Azure Active Directory

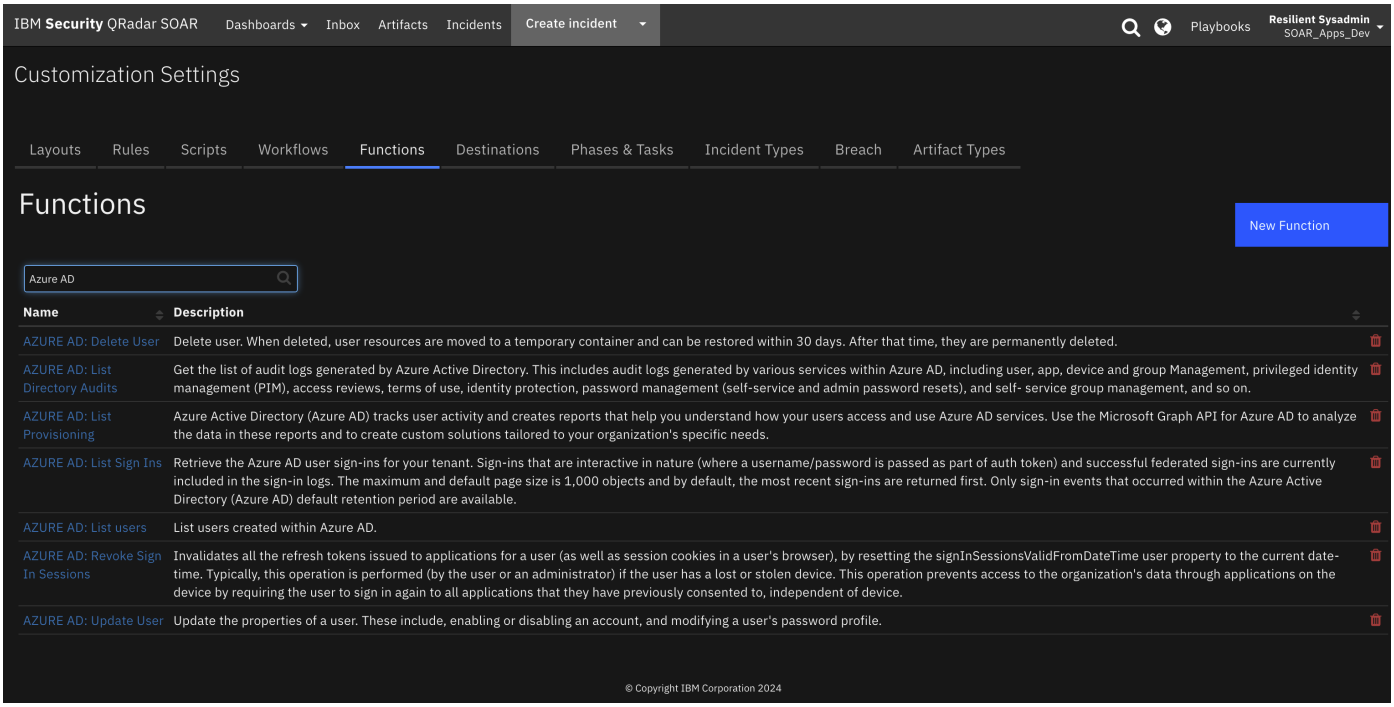
Table of Contents

Release Notes

Version	Date	Notes
1.1.1	01/2024	Fix bug that causes error when installing on SOAR.
1.1.0	12/2023	Converted Rules/Workflows to Playbooks
1.0.0	11/2021	Initial Release

Overview

SOAR Components for Azure Active Directory



Integration with Azure Active Directory to facilitate manual enrichment and targeted remediation actions.

```
Teams can investigate an attack by searching for Azure AD user accounts across Microsoft cloud, investigate actions
and sign ins performed by users and quickly respond to attacks by executing remediation actions, such as removing or
deactivating login profiles for suspicious accounts from within the SOAR platform.
```

Key Features

You can execute the following types of queries:

- Get a list of users and filter the list by display name, user id, account status

You can also fetch reports of users' activities

- Get sign in reports
- Get provisioning reports
- Get directory audit reports

You can also use the integration to make the following changes to an Azure AD environment:

- Update user account including modifying the password, disabling the account, and forcing the user to change their password on next sign in
- Delete a user account

Requirements

This app supports the IBM Security QRadar SOAR Platform and the IBM Security QRadar SOAR for IBM Cloud Pak for Security.

SOAR platform

The SOAR platform supports two app deployment mechanisms, Edge Gateway (formerly App Host) and integration server.

If deploying to a SOAR platform with an Edge Gateway, the requirements are:

- SOAR platform >= `46.0.0`.
- The app is in a container-based format (available from the AppExchange as a `zip` file).

If deploying to a SOAR platform with an integration server, the requirements are:

- SOAR platform >= `46.0.0`.
- The app is in the older integration format (available from the AppExchange as a `zip` file which contains a `tar.gz` file).
- Integration server is running `resilient-circuits>=46.0.0`.
- If using an API key account, make sure the account provides the following minimum permissions:

Name	Permissions
Org Data	Read
Function	Read
layout	Read, Edit

The following SOAR platform guides provide additional information:

- *Edge Gateway Deployment Guide* or *App Host Deployment Guide*: provides installation, configuration, and troubleshooting information, including proxy server settings.
- *Integration Server Guide*: provides installation, configuration, and troubleshooting information, including proxy server settings.
- *System Administrator Guide*: provides the procedure to install, configure and deploy apps.

The above guides are available on the IBM Documentation website at ibm.biz/soar-docs. On this web page, select your SOAR platform version. On the follow-on page, you can find the *Edge Gateway Deployment Guide*, *App Host Deployment Guide*, or *Integration Server Guide* by expanding **Apps** in the Table of Contents pane. The System Administrator Guide is available by expanding **System Administrator**.

Cloud Pak for Security

If you are deploying to IBM Cloud Pak for Security, the requirements are:

- IBM Cloud Pak for Security >= `1.8`.
- Cloud Pak is configured with an Edge Gateway.
- The app is in a container-based format (available from the AppExchange as a `zip` file).

The following Cloud Pak guides provide additional information:

- *Edge Gateway Deployment Guide* or *App Host Deployment Guide*: provides installation, configuration, and troubleshooting information, including proxy server settings. From the Table of Contents, select Case Management and Orchestration & Automation > **Orchestration and Automation Apps**.
- *System Administrator Guide*: provides information to install, configure, and deploy apps. From the IBM Cloud Pak for Security IBM Documentation table of contents, select Case Management and Orchestration & Automation > **System administrator**.

These guides are available on the IBM Documentation website at ibm.biz/cp4s-docs. From this web page, select your IBM Cloud Pak for Security version. From the version-specific IBM Documentation page, select Case Management and Orchestration & Automation.

Proxy Server

The app **does not** support a proxy server.

Python Environment

Python 3.6 and Python 3.9 are supported. Additional package dependencies may exist for each of these packages:

- azure-identity
- msgraph-core
- resilient-circuits>=46.0.0
- resilient-lib>=46.0.0

Installation

Install

- To install or uninstall an App or Integration on the *SOAR platform*, see the documentation at ibm.biz/soar-docs.
- To install or uninstall an App on *IBM Cloud Pak for Security*, see the documentation at ibm.biz/cp4s-docs and follow the instructions above to navigate to Orchestration and Automation.

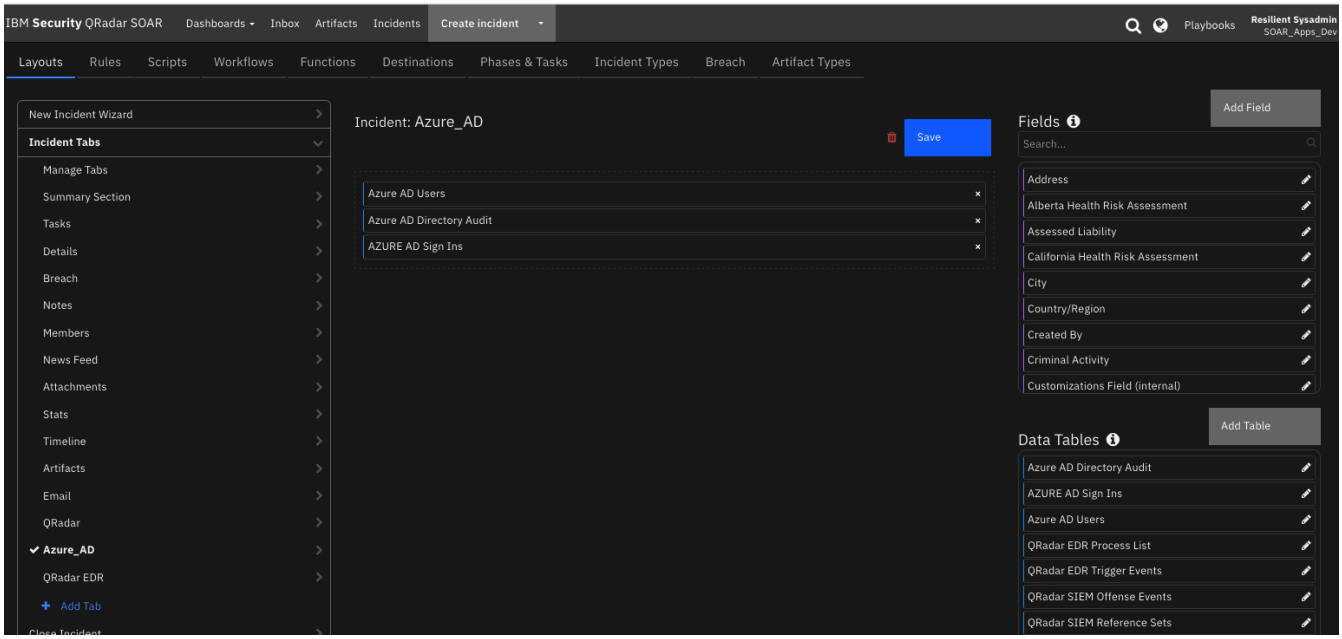
App Configuration

The following table provides the settings you need to configure the app. These settings are made in the app.config file. See the documentation discussed in the Requirements section for the procedure.

