Marketplace user directory sync - user guide

User Directory Sync User Guide

Key points

The User Directory Sync module is a high-performance application designed to automate the synchronisation of user attributes from external identity providers, such as Azure / Entra AD, Okta and external CSV file to the Claromentis intranet. By leveraging modern API-based connections, this module eliminates the security risks associated with direct LDAP connections to Active Directory servers and significantly reduces the complexity of Single Sign-On (SSO) configurations.

Key Technical Concepts:

- Multi-IDP Architecture: The module supports the simultaneous management of multiple independent Azure AD (Entra) connections within a single intranet instance.

- Connection Scoping: Every configuration—including credentials, group selections, and attribute mappings—is strictly scoped to a named "Connection Profile," allowing for granular control over different organisational tenants.

- Enhanced Group Synchronisation: Beyond standard security groups and OUs, the system now supports Microsoft Exchange and Microsoft 365 Mail-enabled security groups.

- Intelligent Group Preservation: Once a group is created in the intranet via synchronisation, it is never deleted by the system, even if it becomes empty or is unselected in the configuration. This ensures that group-based permissions throughout the intranet remain intact.

- Ad-hoc & Scheduled Processing: Background tasks handle high-volume updates on a schedule, while the "Save and Sync" feature allows for immediate, profile-specific updates.

- Automated User Provisioning: The system automatically manages the lifecycle of user accounts, including creation, attribute updates, and deprovisioning (disabling) based on directory status.

Important! The following user guide is written in a step-by-step format to help you configure your User Sync module. It is intended for setting up user directory sync from scratch and assumes that you do not have an existing user directory on your system. If you already have a directory configured on your intranet, please contact Claromentis support team for assistance with migrating your existing directory to work with the User Directory Sync application. Please see the deployment guide for more details.

Currently, the User Sync module supports three user provisioning options: Okta, Azure AD (Entra) and CSV.

Each option has its own section below that will cover the initial configuration and setup.

Setup

The very first step is to locate the User Directory Sync application via Applications > Admin > User Directory Sync icon

You will then be able to navigate to the "Configuration" tab in the User Sync module's admin panel and check the box next to the type of user provisioning that you wish to configure and press "Save". Once you have done so, a new tab will appear in the admin panel of the User Sync module

to allow you to continue the configuration. Henceforth, we will refer to this new tab as the "Provider Tab".

The new tab that appears is intended to resemble the LDAP configuration tab in the core system's Sytem Administration panel. So, if you have used that page before, the configuration tabs in the User Sync module should seem familiar.

Option: Azure AD

In order to connect to Azure AD, you need to:

1. Register an App

2. Generate a Secret

3. Grant the appropriate rights

1.0 Register an App

1. Navigate to https://portal.azure.com and sign in.

2. Navigate to the "All Services" page and select "App Registrations" from the "Manage" menu on the left hand side of the screen.

3. At the top of the page, select the "+ New Registration" option.

4. Choose a name that will make the integration identifiable, such as "Claromentis User Sync".

5. Select the account types that you wish to provide access to. For help on which option should be selected, you can find more information by selecting "Help me choose...".

6. Leave the redirect URI blank and click "Register".

7. At this point, you can view the registered application to retrieve the following fields and populate them in the User Sync Provider Tab:

- Application (Client) ID

- Directory (Tenant) ID

- Connection Name: You must create a unique "Connection Name" for each profile. This name is the primary reference used to identify the directory across Claromentis system and is used for attribution in audit logs and sync requests.

2.0 Generate a Client Secret

1. Navigate to "App Registrations" in Azure and select your Claromentis app according to the display name that you've chosen.

2. Select "Certificates & Secrets" under the "Manage" rubric on the left-hand side of the screen.

3. Click "+ New client secret".

4. Select an appropriate expiry for the secret. Remember to renew the secret if you set an expiry regime.

5. Click "Add".

6. The secret should now appear under the "Client secrets" section of the Application Registration overview. Copy the "Value" code from your newly created secret and navigate to the User Sync module's administration section of your Claromentis installation. Add this to the "Client Secret" input of the Azure Provider Tab.

 7. **Important:** Click "Save" button at the bottom of the config page of Claromentis User Directory Sync application.

