**Active Directory to Atlassian Cloud User Synchronization Tool (ADUserSync)**

**Installation Guide**

# Installation Package

|  |  |  |
| --- | --- | --- |
| **Component** | **Description** | **File** |
| Scheduled task definition | Creates a Windows scheduled task that will be triggered when new user is created in Active Directory. | ADUserCreated.xml |
| User synchronization script | This script will be invoked by the scheduled task. | ADUserSync.ps1 |
| Settings | This script contains the environment settings. | Settings.ini |
| Code signer certificate | This self-signed code signer certificate is used to initially sign the PowerShell script. | ADUserSync Code Signer.cer |

# Prerequisites

1. This tool is to be installed on all Windows domain servers.
2. Windows Server 2008 or later is required.
3. PowerShell 5.1 or above is required.

# Pre-Installation Procedures

You can perform the following steps on one of the domain servers.

## Prepare Staging Folder

1. Copy the files in [Installation Package](#_Installation_Package) section to a folder. This document will refer to this folder as [Staging Folder].
2. Open browser to admin.atlassian.com, login and select your organization.
3. Select Directory, then select User provisioning. If you have the improved user management experience, select Settings, then select User provisioning.
4. Select the Directory tab, then select the Regenerate API key button.
5. Select Regenerate key.
6. Copy the SCIM base URL and the API key to a safe place.
7. Select Done.
8. Open [Staging Folder]\Settings.ini with Notepad:
   1. Update SCIMBaseURL setting with value retrieved from admin.atlassian.com.
   2. Update APIKey setting with value retrieved from admin.atlassian.com.
   3. Adjust EmailRetry setting:
      1. After creation, the user in Active Directory will not immediately have an email address. The email address is typically added by manual or automatic process after creation.
      2. However, to create a user in Atlassian Cloud, it is mandatory to have an email address.
      3. Therefore, ADUserSync will attempt to retry until an email address is found for the user before creating it in Atlassian Cloud.
      4. The EmailRetry settings configures how many retry attempts are to be performed.
      5. Set to 0 for no retry.
   4. Adjust EmailSleep settings:
      1. This setting defines how many seconds to wait between retrying for email.
   5. Save and close Notepad.

## Digital Signature for PowerShell Script

The PowerShell script in the installation package is already signed with the public certificate provided. You may choose to use it as is, or you can update the signature.

To update the signature, you may choose to generate a new code signing certificate or use your own certificate.

If you have a code signing certificate, skip to section [Perform Signing](#_Perform_Signing). Otherwise, proceed to section [Generate Self-Signed Code Signing Certificate](#_Generate_Self-Signed_Code).

### Generate Self-Signed Code Signing Certificate

1. This document will refer to the subject field of the certificate as [Subject]. The default value is “ADUserSync Code Signer”.
2. Start | Powershell | Right-click and select “Run as administrator”.
3. Change directory to [Staging Folder]:   
   cd [Staging Folder]
4. Generate the self-signed certificate:   
   New-SelfSignedCertificate -Type CodeSigning -Subject "CN=[Subject]" -KeyAlgorithm RSA -KeyLength 4096 -HashAlgorithm sha256 -CertStoreLocation "Cert:\LocalMachine\My"
5. Export the public certificate:   
   Get-ChildItem -Path "Cert:\LocalMachine\My" | Where-Object { $\_.Subject -match "[Subject]" } | Export-Certificate -FilePath ADUserSyncCodeSigner.cer
6. Import the certificate to trusted root:   
   Import-Certificate -FilePath ADUserSyncCodeSigner.cer -CertStoreLocation "Cert:\LocalMachine\Root"
7. Import the certificate to trusted publisher:   
   Import-Certificate -FilePath ADUserSyncCodeSigner.cer -CertStoreLocation "Cert:\LocalMachine\TrustedPublisher"

### Perform Signing

1. Start | Powershell | Right-click and select “Run as administrator”.
2. Change directory to [Staging Folder]:   
   cd [Staging Folder]
3. Retrieve the signer certificate:   
   $signerCert = Get-ChildItem -Path "Cert:\LocalMachine\My" | Where-Object { $\_.Subject -match "[Subject]" }
4. Perform signing:   
   Set-AuthenticodeSignature -File ADUserSync.ps1 -Cert $signerCert
5. Verify the signature:   
   Get-AuthenticodeSignature -FilePath ADUserSync.ps1  
   If the signature is validated, the Status column will display “Valid”.