Config	Required	Example	Description
azure_ad_client_id	Yes	`<AZURE_AD_CLIENT_ID>`	*The client id for the registered application in Azure AD.*
azure_ad_client_secret	Yes	`<AZURE_AD_CLIENT_SECRET>`	*The client secret for the registered application in Azure AD.*
azure_ad_tenant_id	Yes	`<AZURE_AD_TENANT_ID>`	*The tenant id corresponding to the registered application in Azure AD.*

Custom Layouts

- Import the Data Tables and Custom Fields like the screenshot below:



Azure Active Directory Requirements

- Register an application in Azure Active Directory
- Get the Tenant id, Client id and the Client secret corresponding to the application and reference that in your app configuration
- Configure the following API Permissions for the Application

API / Permissions name	Type	Description
AuditLog.Read.All	Application	`Read all audit log data`
User.ReadWrite.All	Application	`Read all audit log data`

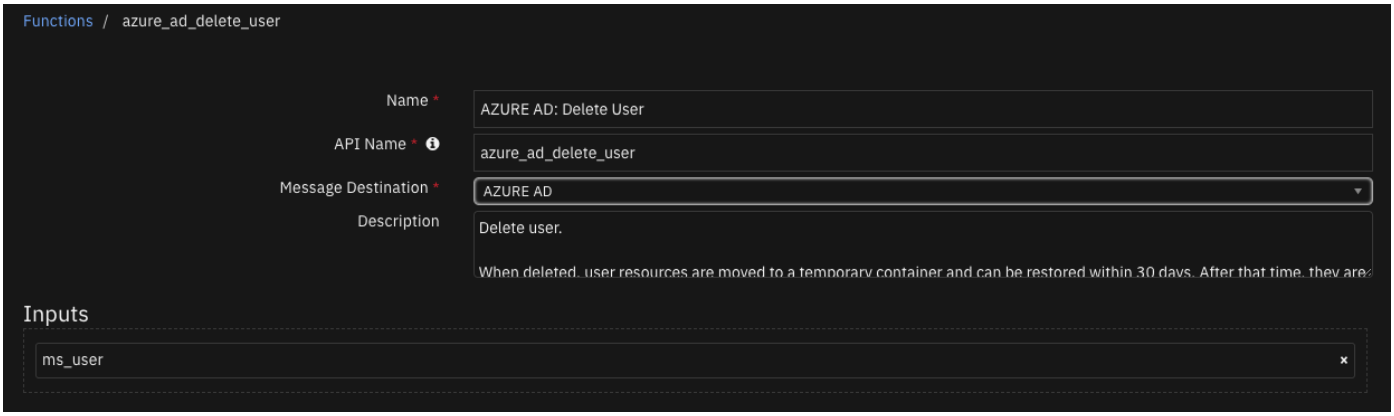
After adding the required permissions, click on `Grant admin consent for default directory` in the API Permissions section.

- Make sure you have assigned `User Administrator` or `Global Administrator` role to the application (whose client ID you have specified in the app config) by using below steps. If this is not done, you are expected to get "Insufficient privileges" error for all user related functions.
  - Navigate to Azure Portal > Azure AD > Roles and administrators > User Administrator > Click on Add Assignments > select the application > click on Add button.
- Licenses for activity reports

Function - AZURE AD: Delete User

Delete user.

When deleted, user resources are moved to a temporary container and can be restored within 30 days. After that time, they are permanently deleted.



▶ Inputs:

Name	Type	Required	Example	Tooltip
`ms_user`	`text`	Yes	`f5eee87c-dc98-4797-861f-5d1755088669 or someuser@contoso.com`	User ID or User Principal Name

▶ Outputs:

> **NOTE:** This example might be in JSON format, but `results` is a Python Dictionary on the SOAR platform.

```
results = {
  'version': '1.0',
  'success': True,
  'reason': None,
  'content': {
    'status': 'ok'
  },
  'raw': '{"status": "ok"}',
  'inputs': {
    'ms_user_id': 'abc-123'
  },
  'metrics': {
    'version': '1.0',
    'package': 'azure-ad',
    'package_version': '1.0.0',
    'host': 'local',
    'execution_time_ms': 7,
    'timestamp': '2021-10-23 04:11:27'
  }
}
```

▶ Example Function Input Script:

```
inputs.ms_user = row.azure_ad_user_user_principal_name
```

▶ Example Function Post Process Script:

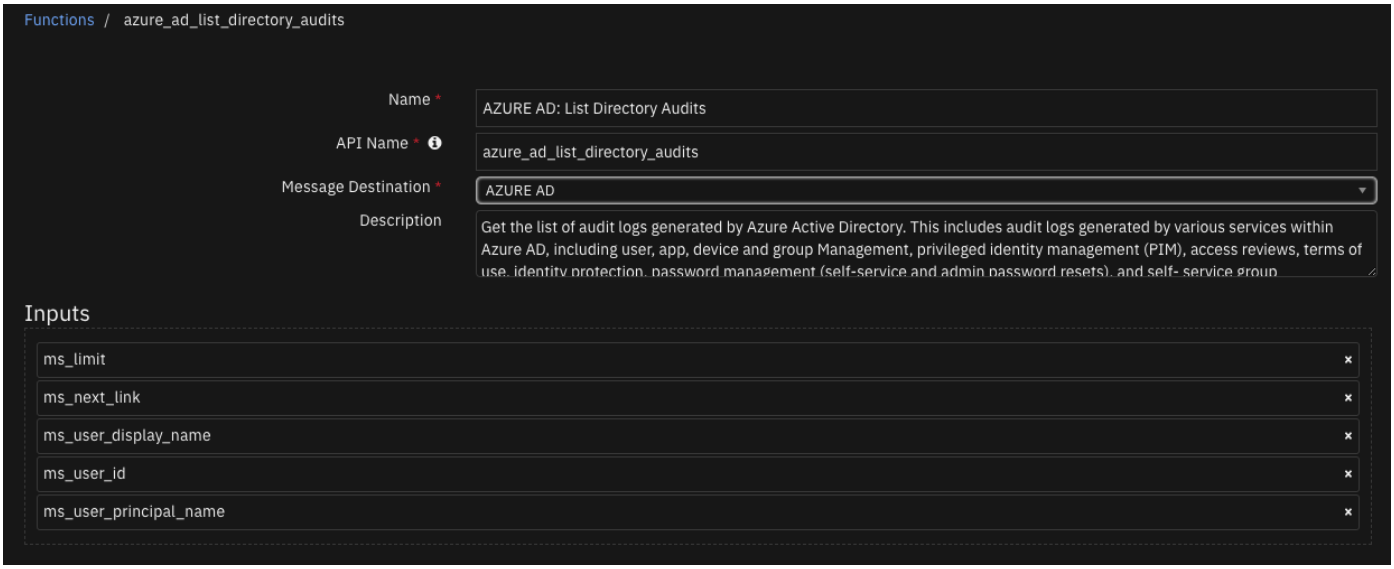
```
results = playbook.functions.results.azure_ad_delete_user_results
note = u"""User ID: {}
User Principal Name: {}
User Display Name: {}
User Given Name: {}
User Job Title: {}
```

```
User Mail: {}
User Mobile Phone: {}
User Surname: {}
""".format(row.azure_ad_user_id, row.azure_ad_user_user_principal_name, row.azure_ad_user_display_name,
row.azure_ad_user_given_name,
    row.azure_ad_user_job_title, row.azure_ad_user_mail,
    row.azure_ad_user_mobile_phone, row.azure_ad_user_surname)
if results.get("success"):
    incident.addNote(u"Successful delete\n{}".format(note))
    row.azure_ad_user_id = "-deleted-"
    row.azure_ad_user_user_principal_name = "-deleted-"
    row.azure_ad_user_display_name = "-deleted-"
    row.azure_ad_user_given_name = "-deleted-"
    row.azure_ad_user_job_title = "-deleted-"
    row.azure_ad_user_mail = "-deleted-"
    row.azure_ad_user_mobile_phone = "-deleted-"
    row.azure_ad_user_surname =  "-deleted-"

else:
    incident.addNote(u"Failure to delete item: {}\n{}".format(results.get("reason"), note))
```

Function - AZURE AD: List Directory Audits

Get the list of audit logs generated by Azure Active Directory. This includes audit logs generated by various services within Azure AD, including user, app, device and group Management, privileged identity management (PIM), access reviews, terms of use, identity protection, password management (self-service and admin password resets), and self- service group management, and so on.