3.0 Grant the appropriate rights

Once you have created a new App Registration for Claromentis, you will need to provide it with the appropriate rights that the User Sync module needs in order to view Users and Groups within Azure AD.

1. Navigate to your Claromentis app registration within the "App Registrations" section of Azure.

2. Select "API Permissions" under the "Manage" menu on the left-hand side of the screen.

3. Select "Add a permission". This will open a new dialogue on the right-hand side of the screen.

4. In the right-hand "Select an API" dialogue, click "Microsoft Graph".

5. Select "Application permissions" in the "What type of permissions does your application require?" dialogue.

6. In the resulting dialogue, search for `Group.Read.All`, `GroupMember.Read.All`, `Member.Read.Hidden`, `People.Read.All`, `User.Export.All`, `User.Read` and `User.Read.All` and check their respective checkboxes to indicate that these permissions should be granted.

7. If admin consent is required for these permissions, click "Grant admin consent for [your_username]" button at the top of the list of your permissions.
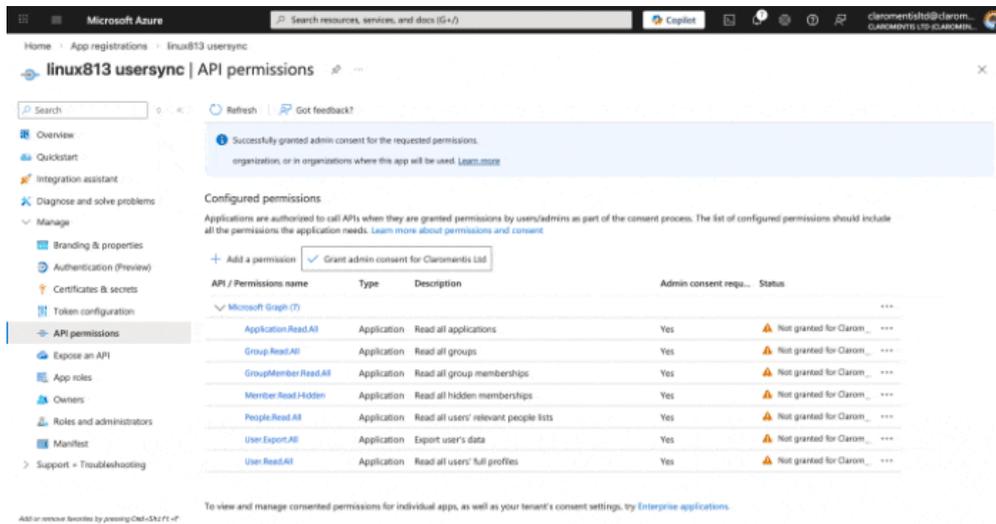
At this point, you should have everything you need. Please see the "Testing" section here for more info on checking if the connection is working. Please additionally note that we found Azure can take up to 10 minutes to start accepting the credentials programmatically provided by Claromentis. So, if it isn't working straight away, please give it some time.

Option: Okta

In order to register with Okta, you will need to:

1. Register an Application.

2. Generate an API Token.

3. Grant the appropriate scopes to the Registered Application.

4. Manage Assignments.

1.0 Register an Application

1. Log in to your Okta Dashboard.

2. Select the "Applications" dropdown from the left-hand pane and select the "Applications" tab within it.

3. In the main page, select "Create App Integration". A popup will appear, showing the "Create a new app integration" dialogue.

4. In the "Create a new app integration" dialogue, select "API Services". This will take you to the "New API Services App Integration" dialogue.

5. In the "New API Services App Integration" dialogue, give your integration a name that will allow you to identify it easily in the future. For example, "Claromentis User Sync". Add your chosen name to the "App integration name" input and click "Save".

6. You should now see a management page for your new App Integration. Within this page you can Retrieve the "Client ID" and a Client Secret (which should have been auto-generated for you) and place them in the Okta Provider Tab of the User Sync module admin panel in Claromentis.

