



Microsoft Dynamics 365 Finance and Operations Connector Guide v2021.x



Copyright

saviynt.com

© 2022 Saviynt. All rights reserved. No part of this document may be reproduced or used in any manner without the prior written permission of the copyright owner.

CONTENTS

ABOUT THIS GUIDE _____ 1

INTRODUCTION _____ 3

UNDERSTANDING THE INTEGRATION BETWEEN EIC AND MICROSOFT
DYNAMICS 365 _____ 6

USING THE MICROSOFT DYNAMICS 365 CONNECTOR _____ 34

TROUBLESHOOTING _____ 36

About this Guide

This guide describes the Microsoft Dynamics 365 Finance and Operations Connector that is used to integrate Saviynt Enterprise Identity Cloud (EIC) with Microsoft Dynamics 365 for Finance and Operations.

Audience

This guide is intended for administrators and target system integration teams responsible for implementing a secure integration service with Microsoft Dynamics 365 Finance and Operations.

Text Conventions

The following text conventions have been used in this document:

Convention	Meaning
bold	Indicates graphical user interface elements that are associated with an action.
<i>italic</i>	Indicates guide titles and placeholder text for which you specify values.
<code>inline code</code>	Indicates code elements, executable commands, cmd prompt input or output details, and URLs.
courier new	Indicates parameter values and directory or file paths.

Related Documents

In addition to the information provided in this guide, refer to the see [Saviynt Enterprise Identity Cloud Connectors](#) page for related information.

Access to Saviynt Support

Saviynt customers can contact Saviynt Support at <https://saviynt.freshdesk.com/support/home>.

Introduction

Microsoft Dynamics 365 is a set of connected modular SaaS applications and services designed to both transform and enable your core customer, employee, contractor, and business activities. Using Dynamics 365, you can integrate your data, business logic, and processes. It's built on Microsoft Azure and uses Common Data Service (CDS) as a foundation for data integration across all Dynamics 365 applications and services, productivity and collaboration apps in Microsoft 365, as well as your in-house and even SaaS applications in other clouds.

Saviynt provides a connector framework to perform the following operations:

- Import users, accounts, roles, duties, privileges, organizations, and permissions from the Dynamics 365 Finance and Operations (F&O) application to Saviynt Enterprise Identity Cloud (EIC).
- Provision user accounts and entitlements from EIC to the Dynamics 365 F&O application.

This framework enables EIC to deliver comprehensive security by providing visibility, management, and governance features - knowing "who has access to what" at the fine-grained level along with the capabilities to monitor unauthorized access assignment(s) and risky access mappings at all times. This connector also provides analytical capabilities such as creating analytical reports and performing SOD analysis.

Supported Features

The connector supports the following features:

Feature	Supported Operation	Description
Import	User Import	Supports full or filter-based import of users (workers, employees, and contractors). For more information about how to import users, see Introduction .
	Accounts Import	Supports full or filter-based import of accounts (SystemUsers) to EIC after the users are available in EIC. For more information, see Introduction .
	Access Import (Roles, Duties, Privileges, Organizations, and Permissions)	Supports full import of Roles, Duties, Privileges, Permissions, and Organizations as entitlements into EIC.
Provisioning	Account Management	<p>Supports the following operations:</p> <ul style="list-style-type: none"> • Creating, updating, enabling, disabling, and removing user accounts (SystemUsers) • Adding and removing SystemUser access for a Security role • Adding an organization for a Security role

Use Cases Supported by the Microsoft Dynamics 365 Connector

The connector can integrate with the Dynamics 365 F&O application to import users, accounts, and access data into EIC and provision the imported user accounts and entitlements.

Access import enables you to manage the following objects in EIC:

- Roles
- Duties
- Privileges
- Organizations
- Permissions

Provisioning enables you to manage user accounts and entitlements from EIC.