▶ Inputs:

Name	Type	Required	Example
ms_limit	number	Yes	10
ms_next_link	text	No	https://graph.microsoft.com/v1.0/users?$top=2&$skiptoken=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAXkwNTAyZ21haWwub25taWNyb3Nv
ms_user_display_name	text	No	Test User

Name	Type	Required	Example
ms_user_id	text	No	f5eee87c-dc98-4797-861f-5d1755088669
ms_user_principal_name	text	No	someuser@contoso.com

▶ Outputs:

NOTE: This example might be in JSON format, but `results` is a Python Dictionary on the SOAR platform.


```
results = {
  'version': '1.0',
  'success': True,
  'reason': None,
  'content': {
    '@odata.context': 'https://graph.microsoft.com/v1.0/$metadata#auditLogs/directoryAudits',
    '@odata.nextLink': 'https://graph.microsoft.com/v1.0/auditLogs/directoryaudits?
$top=1&$filter=&$skiptoken=0ea5dc03b4b52debb0a07ad995024747_1',
    'value': [
      {
        'id': 'Directory_xxxxxxxx-cfc7-4cc5-964f-xxxxxxxxxxxx_J8EYS_395153735',
        'category': 'GroupManagement',
        'correlationId': 'bb14d1bd-cfc7-4cc5-964f-44cf462992fb',
        'result': 'success',
        'resultReason': '',
        'activityDisplayName': 'Add owner to group',
        'activityDateTime': '2021-10-20T06:43:17.8065708Z',
        'loggedByService': 'Core Directory',
        'operationType': 'Assign',
        'initiatedBy': {
          'app': None,
          'user': {
            'id': 'xxxxxxxx-08de-4311-aaa1-xxxxxxxxxxxx',
            'displayName': None,
            'userPrincipalName': 'TestU@xyz.onmicrosoft.com',
            'ipAddress': '20.190.145.169',
            'userType': None,
            'homeTenantId': None,
            'homeTenantName': None
          }
        },
        'targetResources': [
          {
            'id': 'xxxxxxxx-5eab-476d-84a0-xxxxxxxxxxxx',
            'displayName': None,
            'type': 'User',
            'userPrincipalName': 'TestU@xyz.onmicrosoft.com',
            'groupType': None,
            'modifiedProperties': [
              {
                'displayName': 'Group.ObjectID',
                'oldValue': None,
                'newValue': '"xxxxxxxx-dab4-4759-bc01-xxxxxxxxxxxx"'
              },
              {
                'displayName': 'Group.DisplayName',
                'oldValue': None,
                'newValue': '"Test Group 1"'
              },
              {
                'displayName': 'Group.WellKnownObjectName',
                'oldValue': None,
                'newValue': None
              }
            ]
          },
          {
            'id': 'xxxxxxxx-dab4-4759-bc01-xxxxxxxxxxxx',
            'displayName': None,
            'type': 'Group',
            'userPrincipalName': None,
            'groupType': 'unknownFutureValue',
            'modifiedProperties': [

            ]
          }
```

```
        ],
        'additionalDetails': [

        ]
      }
    ]
  },
  'raw': '{"@odata.context": "https://graph.microsoft.com/v1.0/$metadata#auditLogs/directoryAudits",
"@odata.nextLink": "https://graph.microsoft.com/v1.0/auditLogs/directoryaudits?
$top=1&$filter=&$skiptoken=0ea5dc03b4b52debb0a07ad995024747_1", "value": [{"id": "Directory_xxxxxxxx-cfc7-4cc5-964f-
xxxxxxxxxxxx_J8EYS_395153735", "category": "GroupManagement", "correlationId": "bb14d1bd-cfc7-4cc5-964f-
44cf462992fb", "result": "success", "resultReason": "", "activityDisplayName": "Add owner to group",
"activityDateTime": "2021-10-20T06:43:17.8065708Z", "loggedByService": "Core Directory", "operationType": "Assign",
"initiatedBy": {"app": null, "user": {"id": "xxxxxxxx-08de-4311-aaa1-xxxxxxxxxxxx", "displayName": null,
"userPrincipalName": "TestU@xyz.onmicrosoft.com", "ipAddress": "20.190.145.169", "userType": null, "homeTenantId":
null, "homeTenantName": null}}, "targetResources": [{"id": "xxxxxxxx-5eab-476d-84a0-xxxxxxxxxxxx", "displayName":
null, "type": "User", "userPrincipalName": "TestU@xyz.onmicrosoft.com", "groupType": null, "modifiedProperties":
[{"displayName": "Group.ObjectID", "oldValue": null, "newValue": "\\"xxxxxxxx-dab4-4759-bc01-xxxxxxxxxxxx\\""},
{"displayName": "Group.DisplayName", "oldValue": null, "newValue": "\\"Test Group 1\\""}, {"displayName":
"Group.WellKnownObjectName", "oldValue": null, "newValue": null}]}, {"id": "xxxxxxxx-dab4-4759-bc01-xxxxxxxxxxxx",
"displayName": null, "type": "Group", "userPrincipalName": null, "groupType": "unknownFutureValue",
"modifiedProperties": []}], "additionalDetails": []}]}',
  'inputs': {
    'ms_limit': 1
  },
  'metrics': {
    'version': '1.0',
    'package': 'azure-ad',
    'package_version': '1.0.0',
    'host': 'local',
    'execution_time_ms': 6,
    'timestamp': '2021-10-23 03:42:04'
  }
}
```


▶ Example Function Input Script:

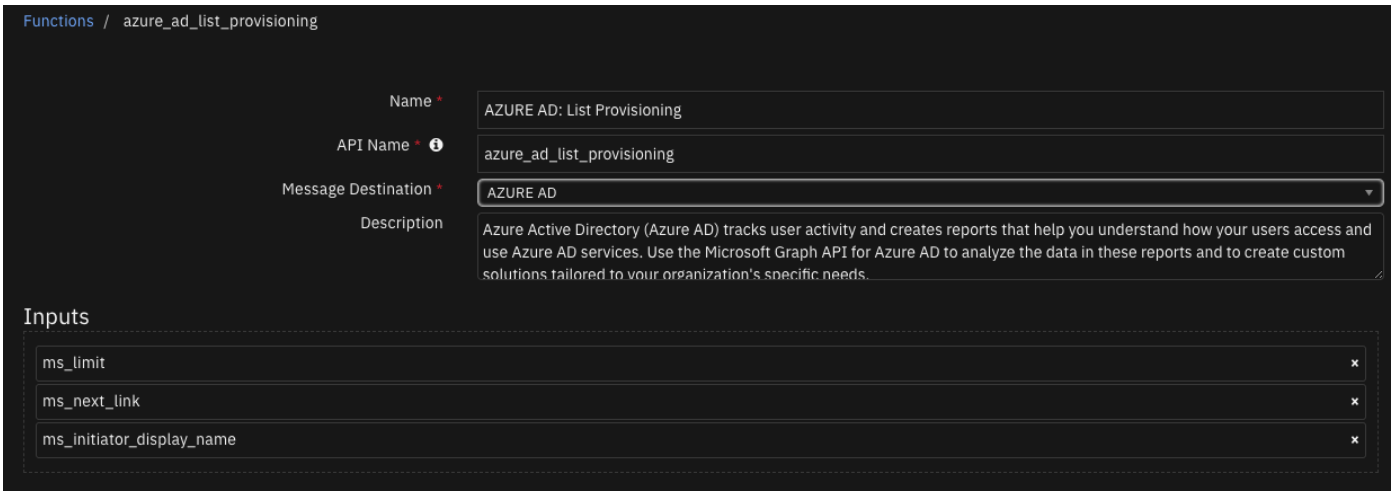
```
inputs.ms_limit = playbook.inputs.azure_ad_ms_limit
inputs.ms_next_link = getattr(playbook.inputs, "azure_ad_ms_next_link") or None
inputs.ms_user_display_name = getattr(playbook.inputs, "azure_ad_ms_user_display_name") or None
inputs.ms_user_id = getattr(playbook.inputs, "azure_ad_ms_user_id") or None
inputs.ms_user_principal_name = getattr(playbook.inputs, "azure_ad_ms_user_principal_name") or None
```

▶ Example Function Post Process Script:

```
from datetime import datetime
results=playbook.functions.results.azure_ad_list_directory_audit_result
current_time = datetime.now().strftime("%Y-%m-%d %H:%M:%S")
if results.get("success"):
  if results.get("content"):
    for user in results.get("content").get("value"):
      message_row = incident.addRow("azure_ad_directory_audit_dt")
      message_row.azure_ad_directory_audit_query_time = current_time
      message_row.azure_ad_id = user.get("id")
      message_row.azure_ad_category = user.get("category")
      message_row.azure_ad_result = user.get("result")
      message_row.azure_ad_result_reason = user.get("resultReason")
      message_row.azure_ad_activity_display_name = user.get("activityDisplayName")
      message_row.azure_ad_activity_date_time = user.get("activityDateTime")
      message_row.azure_ad_logged_by_service = user.get("loggedByService")
      message_row.azure_ad_operation_type = user.get("operationType")
    incident.addNote("AZURE AD: List Directory Audits: {} Active Directory Audits
queried".format(len(results.get("content").get("value"))))
  else:
    incident.addNote("No Active Directory Audit found")
else:
  incident.addNote("An error occurred getting Active Directory Audit: {}".format(results.get("reason")))
```

Function - AZURE AD: List Provisioning

Azure Active Directory (Azure AD) tracks user activity and creates reports that help you understand how your users access and use Azure AD services. Use the Microsoft Graph API for Azure AD to analyze the data in these reports and to create custom solutions tailored to your organization's specific needs.



