_LINE\_4']/text() |
| AddressLine5Data | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Business\_Site\_Summary\_Data/wd:Address\_Data/wd:Address\_Line\_Data[@wd:Type='ADDRESS\_LINE\_5']/text() |
| AddressLine6Data | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Business\_Site\_Summary\_Data/wd:Address\_Data/wd:Address\_Line\_Data[@wd:Type='ADDRESS\_LINE\_6']/text() |
| AddressLine7Data | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Business\_Site\_Summary\_Data/wd:Address\_Data/wd:Address\_Line\_Data[@wd:Type='ADDRESS\_LINE\_7']/text() |
| AddressLine8Data | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Business\_Site\_Summary\_Data/wd:Address\_Data/wd:Address\_Line\_Data[@wd:Type='ADDRESS\_LINE\_8']/text() |
| AddressLine9Data | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Business\_Site\_Summary\_Data/wd:Address\_Data/wd:Address\_Line\_Data[@wd:Type='ADDRESS\_LINE\_9']/text() |
| AddressLineData | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Business\_Site\_Summary\_Data/wd:Address\_Data/wd:Address\_Line\_Data/text() |
| BusinessTitle | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Business\_Title/text() |
| Company | wd:Worker/wd:Worker\_Data/wd:Organization\_Data/wd:Worker\_Organization\_Data[translate(string(wd:Organization\_Data/wd:Organization\_Type\_Reference/wd:ID[@wd:type='Organization\_Type\_ID']),'abcdefghijklmnopqrstuvwxyz','ABCDEFGHIJKLMNOPQRSTUVWXYZ')='COMPANY']/wd:Organization\_Reference/@wd:Descriptor |
| ContingentWorkerID | wd:Worker/wd:Worker\_Reference/wd:ID[@wd:type='Contingent\_Worker\_ID']/text() |
| CountryReference | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Business\_Site\_Summary\_Data/wd:Address\_Data/wd:Country\_Reference/wd:ID[@wd:type='ISO\_3166-1\_Alpha-3\_Code']/text() |
| CountryReferenceFriendly | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Business\_Site\_Summary\_Data/wd:Address\_Data/wd:Country\_Reference/@wd:Descriptor |
| CountryReferenceNumeric | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Business\_Site\_Summary\_Data/wd:Address\_Data/wd:Country\_Reference/wd:ID[@wd:type='ISO\_3166-1\_Numeric-3\_Code']/text() |
| CountryReferenceTwoLetter | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Business\_Site\_Summary\_Data/wd:Address\_Data/wd:Country\_Reference/wd:ID[@wd:type='ISO\_3166-1\_Alpha-2\_Code']/text() |
| CountryRegionReference | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Business\_Site\_Summary\_Data/wd:Address\_Data/wd:Country\_Region\_Reference/@wd:Descriptor |
| EmailAddress | wd:Worker/wd:Worker\_Data/wd:Personal\_Data/wd:Contact\_Data/wd:Email\_Address\_Data[translate(string(wd:Usage\_Data/wd:Type\_Data/wd:Type\_Reference/@wd:Descriptor),'abcdefghijklmnopqrstuvwxyz','ABCDEFGHIJKLMNOPQRSTUVWXYZ')='WORK']/wd:Email\_Address/text() |
| EmployeeID | wd:Worker/wd:Worker\_Reference/wd:ID[@wd:type='Employee\_ID']/text() |
| FacilityLocation | wd:Worker/wd:Worker\_Data/wd:Organization\_Data/wd:Worker\_Organization\_Data[translate(string(wd:Organization\_Data/wd:Organization\_Type\_Reference/wd:ID[@wd:type='Organization\_Type\_ID']),'abcdefghijklmnopqrstuvwxyz','ABCDEFGHIJKLMNOPQRSTUVWXYZ')='FACILITY']/wd:Organization\_Reference/@wd:Descriptor |
| Fax | wd:Worker/wd:Worker\_Data/wd:Personal\_Data/wd:Contact\_Data/wd:Phone\_Data[translate(string(wd:Phone\_Device\_Type\_Reference/@wd:Descriptor),'abcdefghijklmnopqrstuvwxyz','ABCDEFGHIJKLMNOPQRSTUVWXYZ')='FAX' and translate(string(wd:Usage\_Data/wd:Type\_Data/wd:Type\_Reference/@wd:Descriptor),'abcdefghijklmnopqrstuvwxyz','ABCDEFGHIJKLMNOPQRSTUVWXYZ')='WORK']/@wd:Formatted\_Phone |
| FirstName | wd:Worker/wd:Worker\_Data/wd:Personal\_Data/wd:Name\_Data/wd:Legal\_Name\_Data/wd:Name\_Detail\_Data/wd:First\_Name/text() |
| JobClassificationID | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Job\_Classification\_Summary\_Data/wd:Job\_Classification\_Reference/wd:ID[@wd:type='Job\_Classification\_Reference\_ID']/text() |