Supported Software Versions

Software	Version
EIC	Version 4.4 and later
Microsoft Dynamics 365	2019 release and later

Understanding the Integration between EIC and Microsoft Dynamics 365

You must create an integration between EIC and the collaboration platform hosted by the target application to perform the import, provisioning, and deprovisioning tasks. The following components are involved in the integration:

Connected Application is the target application for which EIC manages the identity repository.

Security System represents the connection between EIC and the target application.

- It comprises of an endpoint, which is the target application for which EIC manages the identity repository. For more information about creating a security system,
- It provides application instance abstraction from connectivity including high-level metadata.

You can select one connection for importing data from the target application and another connection for provisioning data to the target application. For more information about creating a security system, see [Creating A Security System](#) in the *Enterprise Identity Cloud Administration Guide*.

Endpoint is an instance of an application within the context of a security system.

- It is the target application or application from where the connector imports the data and performs provisioning or deprovisioning of identity objects such as users, accounts, and entitlements.
- It is mandatory to create an endpoint after creating the security system.

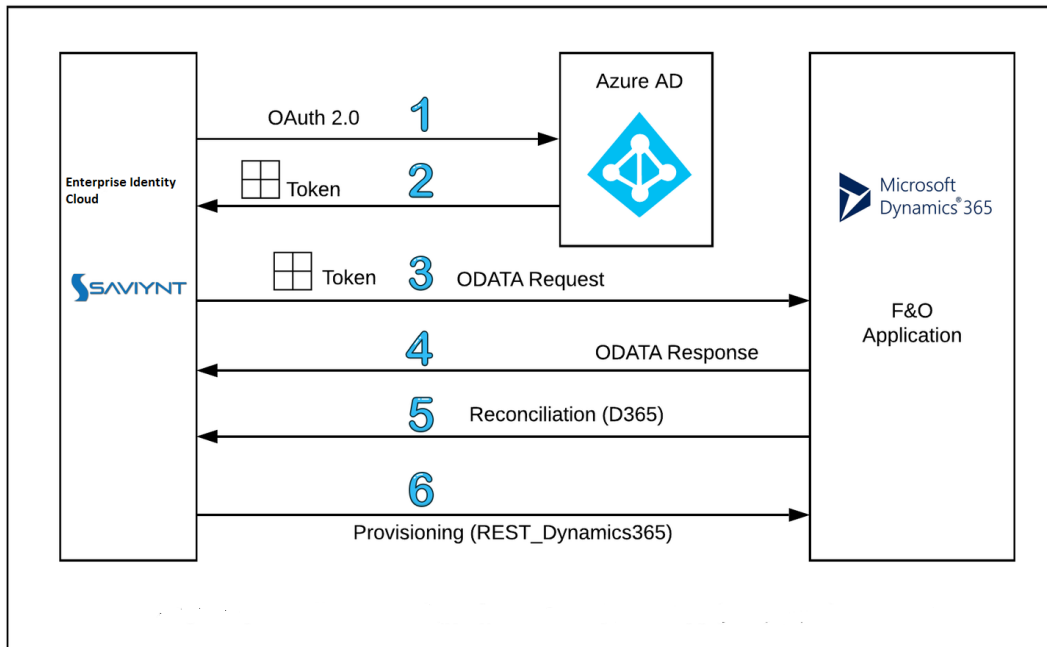
You can associate a single security system with multiple endpoints if the deployment involves modelling of multiple isolated virtual applications (based on sets of specific entitlements according to certain categories) within a single application instance. For more information, see [Creating Endpoints](#) in the *Enterprise Identity Cloud Administration Guide*.

Connector is a software component that enables communication between EIC and the target application through the Open Data Protocol (OData).

It provides a simplified integration mechanism where you only need to create a connection with minimal connectivity information for your target application. For example, to create a connection, select the **D365** connection type for importing data, the **REST_Dynamics365 (REST)** connection type for performing provisioning and de-provisioning tasks, and specify Base URL, Tenant ID, Login URL, Client ID, and Client Secret to connect it.

Connector Architecture

The connector integrates with Dynamics 365 via the OData Protocol. The following diagram illustrates the connector architecture and communication with the target application.