▶ Inputs:

Name	Type	Required	Example
ms_initiator_display_name	text	No	Test User
ms_limit	number	Yes	10
ms_next_link	text	No	https://graph.microsoft.com/v1.0/users?$top=2&$skiptoken=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAXkwNTAyZ21haWwub25taWNyb

▶ Outputs:

> **NOTE:** This example might be in JSON format, but `results` is a Python Dictionary on the SOAR platform.

```
results = {
  'version': '1.0',
  'success': True,
  'reason': None,
  'content': {
    '@odata.context': 'https://graph.microsoft.com/v1.0/$metadata#auditLogs/provisioning',
    'value': [
      {
        'id': '75b5b0ae-9fc5-8d0e-e0a9-7y6a4728de56',
        'activityDateTime': '2019-05-04T03:00:54Z',
        'tenantId': '74beb175-3b80-7b63-b9d5-6f0b76082b16',
        'jobId': 'aws.74beb1753b704b63b8d56f0b76082b16.10a7a801-7101-4c69-ae00-ce9f75f8460a',
        'cycleId': 'b6502552-018d-79bd-8869-j47194dc65c1',
        'changeId': 'b6502552-018d-89bd-9969-b49194dc65c1',
        'provisioningAction': 'create',
        'durationInMilliseconds': 3236,
        'provisioningStatusInfo': {
          'status': 'success',
          'errorInformation': 'null'
        },
        'provisioningSteps': [
          {
            'name': 'EntryImport',
            'provisioningStepType': 'Import',
            'status': 'success',
```

```
            'description': "Retrieved RolesCompound '10a7a801-7101-4c69-ae00-ce9f75f8460a' from Contoso",
            'details': {

            }
          },
          {
            'name': 'EntryExportUpdate',
            'provisioningStepType': 'Export',
            'status': 'success',
            'description': "RolesCompound '60a7a801-7101-4c69-ae00-ce9f75f8460a' was updated in Azure Active
Directory",
            'details': {
              'ReportableIdentifier': '60a7a801-7101-4c69-ae00-ce9f75f8460a'
            }
          }
        ],
        'modifiedProperties': [
          {
            'displayName': 'appId',
            'oldValue': 'null',
            'newValue': '60a7a801-7101-4c69-ae00-ce9f75f8460a'
          },
          {
            'displayName': 'Roles',
            'oldValue': 'null',
            'newValue': 'jaws-prod-role2,jaws-prod-saml2, jayaws-role,jayaws-saml, TestRole,super-saml'
          },
          {
            'displayName': 'objectId',
            'oldValue': 'null',
            'newValue': '6nn37b93-185a-4485-a519-50c09549f3ad'
          },
          {
            'displayName': 'displayName',
            'oldValue': 'null',
            'newValue': 'Contoso'
          },
          {
            'displayName': 'homepage',
            'oldValue': 'null',
            'newValue': 'https://signin.contoso.com/saml?metadata=contoso|ISV9.1|primary|z'
          }
        ],
        'servicePrincipal': {
          'id': '6cc35b93-185a-4485-a519-50c09549g3ad',
          'displayName': 'Contoso'
        },
        'sourceSystem': {
          'id': 'd1e090e1-f2f4-4678-be44-6442ffff0621',
          'displayName': 'Contoso',
          'details': {

          }
        },
        'targetSystem': {
          'id': 'e69d4bd2-2da2-483e-bc49-aad4080b91b3',
          'displayName': 'Azure Active Directory',
          'details': {
            'ApplicationId': 'bcf4d658-ac9f-408d-bf04-e86dc10328fb',
            'ServicePrincipalId': '6nn35b93-185a-4485-a519-50c09549f3ad',
            'ServicePrincipalDisplayName': 'Contoso'
          }
        },
        'initiatedBy': {
          'initiatingType': 'system',
          'id': '',
          'displayName': 'Azure AD Provisioning Service'
        },
        'sourceIdentity': {
          'identityType': 'RolesCompound',
          'id': '60a7a801-7101-4c69-ae00-ce9f75f8460a',
          'displayName': '',
          'details': {

          }
        },
        'targetIdentity': {
          'identityType': 'ServicePrincipal',
          'id': '6nn35b93-185a-4485-a519-50c09549f3ad',
          'displayName': '',
          'details': {
```

```
          }
        }
      }
    ]
  },
  'raw': '{"@odata.context": "https://graph.microsoft.com/v1.0/$metadata#auditLogs/provisioning", "value": [{"id":
"75b5b0ae-9fc5-8d0e-e0a9-7y6a4728de56", "activityDateTime": "2019-05-04T03:00:54Z", "tenantId": "74beb175-3b80-7b63-
b9d5-6f0b76082b16", "jobId": "aws.74beb1753b704b63b8d56f0b76082b16.10a7a801-7101-4c69-ae00-ce9f75f8460a", "cycleId":
"b6502552-018d-79bd-8869-j47194dc65c1", "changeId": "b6502552-018d-89bd-9969-b49194dc65c1", "provisioningAction":
"create", "durationInMilliseconds": 3236, "provisioningStatusInfo": {"status": "success", "errorInformation":
"null"}, "provisioningSteps": [{"name": "EntryImport", "provisioningStepType": "Import", "status": "success",
"description": "Retrieved RolesCompound \'10a7a801-7101-4c69-ae00-ce9f75f8460a\' from Contoso", "details": {}},
{"name": "EntryExportUpdate", "provisioningStepType": "Export", "status": "success", "description": "RolesCompound
\'60a7a801-7101-4c69-ae00-ce9f75f8460a\' was updated in Azure Active Directory", "details": {"ReportableIdentifier":
"60a7a801-7101-4c69-ae00-ce9f75f8460a"}}], "modifiedProperties": [{"displayName": "appId", "oldValue": "null",
"newValue": "60a7a801-7101-4c69-ae00-ce9f75f8460a"}, {"displayName": "Roles", "oldValue": "null", "newValue": "jaws-
prod-role2,jaws-prod-saml2, jayaws-role,jayaws-saml, TestRole,super-saml"}, {"displayName": "objectId", "oldValue":
"null", "newValue": "6nn37b93-185a-4485-a519-50c09549f3ad"}, {"displayName": "displayName", "oldValue": "null",
"newValue": "Contoso"}, {"displayName": "homepage", "oldValue": "null", "newValue": "https://signin.contoso.com/saml?
metadata=contoso|ISV9.1|primary|z"}], "servicePrincipal": {"id": "6cc35b93-185a-4485-a519-50c09549g3ad",
"displayName": "Contoso"}, "sourceSystem": {"id": "d1e090e1-f2f4-4678-be44-6442ffff0621", "displayName": "Contoso",
"details": {}}, "targetSystem": {"id": "e69d4bd2-2da2-483e-bc49-aad4080b91b3", "displayName": "Azure Active
Directory", "details": {"ApplicationId": "bcf4d658-ac9f-408d-bf04-e86dc10328fb", "ServicePrincipalId": "6nn35b93-
185a-4485-a519-50c09549f3ad", "ServicePrincipalDisplayName": "Contoso"}}, "initiatedBy": {"initiatingType": "system",
"id": "", "displayName": "Azure AD Provisioning Service"}, "sourceIdentity": {"identityType": "RolesCompound", "id":
"60a7a801-7101-4c69-ae00-ce9f75f8460a", "displayName": "", "details": {}}, "targetIdentity": {"identityType":
"ServicePrincipal", "id": "6nn35b93-185a-4485-a519-50c09549f3ad", "displayName": "", "details": {}}}]}',
  'inputs': {
    'ms_limit': 1,
    'ms_initiator_display_name': 'test'
  },
  'metrics': {
    'version': '1.0',
    'package': 'azure-ad',
    'package_version': '1.0.0',
    'host': 'local',
    'execution_time_ms': 6,
    'timestamp': '2021-10-23 02:44:31'
  }
}
```