| JobFamilyID | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Job\_Profile\_Summary\_Data/wd:Job\_Family\_Reference/wd:ID[@wd:type='Job\_Family\_ID']/text() |
| LastName | wd:Worker/wd:Worker\_Data/wd:Personal\_Data/wd:Name\_Data/wd:Legal\_Name\_Data/wd:Name\_Detail\_Data/wd:Last\_Name/text() |
| LeaveAbsenceType | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Leave\_Status\_Data[wd:On\_Leave='1']/wd:Leave\_of\_Absence\_Type\_Reference/wd:ID[@wd:type='Leave\_of\_Absence\_Type\_ID']/text() |
| LocalReference | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Business\_Site\_Summary\_Data/wd:Local\_Reference/wd:ID[@wd:type='Locale\_ID']/text() |
| LocationIdentifier | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Business\_Site\_Summary\_Data/wd:Location\_Reference/wd:ID[@wd:type='Location\_ID']/text() |
| ManagerReference | wd:Worker/wd:Worker\_Data/wd:Management\_Chain\_Data/wd:Worker\_Supervisory\_Management\_Chain\_Data[position()=1]/wd:Management\_Chain\_Data[last()=position()]/wd:Manager\_Reference/wd:ID[@wd:type='WID']/text() |
| MiddleName | wd:Worker/wd:Worker\_Data/wd:Personal\_Data/wd:Name\_Data/wd:Legal\_Name\_Data/wd:Name\_Detail\_Data/wd:Middle\_Name/text() |
| Mobile | wd:Worker/wd:Worker\_Data/wd:Personal\_Data/wd:Contact\_Data/wd:Phone\_Data[translate(string(wd:Phone\_Device\_Type\_Reference/@wd:Descriptor),'abcdefghijklmnopqrstuvwxyz','ABCDEFGHIJKLMNOPQRSTUVWXYZ')='MOBILE' and translate(string(wd:Usage\_Data/wd:Type\_Data/wd:Type\_Reference/@wd:Descriptor),'abcdefghijklmnopqrstuvwxyz','ABCDEFGHIJKLMNOPQRSTUVWXYZ')='WORK']/@wd:Formatted\_Phone |
| Municipality | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Business\_Site\_Summary\_Data/wd:Address\_Data/wd:Municipality/text() |
| PositionID | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Position\_ID/text() |
| PositionTitle | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Position\_Title/text() |
| PostalCode | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Business\_Site\_Summary\_Data/wd:Address\_Data/wd:Postal\_Code/text() |
| PreferredFirstName | wd:Worker/wd:Worker\_Data/wd:Personal\_Data/wd:Name\_Data/wd:Preferred\_Name\_Data/wd:Name\_Detail\_Data/wd:First\_Name/text() |
| PreferredLastName | wd:Worker/wd:Worker\_Data/wd:Personal\_Data/wd:Name\_Data/wd:Preferred\_Name\_Data/wd:Name\_Detail\_Data/wd:Last\_Name/text() |
| PreferredMiddleName | wd:Worker/wd:Worker\_Data/wd:Personal\_Data/wd:Name\_Data/wd:Preferred\_Name\_Data/wd:Name\_Detail\_Data/wd:Middle\_Name/text() |
| PreferredNameData | wd:Worker/wd:Worker\_Data/wd:Personal\_Data/wd:Name\_Data/wd:Preferred\_Name\_Data/wd:Name\_Detail\_Data/@wd:Formatted\_Name |
| PrimaryWorkTelephone | wd:Worker/wd:Worker\_Data/wd:Personal\_Data/wd:Contact\_Data/wd:Phone\_Data[wd:Usage\_Data/wd:Type\_Data/@wd:Primary='1' and translate(string(wd:Usage\_Data/wd:Type\_Data/wd:Type\_Reference/@wd:Descriptor),'abcdefghijklmnopqrstuvwxyz','ABCDEFGHIJKLMNOPQRSTUVWXYZ')='WORK']/@wd:Formatted\_Phone |
| StatusAcademisTenureDate | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Academic\_Tenure\_Date/text() |
| StatusActiveStatusDate | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Active\_Status\_Date/text() |
| StatusBenefitsServiceDate | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Benefits\_Service\_Date/text() |
| StatusCompanyServiceDate | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Company\_Service\_Date/text() |
| StatusContinuousFirstDayOfWork | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:First\_Day\_of\_Work/text() |
| StatusContinuousServiceDate | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Continuous\_Service\_Date/text() |
| StatusDateEnteredWorkforce | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Date\_Entered\_Workforce/text() |
| StatusDaysUnemployed | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Days\_Unemployed/text() |
| StatusEndEmploymentDate | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:End\_Employment\_Date/text() |