# Installation Procedures

The following steps are to be performed on the domain controllers.

## Update Group Policy

We need to update group policy for domain controllers to:

1. Enable successful audit on account management.
2. Enable PowerShell script execution for signed scripts.
3. Distribute code signing certificate.

**Note:** If you have existing domain controller policies, you should merge the following settings with your existing ones.

1. Start | Group Policy Management.
2. Expand target forest | Domains | Expand target domain.
3. Proceed to the following sections.

### Distribute Code Signing Certificate

1. Expand Group Policy Objects.
2. Right-click on Default Domain Controllers Policy, select Edit…
3. Expand Computer Configuration | Policies | Windows Settings.
4. Expand Security Settings | Public Key Policies.
5. Right-click on Trusted Root Certification Authorities, select Import… and click Next.
6. If you have used your own code signing cert:
   1. Browse for the certificate of your code signing cert’s issuer.
   2. Otherwise, browse for ADUserSyncCodeSigner.cer in [Staging Folder].
7. Click Next twice, then click Finish.
8. Right-click on Trusted Publishers, select Import… and click Next.
9. If you have used your own code signing cert:
   1. Browse for your code signing certificate.
   2. Otherwise, browse for ADUserSyncCodeSigner.cer in [Staging Folder].
10. Click Next twice, then click Finish.

### Allow Execution for Signed PowerShell Scripts

1. Expand Domain Controllers | Right-click on Default Domain Controllers Policy and select Edit…
2. Expand Computer Configuration | Expand Policies | Expand Administrative Templates.
3. Expand Windows Components | Windows PowerShell.
4. Double-click Turn on Script Execution.
5. Put a check to Enabled.
6. Select “Allow only signed scripts” in Execution Policy.
7. Click OK to save.
8. With the above steps, signed PowerShell scripts can be executed.

### Configure Domain Policy to Audit User Creation

1. Expand Domain Controllers | Right-click on Default Domain Controllers Policy and select Edit…
2. Expand Computer Configuration | Expand Policies | Expand Windows Settings.
3. Expand Security Settings | Expand Advanced Audit Policy Configuration.
4. Expand Audit Policies | Select Account Management.
5. Double-click Audit User Account Management.
6. Check Configure the following audit events.
7. Check Success.
8. Click OK to save.
9. With the above steps, audit log will include create/delete/modify events for active directory users. The event ID for user creation is 4720.

**Note:** It may take some time for the policy to be synchronized to all servers. To force an update:

1. Log on to each individual domain controller.
2. Start | PowerShell.
3. Enter command:   
   gpupdate /force

## Per-server Installation Procedures

### Deploy Synchronization Tool

1. Copy the files from [Staging Folder] to a new folder on the current server. This document will refer to this folder as [Deployment Folder]. The default value is assumed to be C:\ADUserSync.
2. Right-click on this folder, select Properties.
3. Switch to Security tab.
4. Restrict access to this folder to Administrators and SYSTEM only. The reason is to protect the INI file containing API token for Atlassian cloud site.

### Install Scheduled Task

1. Start | Task Scheduler.
2. Expand Task Scheduler Library | Select Event Viewer Tasks.
3. Right-click on Event Viewer Tasks, select Import Task…
4. Select ADUserCreated.xml from [Deployment Folder].
5. The Create Task dialog appears.
6. In Security options, click Change User or Group… button to select a user in the Administrator group.
7. Optionally, define a delay before the execution of the script:
   1. Switch to Triggers tab.
   2. Double-click on “On an event”.
   3. Put a check to “Delay task for”.
   4. Select the amount of delay.
   5. Click OK.
8. Switch to Actions tab.
9. Double-click on “Start a program”.
10. The Edit Action dialog appears.
11. In Add arguments (optional) field, the original value is:   
    -File "C:\ADUserSync\ADUserSync.ps1" "-eventTriggered -sAMAccountName "$(SamAccountName)"
12. If you have chosen a different [Deployment Folder], update it to:   
    -File "[Deployment Folder]\ADUserSync.ps1" "-eventTriggered -sAMAccountName "$(SamAccountName)"
13. Click OK to save.
14. Click OK again to create the scheduled task.