1. EIC connects with Azure AD using the Dynamics 365 connector and requests an access token.
2. The Azure AD provides the access token to EIC via the Dynamics 365 connector.
3. The connector uses the access token to authenticate to the Dynamics 365 F&O application (ODATA request). Data from the Dynamics 365 F&O application (ODATA response) is returned to EIC.
4. Data from the Dynamics 365 F&O application (ODATA response) is returned to EIC. For more details about OAuth 2.0 on the Microsoft identity platform, see the [Microsoft documentation](#) web site.
5. User accounts and access information is imported from the Dynamics 365 F&O application to EIC.
6. (Optional) Account management operation (provisioning) is performed from EIC to the Dynamics 365 F&O application.

Data Model

The following table provides details about the mapping of data-types and objects between the Dynamics 365 F&O application and EIC.

Saviynt Object	Dynamics 365 F&O Object
User	Workers (Employees and Contractors)
Accounts	SystemUsers
Entitlement	Roles, Duties, Privileges, Organizations, and Permissions

Terms Used in this Document

The following terms are used in this document:

Terms	Description
User	Workers/employees/contractors objects in the Dynamics 365 F&O environment.
Role	Group of duties required for a job function.
Privilege	Access required to do a job.
Duty	Group of related privileges required for a job function.
Permission	Group of base objects and required permissions.

Configuring a Connection

You must perform the following tasks in sequence to integrate EIC with the target application:

1. Register the Dynamics 365 F&O connector application in the Azure environment
2. Create a connection
 - a. Define the connection and reconciliation properties.
 - b. Create a security system.
 - c. Create an endpoint for the security system.
3. Import users, account, and other objects
 - a. Run the User Import job to import users.
 - b. Run the Data Import job to import accounts.
 - c. Run the Data Import job to import access related objects.
4. (Optional) Provision/de-provision accounts and entitlements to users
 - a. Create a request.
 - b. Approve the request.
 - c. Run the provisioning job.

Registering the Connector in the Azure Environment

You must register the Dynamics 365 F&O connector as a client application in the Azure environment to obtain the client ID and client secret for authenticating to the Dynamics 365 F&O application. Perform the following steps to register an application and provide the required permissions in the Azure Portal:

1. Login into Azure Portal <https://portal.azure.com/> with Azure Admin credentials to access the Azure AD directory associated with Azure ID Tenant.
2. Click **Azure Active Directory>App registrations>New registration** to register a new application.
3. Enter the user-facing display name of the application in the **Name** field.
4. Select **Accounts in this organizational directory only (your enterprise directory [example: Saviynt.com])** under the **Supported account types** field.
5. Click **Register** to register the new application.
6. Click **View API Permissions** to view the configured permissions.
7. Click **Add a permission > APIs my organization uses** and select **ConnectorFullAccess** application API permission. The user must be a global administrator in the Azure ID tenant and have the System administrator role in the Azure Finance and Operations application.
8. Click **Add Permissions** to add the selected permission. You can now access the AccessDynamics Connector Service APIs.
9. Click **System administration** located on the left navigation pane and navigate to **Workspaces>Setup > Azure Active Directory applications** to view the added Azure active directory applications client IDs.
10. Select **New** to add a new active directory application.
11. Fill in the following fields for the new record:
 - Enter the application ID that you have registered in Azure AD in the **Client ID** field.
 - Enter a name for the application in the **Name** field.

- Select an appropriate service account user ID in the **User ID** field. You must provide a dedicated service account that has the correct permissions for the operations that must be performed.

12. Click **Save**.

Creating a Connection

You must create two separate connections to perform reconciliation (D365 connection type) and provisioning operations. While the connection parameters for authenticating to Azure AD are common for both connections, the provisioning connection (REST_Dynamics365 (REST) connection type needs you to specify additional parameters for REST connectivity to the target application.