| StatusExpectedRetirementDate | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Expected\_Retirement\_Date/text() |
| StatusHireDate | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Hire\_Date/text() |
| StatusMonthsContinuousPriorEmployment | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Months\_Continuous\_Prior\_Employment/text() |
| StatusNotEligibleForHire | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Not\_Eligible\_For\_Hire/text() |
| StatusNotEligibleForRehire | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Not\_Eligible\_for\_Rehire/text() |
| StatusOriginalHireDate | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Original\_Hire\_Date/text() |
| StatusProbationEndDate | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Probation\_End\_Date/text() |
| StatusProbationStartDate | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Probation\_Start\_Date/text() |
| StatusRegrettableTermination | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Regrettable\_Termination/text() |
| StatusRehire | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Rehire/text() |
| StatusResignationDate | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Resignation\_Date/text() |
| StatusRetired | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Retired/text() |
| StatusRetirementDate | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Retirement\_Date/text() |
| StatusRetirementEligibilityDate | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Retirement\_Eligibility\_Date/text() |
| StatusSeniorityDate | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Seniority\_Date/text() |
| StatusSeveranceDate | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Severance\_Date/text() |
| StatusTerminated | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Terminated/text() |
| StatusTerminationDate | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Termination\_Date/text() |
| StatusTerminationInvoluntary | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Termination\_Involuntary/text() |
| StatusTerminationLastDayOfWork | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Termination\_Last\_Day\_of\_Work/text() |
| StatusTimeOffServiceDate | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Time\_Off\_Service\_Date/text() |
| StatusVestingDate | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Worker\_Status\_Data/wd:Vesting\_Date/text() |
| SupervisoryOrganization | wd:Worker/wd:Worker\_Data/wd:Organization\_Data/wd:Worker\_Organization\_Data/wd:Organization\_Data[translate(string(wd:Organization\_Type\_Reference/wd:ID[@wd:type='Organization\_Type\_ID']),'abcdefghijklmnopqrstuvwxyz','ABCDEFGHIJKLMNOPQRSTUVWXYZ')='SUPERVISORY']/wd:Organization\_Name/text() |
| Telephone | wd:Worker/wd:Worker\_Data/wd:Personal\_Data/wd:Contact\_Data/wd:Phone\_Data[translate(string(wd:Phone\_Device\_Type\_Reference/@wd:Descriptor),'abcdefghijklmnopqrstuvwxyz','ABCDEFGHIJKLMNOPQRSTUVWXYZ')='TELEPHONE' and translate(string(wd:Usage\_Data/wd:Type\_Data/wd:Type\_Reference/@wd:Descriptor),'abcdefghijklmnopqrstuvwxyz','ABCDEFGHIJKLMNOPQRSTUVWXYZ')='WORK']/@wd:Formatted\_Phone |
| TransactionLogData | wd:Worker/wd:Worker\_Data/wd:Transaction\_Log\_Entry\_Data/wd:Transaction\_Log\_Entry |
| UserID | wd:Worker/wd:Worker\_Data/wd:User\_ID/text() |
| WID | wd:Worker/wd:Worker\_Reference/wd:ID[@wd:type='WID']/text() |
| WorkerID | wd:Worker/wd:Worker\_Data/wd:Worker\_ID/text() |
| WorkerType | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Worker\_Type\_Reference/@wd:Descriptor |
| WorkSpaceReference | wd:Worker/wd:Worker\_Data/wd:Employment\_Data/wd:Position\_Data/wd:Work\_Space\_\_Reference/@wd:Descriptor |

**IMPORTANT NOTICES**

© 2018 Microsoft Corporation.  All rights reserved.  This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.   
Some examples are for illustration only and are fictitious. No real association is intended or inferred.   
   
This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You may modify this document for your internal, reference purposes