▶ Example Function Input Script:

```
None
```

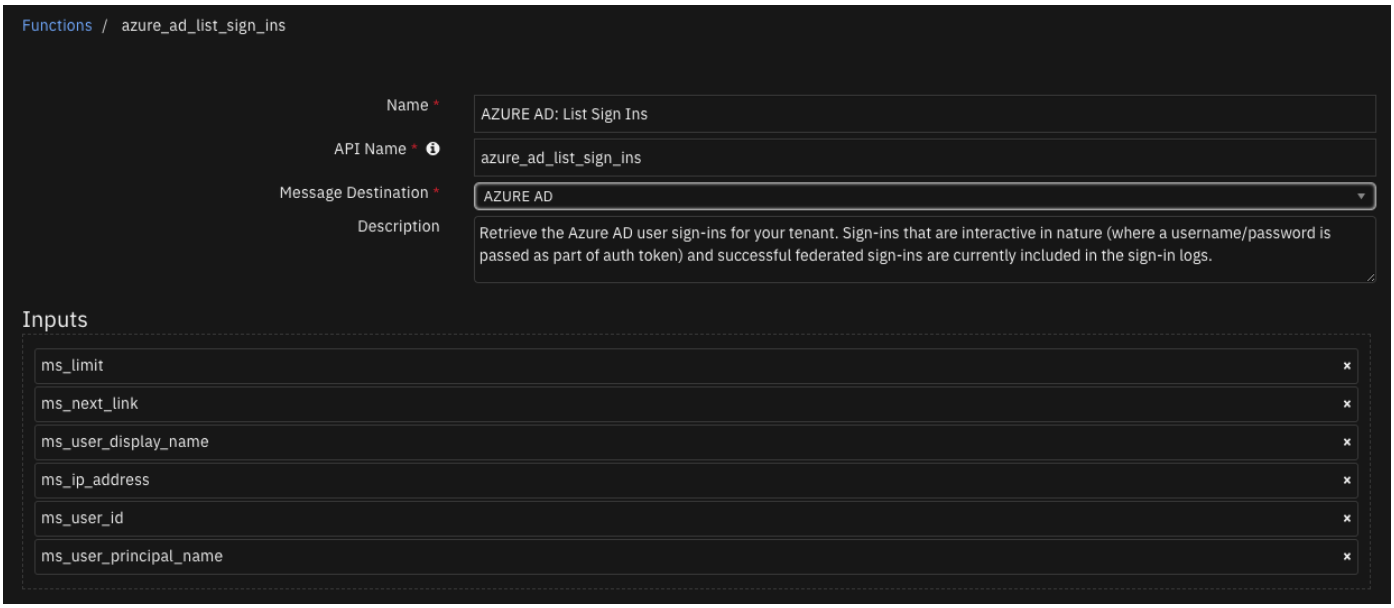
▶ Example Function Post Process Script:

```
None
```

Function - AZURE AD: List Sign Ins

Retrieve the Azure AD user sign-ins for your tenant. Sign-ins that are interactive in nature (where a username/password is passed as part of auth token) and successful federated sign-ins are currently included in the sign-in logs.

The maximum and default page size is 1,000 objects and by default, the most recent sign-ins are returned first. Only sign-in events that occurred within the Azure Active Directory (Azure AD) default retention period are available.



▶ Inputs:

Name	Type	Required	Example
ms_ip_address	text	No	45.129.28.55
ms_limit	number	Yes	10
ms_next_link	text	No	https://graph.microsoft.com/v1.0/users?$top=2&$skiptoken=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAXkwNTAyZ21haWwub25taWNyb3Nv
ms_user_display_name	text	No	Test User
ms_user_id	text	No	f5eee87c-dc98-4797-861f-5d1755088669
ms_user_principal_name	text	No	someuser@contoso.com

▶ Outputs:

> **NOTE:** This example might be in JSON format, but `results` is a Python Dictionary on the SOAR platform.

```
results = {
  'version': '1.0',
  'success': True,
  'reason': None,
  'content': {
    '@odata.context': 'https://graph.microsoft.com/v1.0/$metadata#auditLogs/signIns',
    'value': [
      {
        'id': '5eeb2156-xxxx-4410-8fb4-xxxxxxxxxxxx',
        'createdDateTime': '2021-10-15T06:51:40Z',
        'userDisplayName': 'Test User',
        'userPrincipalName': 'TestU@xyz.onmicrosoft.com',
```

```
        'userId': 'exists',
        'appId': 'xxxxxxxx-3bb0-49c1-b47d-xxxxxxxxxxxx',
        'appDisplayName': 'Azure Portal',
        'ipAddress': '1.2.3.4',
        'clientAppUsed': 'Browser',
        'correlationId': 'xxxxxxxx-d8a0-4e6c-a3b8-xxxxxxxxxxxx',
        'conditionalAccessStatus': 'notApplied',
        'isInteractive': True,
        'riskDetail': 'none',
        'riskLevelAggregated': 'none',
        'riskLevelDuringSignIn': 'none',
        'riskState': 'none',
        'riskEventTypes': [

        ],
        'riskEventTypes_v2': [

        ],
        'resourceDisplayName': 'Windows Azure Service Management API',
        'resourceId': 'xxxxxxxx-ba00-4fd7-ba43-xxxxxxxxxxxx',
        'status': {
          'errorCode': 0,
          'failureReason': 'Other.',
          'additionalDetails': None
        },
        'deviceDetail': {
          'deviceId': '',
          'displayName': '',
          'operatingSystem': 'MacOs',
          'browser': 'Chrome 94.0.4606',
          'isCompliant': False,
          'isManaged': False,
          'trustType': ''
        },
        'location': {
          'city': 'Kasthuribai Nagar (Tambaram)',
          'state': 'Tamil Nadu',
          'countryOrRegion': 'IN',
          'geoCoordinates': {
            'altitude': None,
            'latitude': 12.934,
            'longitude': 80.114
          }
        },
        'appliedConditionalAccessPolicies': [

        ]
      }
    ]
  },
  'raw': '{"@odata.context": "https://graph.microsoft.com/v1.0/$metadata#auditLogs/signIns", "value": [{"id":
"5eeb2156-xxxx-4410-8fb4-xxxxxxxxxxxx", "createdDateTime": "2021-10-15T06:51:40Z", "userDisplayName": "Test User",
"userPrincipalName": "TestU@xyz.onmicrosoft.com", "userId": "exists", "appId": "xxxxxxxx-3bb0-49c1-b47d-
xxxxxxxxxxxx", "appDisplayName": "Azure Portal", "ipAddress": "1.2.3.4", "clientAppUsed": "Browser", "correlationId":
"xxxxxxxx-d8a0-4e6c-a3b8-xxxxxxxxxxxx", "conditionalAccessStatus": "notApplied", "isInteractive": true, "riskDetail":
"none", "riskLevelAggregated": "none", "riskLevelDuringSignIn": "none", "riskState": "none", "riskEventTypes": [],
"riskEventTypes_v2": [], "resourceDisplayName": "Windows Azure Service Management API", "resourceId": "xxxxxxxx-ba00-
4fd7-ba43-xxxxxxxxxxxx", "status": {"errorCode": 0, "failureReason": "Other.", "additionalDetails": null},
"deviceDetail": {"deviceId": "", "displayName": "", "operatingSystem": "MacOs", "browser": "Chrome 94.0.4606",
"isCompliant": false, "isManaged": false, "trustType": ""}, "location": {"city": "Kasthuribai Nagar (Tambaram)",
"state": "Tamil Nadu", "countryOrRegion": "IN", "geoCoordinates": {"altitude": null, "latitude": 12.934, "longitude":
80.114}}, "appliedConditionalAccessPolicies": []}]}',
  'inputs': {
    'ms_limit': 1
  },
  'metrics': {
    'version': '1.0',
    'package': 'azure-ad',
    'package_version': '1.0.0',
    'host': 'local',
    'execution_time_ms': 6,
    'timestamp': '2021-10-23 03:23:27'
  }
}
```


▶ Example Function Input Script:

```
inputs.ms_limit = playbook.inputs.azure_ad_ms_limit
inputs.ms_next_link = getattr(playbook.inputs, "azure_ad_ms_next_link") or None
```

```
inputs.ms_user_display_name = getattr(playbook.inputs, "azure_ad_user_display_name") or None
inputs.ms_ip_address = getattr(playbook.inputs, "azure_ad_ms_ip_address_") or None
inputs.ms_user_id = getattr(playbook.inputs, "azure_ad_ms_user_id") or None
inputs.ms_user_principal_name = getattr(playbook.inputs, "azure_ad_ms_user_principal_name") or None
```