Note

The Connection Template displays the connection parameters in two categories such as **Basic Config** and **Advanced Config**. The **Basic Config** category displays the minimum set of parameters required to establish a connection. The **Advanced Config** category displays the advanced parameters. When you define and save the values for the parameters in **Basic Config**, those values are automatically populated in the **Advanced Config** page for the parameters where they are referred. To modify any of the values for advanced parameters, click **Advanced Config**.

To create a connection, perform the following steps:

1. Log in to EIC.
2. Click **ADMIN > Identity Repository > Connections > Create Connection**.

3. Specify the values for the following fields and click **Save & Test Connection**.

Ensure that all mandatory parameters are specified.

Parameters for Establishing a Connection

The following parameters are required for establishing a connection:



Note

Do not populate the parameters that are not listed in the below table.


Parameter	Description
Connection Name	Provide a name for the connection.
Connection Description	Provide a description for the connection.
Connection Type	<p>Select a Connection Type based on the operation you want the connector to perform:</p> <ul style="list-style-type: none"> • Select the connection type as D365 for reconciliation operations. • Select REST_Dynamics365 (REST) for provisioning and de-provisioning operations.
Base URL	<p>Provide the Base URL for the application. It will differ based on your access URL. For example:</p> <p>https://acme.cloudax.dynamics.com</p>


Parameter	Description
TENANT_ID	<p>Provide the tenant ID.</p> <p>Example: xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx</p>
LOGIN_URL	<p>Provide the Microsoft authentication URL.</p> <p>https://login.microsoftonline.com</p>
CLIENT_ID	<p>Specify the Client ID for authenticating to Azure AD and for generating the access token. The Client ID is generated while creating a new connected app for the connector. For more information, see Registering the Connector in the Azure Environment.</p> <p>Example: xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx</p>
CLIENT_SECRET	<p>Specify the secret of the Client ID for authenticating to Azure AD and for generating the access token. The CLIENT_SECRET is generated while creating a new Connected app for the connector. For more information, see Registering the Connector in the Azure Environment.</p>
Scope	<p>Specify this parameter if you want to invoke Microsoft Graph 2.0 APIs to enforce the least privilege model for the connector on Dynamics 365 Finance and Operations objects.</p> <p>Syntax: <code>https://<tenant_url>/default</code></p>

Parameter	Description
	If you do not specify a value for the parameter, Microsoft Graph 1.0 APIs are used.

Specifying Parameters for Reconciliation Operations

After defining the connection parameters, specify the following parameters for performing reconciliation:

Parameter	Description
USER_FILTER	<p>Specify the particular set of users to import. The options are:</p> <ul style="list-style-type: none"> • All: To import all employees and contractors. • Employees: To import only employees. • Contractors: To import only contractors. <div data-bbox="753 1312 1333 1793" style="background-color: #e6f2ff; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Do not change the filter from superset to subset. For example, if you import the users by specifying the ALL option and then change the option to Employees then the</p> </div>

Parameter	Description
	<p>contactors will be deactivated.</p>
<p>USER_IMPORT_MAPPING</p>	<p>Specify the mapping of users to import into EIC in the following format:</p> <div data-bbox="753 646 1333 1461" style="background-color: #e6f2ff; padding: 10px; border: 1px solid #d9e1f2;"> <p> Note</p> <p>The DimensionDisplayValue attribute contains information about the Business Unit (OrgUnit) and Cost Cente configured in Microsoft Dynamics 365. You can configure the DimensionDisplayValue format by raising a ticket in Freshdesk to contact the Saviynt Support team.</p> </div> <p>JSON</p> <pre data-bbox="753 1514 1333 1892"> { "DimensionalDisplayValue_Delimiter": "-", "city": "AddressCity~#~char" , "country": "AddressCountryRegionISOCode~#~char", </pre>