# Execution Flow

This section describes the details of the event trigger and user synchronization PowerShell script:

1. A new user is created in Active Directory.
2. Domain controller logs event ID 4720.
3. At this point, the user creation process may or may not be complete. The user object has already been created, but the creation process may still be running, updating attributes in the user object (for example, mail attribute to set email address).
4. Task scheduler invokes PowerShell script ADUserSync.ps1 after an optional delay, providing the created user’s sAMAccountName attribute as parameter.
5. ADUserSync.ps1 will confirm if the user has mail attribute. If mail attribute is empty, the script will perform retries according to EmailRetry and EmailSleep settings in Settings.ini.
6. If after configured number of retries, the user still has no mail attribute, an error is logged, and the synchronization fails.
7. Otherwise, the script retrieves information of the user from Active Directory.
8. The script constructs the payload to create user in Atlassian Cloud.
9. The script invokes create user SCIM API of Atlassian Cloud.
10. The payload and response are logged.

# Manual User Synchronization

You can perform manual user synchronization for users that already exist in Active Directory, or in case you need to retry after errors occurred.

1. Login to domain controller.
2. Start | PowerShell.
3. Change to [Deployment Folder]:   
   cd [Deployment Folder]
4. Enter command:   
   .\ADUserSync.ps1 -sAMAccountName [sAMAccountName]  
   where [sAMAccountName] is the Windows login ID of the user to be created on Atlassian Cloud.
5. When manually invoked, there is no retry for users with no mail attribute; it will fail immediately.
6. The result will be displayed on-screen as well as logged.

# Logging

Log is written to Event Viewer, under Applications and Services Logs | User Sync.

## Source

The following sources are defined:

|  |  |
| --- | --- |
| **Source** | **Description** |
| Event | The script is triggered on user creation. |
| Manual | The script is manually invoked. |
| Network | This log contains payload and response to Atlassian Cloud SCIM API. |

## Event ID

The following event IDs are defined:

|  |  |
| --- | --- |
| **Event ID** | **Description** |
| 0 | Success / Information |
| 1 | Script is invoked with invalid parameter |
| 2 | Settings.ini configuration error |
| 3 | User is not found in Active Directory |
| 4 | User already exists on Atlassian Cloud |
| 5 | User has no email (after retries have been exhausted) |
| 6 | Atlassian SCIM API returned error |
| 7 | Atlassian service is unavailable |
| 8 | Internal error |

You can find additional information in the event log’s message and event data, e.g., payload and response from SCIM API.

# Troubleshooting

You can use the following methods to trace the execution of ADUserSync.

## Event Viewer (User Management Events)

The starting point is the event logged by Windows when a user is created in Active Directory.

1. Start | Event Viewer.
2. Windows Logs | Security.
3. Right-click and select Filter Current Log…
4. In <All Event IDs>, type “4720”.
5. Click OK.

## Task Scheduler

You can verify that ADUserSync has been launched via Task Scheduler.

1. Start | Task Scheduler.
2. Expand Task Scheduler Library | Event Viewer Tasks.
3. Double-click ADUserCreated.
4. Switch to History tab.
5. Look for “Action started” and “Action completed” entries.
6. For successful execution, “Action completed” should report a return code of 0.

## Event Viewer (ADUserSync Events)

ADUserSync writes event logs to its own category.

1. Start | Event Viewer.
2. Expand Applications and Services Log | User Sync.
3. Refer to section [Logging](#_Logging) for the list of source and event ID values.