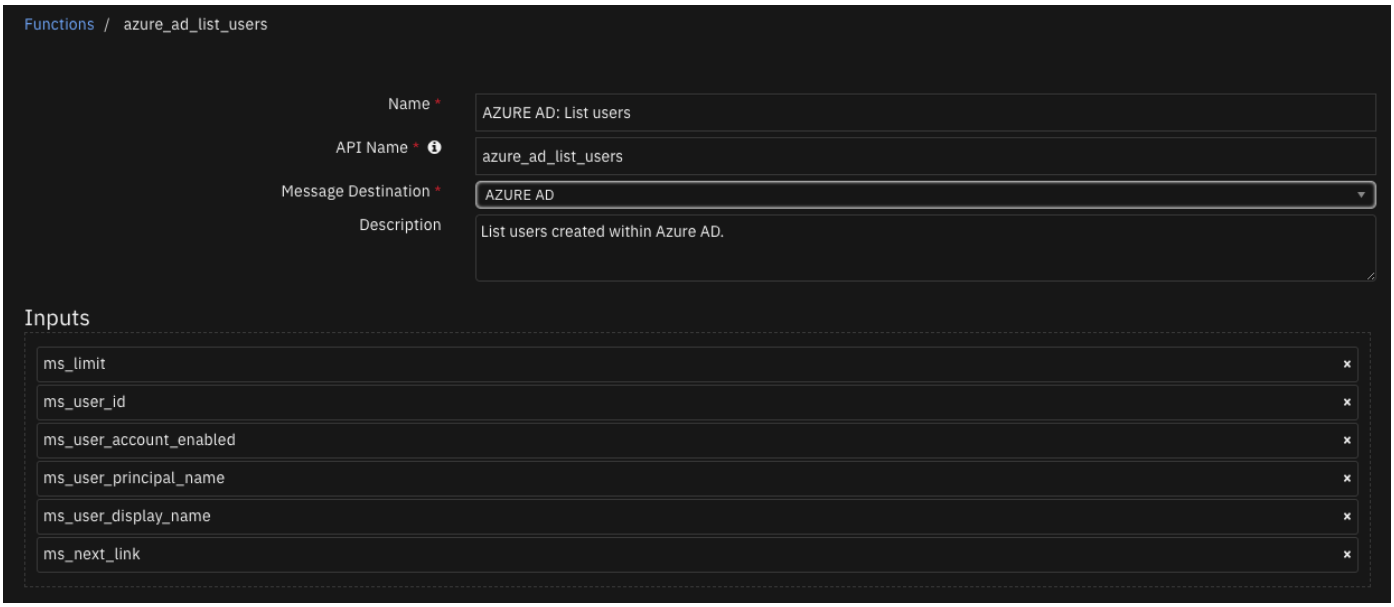
▶ Example Function Post Process Script:

```
from datetime import datetime
results=playbook.functions.results.azure_ad_list_sign_ins_result
current_time = datetime.now().strftime("%Y-%m-%d %H:%M:%S")

if results.get("success"):
  if results.get("content"):
    for user in results.get("content").get("value"):
      message_row = incident.addRow("azure_ad_sign_ins_dt")
      message_row.azure_ad_user_sign_in_query_time = current_time
      message_row.azure_ad_id = user.get("id")
      message_row.azure_ad_created_date_time = user.get("createdDateTime")
      message_row.azure_ad_user_display_name = user.get("userDisplayName")
      message_row.azure_ad_user_user_principal_name = user.get("userPrincipalName")
      message_row.azure_ad_user_id = user.get("userId")
      message_row.azure_ad_app_id = user.get("appId")
      message_row.azure_ad_app_display_name = user.get("appDisplayName")
      message_row.azure_ad_ip_address = user.get("ipAddress")
    incident.addNote("AZURE AD: List Sign Ins: {} Active Directory Sign ins
queried".format(len(results.get("content").get("value"))))
  else:
    incident.addNote("No Active Directory Sign in found")
else:
  incident.addNote("An error occurred getting Active Directory Sign in: {}".format(results.get("reason")))
```

Function - AZURE AD: List users

List users created within Azure AD.



▶ Inputs:

Name	Type	Required	Example
ms_limit	number	Yes	10

Name	Type	Required	Example
`ms_next_link`	`text`	No	`https://graph.microsoft.com/v1.0/users?$top=2&$skiptoken=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAXkwNTAyZ21haWwub25taWNyb3`
`ms_user_account_enabled`	`boolean`	No	`-`
`ms_user_display_name`	`text`	No	`Test User`
`ms_user_id`	`text`	No	`f5eee87c-dc98-4797-861f-5d1755088669`
`ms_user_principal_name`	`text`	No	`someuser@contoso.com`

▶ Outputs:

> **NOTE:** This example might be in JSON format, but `results` is a Python Dictionary on the SOAR platform.

```
results = {
  'version': '1.0',
  'success': True,
  'reason': None,
  'content': {
    '@odata.context': 'https://graph.microsoft.com/v1.0/$metadata#users',
    '@odata.nextLink': 'https://graph.microsoft.com/v1.0/users?
$top=2&$skiptoken=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA',
    'value': [
      {
        'businessPhones': [

        ],
        'displayName': 'Adele Vance',
        'givenName': None,
        'jobTitle': None,
        'mail': None,
        'mobilePhone': None,
        'officeLocation': None,
        'preferredLanguage': None,
        'surname': None,
        'userPrincipalName': 'AdeleV@xyz.onmicrosoft.com',
        'id': 'e0d56b1a-f5aa-4f7f-a84e-d4c44d65bf64'
      },
      {
        'businessPhones': [

        ],
        'displayName': 'Test User',
        'givenName': None,
        'jobTitle': None,
        'mail': None,
        'mobilePhone': None,
        'officeLocation': None,
        'preferredLanguage': None,
        'surname': None,
        'userPrincipalName': 'TestU@xyz.onmicrosoft.com',
        'id': '5f41d8e0-5eab-476d-84a0-94ee23977601'
```

```
      }
    ]
  },
  'raw': '{"@odata.context": "https://graph.microsoft.com/v1.0/$metadata#users", "@odata.nextLink":
"https://graph.microsoft.com/v1.0/users?
$top=2&$skiptoken=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA", "value": [{"businessPhones": [], "displayName": "Adele Vance",
"givenName": null, "jobTitle": null, "mail": null, "mobilePhone": null, "officeLocation": null, "preferredLanguage":
null, "surname": null, "userPrincipalName": "AdeleV@xyz.onmicrosoft.com", "id": "e0d56b1a-f5aa-4f7f-a84e-
d4c44d65bf64"}, {"businessPhones": [], "displayName": "Test User", "givenName": null, "jobTitle": null, "mail": null,
"mobilePhone": null, "officeLocation": null, "preferredLanguage": null, "surname": null, "userPrincipalName":
"TestU@xyz.onmicrosoft.com", "id": "5f41d8e0-5eab-476d-84a0-94ee23977601"}]}',
  'inputs': {
    'ms_limit': 2
  },
  'metrics': {
    'version': '1.0',
    'package': 'azure-ad',
    'package_version': '1.0.0',
    'host': 'local',
    'execution_time_ms': 5,
    'timestamp': '2021-10-23 03:46:39'
  }
}
```


▶ Example Function Input Script:

```
inputs.ms_limit = playbook.inputs.azure_ad_ms_limit
inputs.ms_next_link = getattr(playbook.inputs, "azure_ad_ms_next_link") or None
inputs.ms_user_account_enabled = getattr(playbook.inputs, "azure_ad_ms_user_account_enabled") or None
inputs.ms_user_id = getattr(playbook.inputs, "azure_ad_ms_user_id") or None
inputs.ms_user_display_name = getattr(playbook.inputs, "azure_ad_ms_user_display_name") or None
```

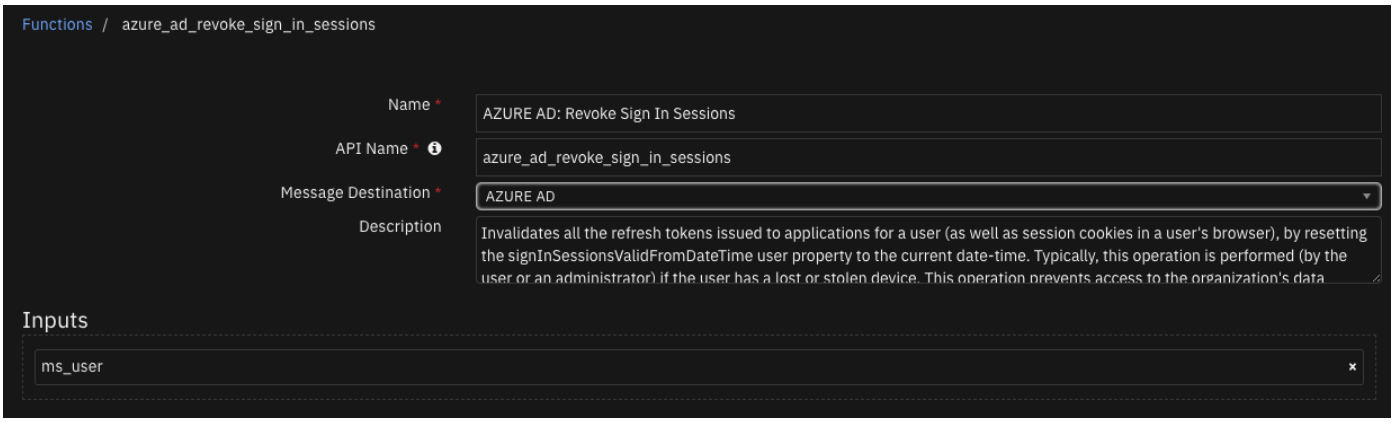
▶ Example Function Post Process Script:

```
from datetime import datetime
results=playbook.functions.results.azure_ad_list_users_results
current_time = datetime.now().strftime("%Y-%m-%d %H:%M:%S")

if results.get("success"):
  if results.get("content"):
    for user in results.get("content").get("value"):
      message_row = incident.addRow("azure_ad_users_dt")
      message_row.azure_ad_user_query_time = current_time
      message_row.azure_ad_user_id = user.get("id")
      message_row.azure_ad_user_user_principal_name = user.get("userPrincipalName")
      message_row.azure_ad_user_display_name = user.get("displayName")
      message_row.azure_ad_user_given_name = user.get("givenName")
      message_row.azure_ad_user_job_title = user.get("jobTitle")
      message_row.azure_ad_user_mail= user.get("mail")
      business_phones = ''
      for businessPhone in user.get("businessPhones"):
        business_phones = business_phones + businessPhone + "\n"
        message_row.azure_ad_business_phone = business_phones
      message_row.azure_ad_user_mobile_phone = user.get("mobilePhone")
      message_row.azure_ad_user_surname = user.get("surname")
    incident.addNote("AZURE AD: List Users in Active Directory: {} Active Directory Users have successfully been
queried".format(len(results.get("content").get("value"))))
  else:
    incident.addNote("No Active Directory User found")
else:
  incident.addNote("An error occurred getting Active Directory Users: {}".format(results.get("reason")))
```

Function - AZURE AD: Revoke Sign In Sessions

Invalidates all the refresh tokens issued to applications for a user (as well as session cookies in a user's browser), by resetting the signInSessionsValidFromDateTime user property to the current date-time. Typically, this operation is performed (by the user or an administrator) if the user has a lost or stolen device. This operation prevents access to the organization's data through applications on the device by requiring the user to sign in again to all applications that they have previously consented to, independent of device.