Parameter	Description
	<pre> "costcenter": "DimensionDisplayValue[2]~#~char", "createdate": "OriginalHireDateTime~#~char", "displayname": "Name~#~char", , "email": "PrimaryContactEmail~#~char", "employeetype": "WorkerType~#~char", "employeeid": "PersonnelNumber~#~char", "enddate": "EmploymentEndDate~#~char", "firstname": "FirstName~#~char", "lastname": "LastName~#~char", , "locationnumber": "OfficeLocationId~#~char", "location": "OfficeLocation~#~char", "middlename": "PhoneticMiddleName~#~char", "orgunitid": "DimensionDisplayValue[1]~#~char", "phonenumber": "PrimaryContactPhone~#~char", "preferredFirstName": "KnownAs~#~char", "regioncode": "AddressZipCode </pre>

Parameter	Description
	<pre>e~#~char", "startdate": "EmploymentStar tDate~#~char", "state": "AddressState~#~cha r", "statuskey": "IsDisabled~#~c har", "street": "AddressStreet~#~c har", "termdate": "TerminationDate ~#~date", "title": "TitleId~#~char", "username": "PersonnelNumber ~#~char", "customproperty1": "NameAlia s~#~char", "customproperty2": "Gender~# ~char", "customproperty3": "Personal Suffix~#~char", "customproperty4": "Dimensio nDisplayValue~#~char", "customproperty5": "StartDat e~#~date", "customproperty6": "Employe ntDetailsExpiration~#~char", "customproperty7": "Employe ntLegalEntityId~#~char", "customproperty8": "WorkerSt atus~#~char", "customproperty9": "PrimaryC</pre>

Parameter	Description
	<pre> ontactPhoneExtension~#~char", "customproperty10": "Primary ContactPhoneIsMobile~#~char", "customproperty11": "Primary ContactPhoneDescription~#~char ", "customproperty12": "Address CountryRegionId~#~char", "customproperty13": "Primary AddressLocation~#~char", "customproperty14": "Address LocationId~#~char", "customproperty15": "Primary ContactEmailDescription~#~char ", "customproperty16": "NativeL anguageId~#~char", "customproperty17": "WorksFr omHome~#~char", "customproperty18": "PartyNu mber~#~char", "customproperty19": "PartyTy pe~#~char", "customproperty20": "Contrac torVendorId~#~char" } </pre>
ACCOUNT_IMPORT_MAPPING	Specify the mapping of accounts to import into EIC in the following format:

Parameter	Description
	<p data-bbox="753 302 834 331">JSON</p> <pre data-bbox="753 344 1333 1843"> { "accountID": "UserID~#~char", "customproperty1": "Alias~#~char", "customproperty10": "Enabled~#~char", "customproperty45": "WorkflowLineItemNotificationFormat~#~char", "customproperty11": "DocumentHandlingActive~#~char", "customproperty12": "UserInfo_defaultPartition~#~char", "customproperty13": "GlobalListPageLinkMode~#~char", "customproperty14": "GlobalExcelExportMode~#~char", "customproperty15": "ShowAttachmentStatus~#~char", "customproperty16": "EventPopUpLinkDestination~#~char", "customproperty17": "NetworkDomain~#~char", "customproperty18": "Company~#~char", "customproperty19": "SqmGUID~#~char", "customproperty2": "Email~#~char", </pre>

Parameter	Description
	<pre> "customproperty20": "SendNotif icationsInEmail~#~char", "customproperty21": "Density~# ~char", "customproperty22": "DefaultCo untryRegion~#~char", "customproperty23": "SendAlert AsEmailMessage~#~char", "customproperty24": "SqmEnable d~#~char", "customproperty25": "GlobalExc elExportFilePath~#~char", "customproperty26": "Language~ #~char", "customproperty27": "EventPopU pDisplayWhen~#~char", "customproperty28": "EventPoll Frequency~#~char", "customproperty29": "EventWork flowShowPopup~#~char", "customproperty3": "EmailProvi derID~#~char", "customproperty30": "StartPage ~#~char", "customproperty31": "Preferred TimeZone~#~char", "customproperty32": "HomePageR efreshDuration~#~char", "customproperty33": "UserInfo_ language~#~char", "customproperty34": "AutoLogOf </pre>

Parameter	Description
	<pre> f~#~char", "customproperty35": "Theme~#~c har", "customproperty36": "MarkEmpty Links~#~char", "customproperty37": "Enabled~# ~char", "customproperty38": "ShowNotificationsInTheMicroso ftDynamicsAX7Client~#~char", "customproperty39": "Helplangu age~#~char", "customproperty4": "PersonName ~#~char", "customproperty40": "EventPopU ps~#~char", "customproperty41": "Preferred Calendar~#~char", "customproperty42": "Preferred Locale~#~char", "customproperty43": "ExternalU ser~#~char", "customproperty44": "Automatic UrlUpdate~#~char", "displayname": "UserName~#~cha r", "name": "UserName~#~char" } </pre>

Parameter	Description
<p>ORGANIZATION_FILTER</p>	<p>Specify the filter to use as search criteria for organizations managed by the target application. By default, the connector searches the following organizations: LegalEntities, OperatingUnits, Departments, BusinessUnits, and CostCenters.</p>
<p>STATUS_THRESHOLD_CONFIG</p>	<p>Specify this parameter if you want to read the status of an account in the target application and update the same status for that account in EIC. An account can have one of the following statuses at one time:</p> <ul style="list-style-type: none"> • Active • Inactive • Suspended from import service. <p>The default value of the parameter is:</p> <p>JSON</p> <pre data-bbox="753 1419 1333 1845"> { "statusAndThresholdConfig": { "statusColumn": "customproperty37", "activeStatus": ["true"], "deleteLinks": true, </pre>

Parameter	Description
	<pre data-bbox="755 294 1323 661"> "accountThresholdValue": 1000, "correlateInactiveAccounts": f alse, "inactivateAccountsNotInFile" : false } } </pre>

Specifying Parameters for Provisioning Operations

After defining the connection parameters, specify the following parameters for performing provisioning and de-provisioning operations via the REST connection:

Parameters	Description
CreateAccountJSON	<p data-bbox="597 1066 1284 1199">Specify this parameter for creating a new account in EIC by mapping the request action and response for Create Account tasks in the following format:</p> <p data-bbox="597 1255 678 1283">JSON</p> <pre data-bbox="600 1297 1323 1879"> { "accountIdPath": "call1.message.User ID", "responseColsToPropsMap": { "displayname": "call1.message.User ID~#~char" }, "call": [{ "name": "call1", "connection": "userAuth", </pre>

Parameters	Description
	<pre> "url": "https://acme.cloudax.dynamics.com/Data/SystemUsers", "httpMethod": "POST", "httpParams": "{\"UserID\":\"\${user.username}\",\"NetworkDomain\":\"https://sts.windows.net/acme.onmicrosoft.com\", \"Company\":\"\${user.customproperty18}\", \"Alias\":\"\${user.customproperty1}\", \"DefaultCountryRegion\":\"\${user.customproperty22}\", \"SqmEnabled\":\"\${user.customproperty24}\", \"StartPage\":\"\${user.customproperty30}\", \"PreferredTimeZone\":\"\${user.customproperty31}\", \"HomePageRefreshDuration\":\"\${user.customproperty32}\", \"UserInfo_language\":\"\${user.customproperty33}\", \"Enabled\":true, \"UserName\":\"\${user.username}\", \"AccountType\":\"ClaimsUser\", \"ExternalUser\":false, \"HlpLanguage\":\"en-us\"}", "httpHeaders": { "Authorization": "\${access_token}", "Accept": "application/json", "OData-Version": "4.0" }, "httpContentType": "application/json" </pre>

Parameters	Description
	<pre data-bbox="602 296 1333 415">] }</pre>
<p data-bbox="240 489 526 525">UpdateAccountJSON</p>	<p data-bbox="602 489 1328 575">Specify this parameter for updating an existing account in EIC in the following format:</p> <p data-bbox="602 625 678 657">JSON</p> <pre data-bbox="602 674 1333 1864">{ "call": [{ "name": "call1", "connection": "userAuth", "url": "https://acme.cloudax.dynamics.com/Data/SystemUsers (UserID='\${account.accountID}')", "httpMethod": "PATCH", "httpParams": "{\"Alias\":\"\${user.email}\"", "httpHeaders": { "Authorization": "\${access_token}", "Accept": "application/json", "OData-Version": "4.0" }, "httpContentType": "application/json", "successResponses": { "statusCode": [200, 201, </pre>