▶ Inputs:

Name	Type	Required	Example	Tooltip
ms_user	text	Yes	f5eee87c-dc98-4797-861f-5d1755088669 or someuser@contoso.com	User ID or User Principal Name

▶ Outputs:

> **NOTE:** This example might be in JSON format, but `results` is a Python Dictionary on the SOAR platform.

```
results = {
  'version': '1.0',
  'success': True,
  'reason': None,
  'content': {
    '@odata.context': 'https://graph.microsoft.com/v1.0/$metadata#Edm.Boolean',
    'value': True
  },
  'raw': '{"@odata.context": "https://graph.microsoft.com/v1.0/$metadata#Edm.Boolean", "value": true}',
  'inputs': {
    'ms_user_id': 'abc-123'
  },
  'metrics': {
    'version': '1.0',
    'package': 'azure-ad',
    'package_version': '1.0.0',
    'host': 'local',
    'execution_time_ms': 6,
    'timestamp': '2021-10-23 04:00:06'
  }
}
```

▶ Example Function Input Script:

```
inputs.ms_user = row.azure_ad_user_user_principal_name
```

▶ Example Function Post Process Script:

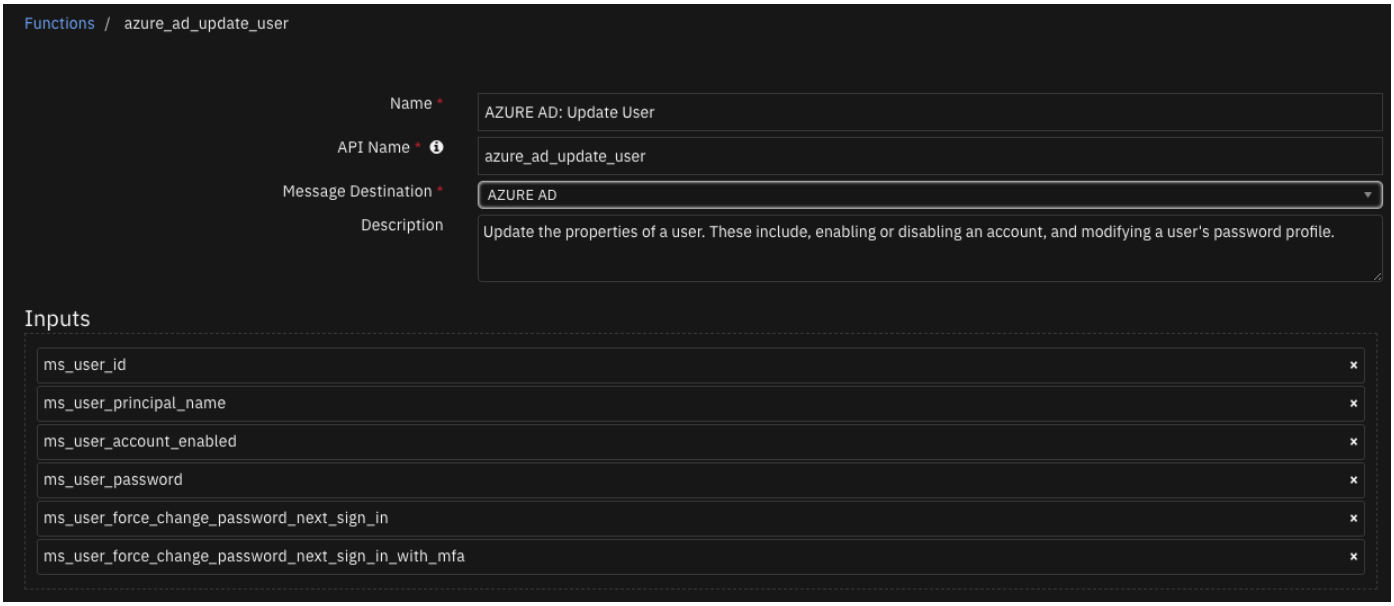
```
results = playbook.functions.results.azure_ad_revoke_sign_in_sessions_results
note = u"""User ID: {}
User Principal Name: {}
User Display Name: {}
User Create Date: {}
User ID: {}
User App ID: {}
User App Display Name: {}
User IP Address: {}
""".format(row.azure_ad_id, row.azure_ad_user_user_principal_name, row.azure_ad_user_display_name,
row.azure_ad_created_date_time,
    row.azure_ad_user_id, row.azure_ad_app_id, row.azure_ad_app_display_name,
    row.azure_ad_ip_address)
if results.get("success"):
    incident.addNote(u"Successful revoked\n{}".format(note))
    row.azure_ad_id = "-revoked-"
    row.azure_ad_user_user_principal_name = "-revoked-"
    row.azure_ad_created_date_time = "-revoked-"
    row.azure_ad_user_display_name = "-revoked-"
    row.azure_ad_user_id= "-revoked-"
    row.azure_ad_app_id = "-revoked-"
```

```
    row.azure_ad_app_display_name = "-revoked-"


else:
    incident.addNote(u"Failure to delete item: {}\n{}".format(results.get("reason"), note))
```

Function - AZURE AD: Update User

Update the properties of a user. These include, enabling or disabling an account, and modifying a user's password profile.



▶ Inputs:

Name	Type	Required	Example	Tooltip
ms_user	text	Yes	f5eee87c-dc98-4797-861f-5d1755088669 or someuser@contoso.com	User ID or User Principal Name
ms_user_account_enabled	boolean	No	-	true if the account is enabled; otherwise, false.
ms_user_force_change_password_next_sign_in	boolean	No	-	true if the user must change her password on the next login; otherwise false.
ms_user_force_change_password_next_sign_in_with_mfa	boolean	No	-	If true, at next sign-in, the user must perform a multi-factor authentication (MFA) before being forced to change their password. The behavior is identical to forceChangePasswordNextSignIn except that the user is required to first perform a multi-factor authentication before password change. After a password change, this property will be automatically reset to false.
ms_user_password	text	No	PZ;Bp[8n'^@"ERT^	Password

▶ Outputs:

> **NOTE:** This example might be in JSON format, but `results` is a Python Dictionary on the SOAR platform.

```
results = {
  'version': '1.0',
  'success': True,
  'reason': None,
  'content': {
    'status': 'ok'
  },
  'raw': '{"status": "ok"}',
```

```
    'inputs': {
      'ms_user_id': 'abc-123',
      'ms_user_account_enabled': False
    },
    'metrics': {
      'version': '1.0',
      'package': 'azure-ad',
      'package_version': '1.0.0',
      'host': 'local',
      'execution_time_ms': 12,
      'timestamp': '2021-10-23 04:07:20'
    }
  }
```

▶ Example Function Input Script:

```
inputs.ms_user = row.azure_ad_user_user_principal_name
inputs.ms_user_account_enabled = getattr(playbook.inputs, "ms_user_account_enabled")
inputs.ms_user_password = getattr(playbook.inputs, "azure_ad_ms_user_password")
inputs.ms_user_force_change_password_next_sign_in = getattr(playbook.inputs,
"azure_ad_ms_user_force_change_password")
inputs.ms_user_force_change_password_next_sign_in_with_mfa = getattr(playbook.inputs,
"azure_ad_ms_user_force_change_password_with_mfa")
```

▶ Example Function Post Process Script:

```
from datetime import datetime
results=playbook.functions.results.azure_ad_update_users_results
content = results.get("content")
note = u"""MS User: {}
User Account Enabled: {}
User Password: (password changed)
User Force Change Password: {}
User Force Change Password with MFA: {}""".format(row.azure_ad_user_user_principal_name,
                            getattr(playbook.inputs, "ms_user_account_enabled"),
                            getattr(playbook.inputs, "azure_ad_ms_user_force_change_password"),
                            getattr(playbook.inputs, "azure_ad_ms_user_force_change_password_with_mfa"))

if results.get("success"):
    incident.addNote(u"Successful updated the user password settings to the following\n{}".format(note))

else:
    incident.addNote(u"Failed to updated items: {}\n{}".format(results.get("reason"), note))
```

Data Table - Azure AD Directory Audit

ID	Category	Result	Result Reason	Activity Display Name	Activity Date Time	Logged By Service	Operation Type
Directory_9d64ebb2-6764-44d6-83ea-629570f05a7d_1HNB1_330894614	ApplicationManagement	success	–	Add service principal	2023-10-26T04:53:30.2175713Z	Core Directory	–
PIM_832ae5ce-ee9c-4bab-bbba-f6df1b710a92_G8YS5_2205118	RoleManagement	success	–	Remove permanent eligible role assignment	2023-10-25T20:52:33.1985122Z	PIM	–
PIM_832ae5ce-ee9c-4bab-bbba-f6df1b710a92_G8YS5_2204668	RoleManagement	success	–	Remove permanent direct role assignment	2023-10-25T20:52:32.9875123Z	PIM	–
PIM_832ae5ce-ee9c-4bab-bbba-f6df1b710a92_G8YS5_2204560	RoleManagement	success	–	Remove permanent direct role assignment	2023-10-25T20:52:32.8815032Z	PIM	–

API Name:

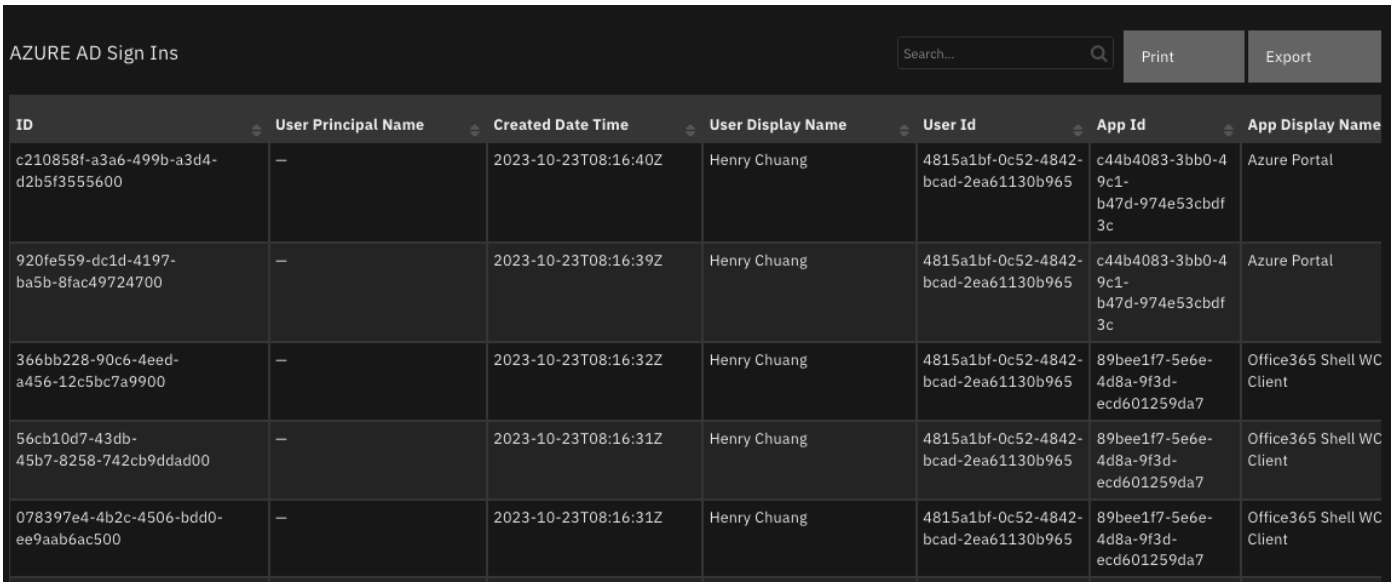
azure_ad_directory_audit_dt

Columns:

Column Name	API Access Name	Type	Tooltip

Column Name	API Access Name	Type	Tooltip
Activity Date Time	azure_ad_activity_date_time	text	-
Activity Display Name	azure_ad_activity_display_name	text	-
Category	azure_ad_category	text	-
ID	azure_ad_id	text	-
Logged By Service	azure_ad_logged_by_service	text	-
Operation Type	azure_ad_operation_type	text	-
Result	azure_ad_result	text	-
Result Reason	azure_ad_result_reason	text	-

Data Table - Azure AD Sign Ins



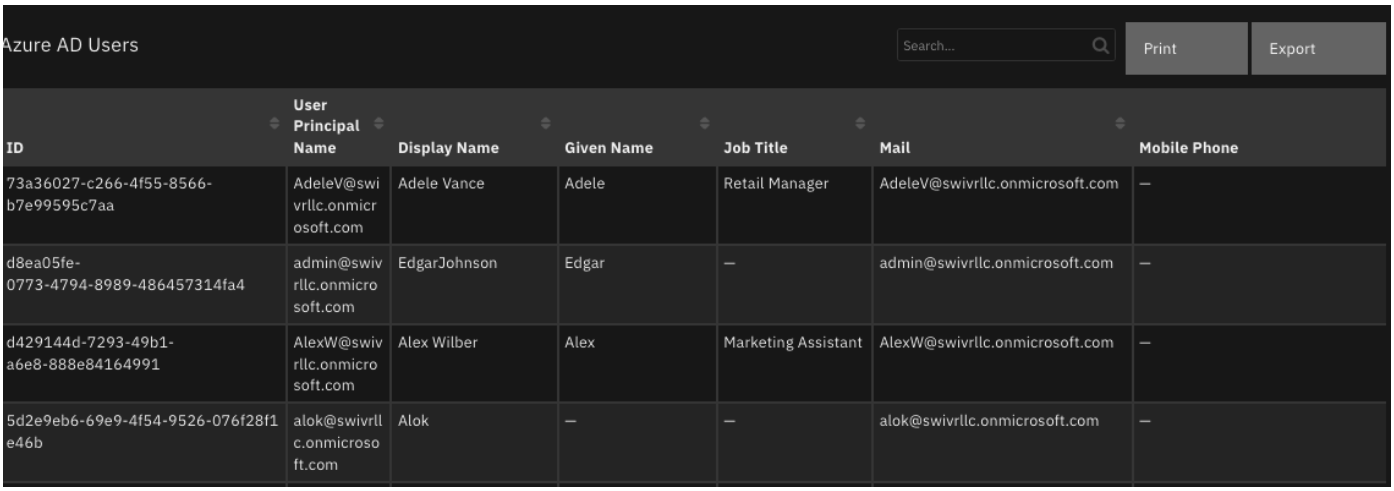
API Name:

azure_ad_sign_ins_dt

Columns:

Column Name	API Access Name	Type	Tooltip
App Display Name	azure_ad_app_display_name	text	-
App Id	azure_ad_app_id	text	-
Created Date Time	azure_ad_created_date_time	text	-
ID	azure_ad_id	text	-
IP Address	azure_ad_ip_address	text	-
User Display Name	azure_ad_user_display_name	text	-
User Id	azure_ad_user_id	text	-
User Principal Name	azure_ad_user_user_principal_name	text	-

Data Table - Azure AD Users



ID	User Principal Name	Display Name	Given Name	Job Title	Mail	Mobile Phone
73a36027-c266-4f55-8566-b7e99595c7aa	AdeleV@swivrllc.onmicrosoft.com	Adele Vance	Adele	Retail Manager	AdeleV@swivrllc.onmicrosoft.com	–
d8ea05fe-0773-4794-8989-486457314fa4	admin@swivrllc.onmicrosoft.com	EdgarJohnson	Edgar	–	admin@swivrllc.onmicrosoft.com	–
d429144d-7293-49b1-a6e8-888e84164991	AlexW@swivrllc.onmicrosoft.com	Alex Wilber	Alex	Marketing Assistant	AlexW@swivrllc.onmicrosoft.com	–
5d2e9eb6-69e9-4f54-9526-076f28f1e46b	alok@swivrllc.onmicrosoft.com	Alok	–	–	alok@swivrllc.onmicrosoft.com	–

API Name:

azure_ad_users_dt

Columns:

Column Name	API Access Name	Type	Tooltip
Business Phone	azure_ad_business_phone	text	-
Display Name	azure_ad_user_display_name	text	-
Given Name	azure_ad_user_given_name	text	-
ID	azured_ad_user_id	text	-
Job Title	azure_ad_user_job_title	text	-
Mail	azure_ad_user_mail	text	-
Mobile Phone	azure_ad_user_mobile_phone	textarea	-
Surname	azure_ad_user_surname	text	-
User Principal Name	azure_ad_user_user_principal_name	text	-

Playbooks

Playbook Name	Description	Activation Type	Object	Status	Condition
Azure Active Directory: Delete Active Directory Users	Delete the user from datatable	Manual	azure_ad_users_dt	enabled	–
Azure Active Directory: Get Directory Audits	Get the list of audit logs generated by Azure Active Directory into a datatable.	Manual	incident	enabled	–
Azure Active Directory: Get Sign Ins	Retrieve the Azure AD user sign-ins for your tenant into a datatable	Manual	incident	enabled	–
Azure Active Directory: Get Users in Active Directory	List users created within Azure AD into a datatable.	Manual	incident	enabled	–
Azure Active Directory: Revoke Sign In Sessions	Invalidates all the refresh tokens issued to applications for the user.	Manual	azure_ad_sign_ins_dt	enabled	–
Azure Active Directory: Update User Status / Password Profile	Update the password properties of the user.	Manual	azure_ad_users_dt	enabled	–

Troubleshooting & Support

Refer to the documentation listed in the Requirements section for troubleshooting information.

For Support

This is an IBM supported app. Please search ibm.com/mysupport for assistance.