Parameters	Description
	<pre data-bbox="602 289 1328 619"> 204] } }] } </pre>
<p data-bbox="240 695 521 726">EnableAccountJSON</p>	<p data-bbox="597 695 1321 932">Specify this parameter for enabling a disabled account on the target application. The connector uses the values specified for this parameter to check the attributes associated with the disabled account before enabling it.</p> <p data-bbox="597 984 1203 1016">Specify this parameter in the following format:</p> <p data-bbox="597 1068 678 1100">JSON</p> <pre data-bbox="602 1115 1328 1850"> { "call": [{ "name": "call1", "connection": "userAuth", "url": "https://acme.cloudax.dynamics.com/Data/SystemUsers (UserID='\${account.accountID}')", "httpMethod": "PATCH", "httpParams": "{\"Enabled\":true}", "httpHeaders": { "Authorization": "\${access_token}" } }] } </pre>

Parameters	Description
	<pre data-bbox="600 294 1323 1081"> "Accept": "application/json", "OData-Version": "4.0" }, "httpContentType": "application/ json", "successResponses": { "statusCode": [200, 201, 204] }] } </pre>
<p data-bbox="235 1155 527 1186">DisableAccountJSON</p>	<p data-bbox="592 1155 1323 1396">Specify this parameter for disabling an account on the target application and then updating that status in EIC. The connector uses the values specified for this parameter to check the attributes associated with the account before disabling it.</p> <p data-bbox="592 1407 1242 1438">Following is the default format of this parameter:</p> <p data-bbox="592 1491 682 1522">JSON</p> <pre data-bbox="600 1543 1323 1858"> { "call": [{ "name": "call1", "connection": "userAuth", "url": "https://acme.cloudax.dynamics. </pre>

Parameters	Description
	<pre> com/Data/SystemUsers (UserID='\${account .accountID}')", "httpMethod": "PATCH", "httpParams": {"Enabled":false}", "httpHeaders": { "Authorization": "\${access_token}", "Accept": "application/json", "OData-Version": "4.0" }, "httpContentType": "application/json", "successResponses": { "statusCode": [200, 201, 204] }] } </pre>
<p>AddAccessJSON</p>	<p>Specify this parameter to add access to an account in the following format:</p> <p>JSON</p> <pre> { "call": [{ "name": "Roles", "connection": "userAuth", </pre>

Parameters	Description
	<pre> "url": "https://acme.cloudax.dynamics.com/Data/SecurityUserRoles", "httpMethod": "POST", "httpParams": {"UserId":"\${account.accountID}","SecurityRoleIdentifier":"\${entitlementValue.entitlementID}","SecurityRoleName":"\${entitlementValue.entitlement_value}","AssignmentStatus": "Enabled","AssignmentMode": "Manual","UserLicenseType": "Activity"}", "httpHeaders": { "Authorization": "\${access_token}", "Accept": "application/json", "OData-Version": "4.0" }, "httpContentType": "application/json", "unsuccessResponses": { "statusCode": [400,401] }, "successResponses": {"statusCode": [200,201,204]} }, { "name": "Organization", "connection": "userAuth", "url": "https://acme.cloudax.dynamics.com/Data/SecurityUserRoles", "httpMethod": "POST", "httpParams": {"UserId":"\${account.accountID}","SecurityRoleIdentifier":"\${entitlementValue.entitlementID}","SecurityRoleName":"\${entitlementValue.entitlement_value}","AssignmentStatus": "E </pre>

Parameters	Description
	<pre> nabled", "AssignmentMode": "Manual", "UserLicenseType": "Activity"}", "httpHeaders": { "Authorization": "\${access_token}", "Accept": "application/json", "OData-Version": "4.0" }, "httpContentType": "application/json", "unsuccessResponses": { "statusCode": [400,401] }, "successResponses": {"statusCode": [200,201,204]} }] } </pre>
<p>RemoveAccessJSON</p>	<p>Specify this parameter if you want to remove access to an account in the following format:</p> <p>JSON</p> <pre> { "call": [{ "name": "Roles", "connection": "userAuth", "url": "https://acme.cloudax.dynamics.com/Data/SecurityUserRoles (UserId='\${account.accountID}', SecurityRoleIdentifier='\${entitlementValue.entitlementID}')", "httpMethod": "DELETE", </pre>

Parameters	Description
	<pre data-bbox="602 296 1330 919"> "headers": { "Authorization": "\${access_token}", "Accept": "application/json", "OData-Version": "4.0" }, "httpContentType": "application/json", "OData-Version": "4.0" }, "httpContent Type": "application/json", "unsuccessR esponses": { "statusCode": [400,401] } , "successResponses": {"statusCode": [200,201,204]} }] </pre>
<p data-bbox="240 1003 537 1035">RemoveAccountJSON</p>	<p data-bbox="602 1003 1235 1087">Specify this parameter if you want to remove the account in the following format:</p> <p data-bbox="602 1140 678 1171">JSON</p> <pre data-bbox="602 1182 1330 1864"> { "call": [{ "name": "call1", "connection": "userAuth", "url": "https://acme.cloudax.dyn amics.com/Data/SystemUsers (UserID='\${a ccount.accountID}')", "httpMethod": "DELETE", "headers": { "Authorization": "\${access_tok en}", "Accept": "application/json", </pre>

Parameters	Description
	<pre data-bbox="602 296 1328 871"> "OData-Version": "4.0" }, "httpContentType": "application/ json", "unsuccessResponses": { "statu sCode": [400,401] }, "successResponses": {"statusCo de": [200,201,204]} }] } </pre>



Note

The connector uses default values for importing users or accounts unless the mapping details to perform a filtered import are specified.

Creating a Security System

For more information about creating a security system, see [Creating A Security System](#) in the *Enterprise Identity Cloud Administration Guide*.

Creating an Endpoint for the Security System

For more information, see [Creating Endpoints](#) in the *Enterprise Identity Cloud Administration Guide*.

Using the Microsoft Dynamics 365 Connector

You can use the connector for performing import and provisioning operations after configuring it to meet your requirements.

Importing Users

For importing users into EIC, you must define the **UserImport** job and specify the parameters applicable to this connector. The imported users are stored in the user table in EIC. For more information, see [Importing Users using UserImportJob](#) in the *Enterprise Identity Cloud Administration Guide*.



Note

Currently the connector supports only full import of users.

Importing Accounts and Accesses

You must import accounts after the users are available in EIC. The accounts are imported using the **Application Data Import** job. Ensure that you define the parameters applicable to this connector. For more information, see [Uploading Entitlements using Other Connection and Application Data Import Job](#) in the *Enterprise Identity Cloud Administration Guide*.

Performing Provisioning Operations

Provisioning involves using EIC to create new accounts, update, remove, or delete accounts, enable or disable accounts, add or remove access for a role, and assign organizations for roles. EIC provides various types of rules that help you to automate

the provisioning actions including assigning access, revoking access, and providing birthright access.

Provisioning is automatically enabled when a connection is configured. EIC supports request-based provisioning operations that involve both end-users and approvers where end-users make requests and approvers approve or reject those requests. Typically, approvers belong to the management hierarchy in the organization. EIC follows a request-based provisioning operation, where the end-user raises or creates a request for provisioning a target system account. This request is then approved by the approver. For detailed information about provisioning, see [Manage your accesses](#) in the *Enterprise Identity Cloud Administration Guide*.

Troubleshooting

To troubleshoot common problems or obtain answers for frequently asked questions for connectors, see the [Common Troubleshooting Guide for Connectors](#).