7. Populate your Okta Domain in the Claromentis User Sync module's Okta Provider Tab. This is simply the domain name of your Okta hosting. Your Okta Domain will look something like:

example.oktapreview.com

example.okta.com

example.okta-emea.com

For more information about your domain, please see the Okta Documentation: https://developer.okta.com/docs/guides/find-your-domain/main/

2.0 Generate an API Token

1. Please review information about Okta API Tokens in the Okta Documentation https://help.okta.com/oie/en-us/Content/Topics/Security/API.htm

2. Log in to Okta as a service user.

3. Open the "Security" dropdown on the left-hand side of the page.

4. Select the "API" Tab at the bottom of the dropdown list.

5. Click on the "Tokens" tab within the main page.

6. Click "Create Token" and then choose a name for your token to identify it.

7. You should now see a pop-up saying that your token was created successfully. At this point, you can copy the "Token Value" and update the Okta Provider Tab in the User Sync Admin panel in your Claromentis intranet. Please do this immediately - you will not be able to review the Token Value after you close the Okta popup.

8. **Important:** Click "Save" button at the bottom of the config page of Claromentis User Directory Sync application.

Important notes:

- The user who generated this token must remain active or the token will be revoked and the User Sync will fail.

- If you disable the Okta User Sync in the Claromentis system for more than 30 days, the token will expire due to lack of use.

3.0 Grant Appropriate Scopes

The Claromentis User Sync module requires read access to your Users and Groups in order to function. This section outlines how to provide access to these scopes within Okta.

1. Within Okta, navigate to the Applications directory and open your Claromentis Application Registration.

2. Click on the "Okta API Scopes" tab, just below your Application's name.

3. Select the "Not Granted" filter beneath the "Consent" heading.

4. Find `okta.groups.read` and `okta.users.read` and click the corresponding "Grant" buttons next to each of them. You may see a popup requesting confirmation to provide access.

5. By selecting the "Granted" filter under the "Consent" heading, you should now see the two scopes (`okta.groups.read` and `okta.users.read`) shown in the resulting list.

4.0 Manage Assignments

Now that your connection to Claromentis is registered, you'll need to assign this app to Groups within Okta

1. Within Okta, Navigate to "Groups" and assign the registered Application to the appropriate groups.

2. These Groups will now appear as options in the User Sync admin panel. Select those groups whose users you wish to sync into the system.

Note: No users will sync if you do not select a group in the Provider tab of the User Sync module.

Option: CSV

The CSV sync option supports two methodologies for getting your CSV into Claromentis; "Remote CSV File" and "Intranet DMS".

User data can be provisioned from CSV files either stored in the Intranet's Document Management System (DMS) or fetched from a remote location via

https request (username and password protected).

1. Please review sections 'Exporting users' and 'Updating CSV' in this article to make sure that you can create a valid CSV export document

2. Go to `https://your.domain/cus/usersync/admin/csv` and under `CSV Location` choose the csv source (remote or dms). Make sure that the document can be accessed before proceeding. Once the csv file can be accessed, save the settings and populate the other settings following the instructions on the page.

3. Some important settings to consider are:

- `User match field` - Column in the csv to be used for the `username` field in Claromentis. This column must also exist as a field in the Claromentis user metadata. The default value is set to `username`.
- `Manager field` - The Claromentis user metadata field where the username of the user's manager will be synched to.
- `Password` - If the users provided in the CSV don't have a password or if it's empty, This password value will be used for each user. If also, the default password is not set, the users can't be synced because each user should have a password.
- `Column x Field Match` - If there are columns in the csv that don't match exactly the user field or metadata in Claromentis then this feature can be used. For example, if in the csv the column containing emails is called `email` it won't match the Claromentis user field `emailad` so it needs to be matched correctly.

> Please note that the system will copy everything from the CSV, blocking all user profiles not included in the CSV directory. Therefore, it is recommended that you create at least one local admin account to be able to restore users in case of a sync with empty CSV file

Test the connection

All the Provider Tabs have a "Test Connection" button that will show a green or a red light to indicate whether the details that you have entered allow a successful connection to your chosen user provisioning service.

Connection issues. In some On Premise systems there may be a network / firewall setup which prevents Claromentis system from establishing a connection to an external user directory. In such case you can run the following command from the server's command prompt to see if this is the case.

For Okta directory: Running `curl -H "Authorization: SSWS API_TOKEN" \ https://client-domain.okta.com/api/v1/users` will return a list of users if the network settings are correct.

Perform test sync

Please ensure that you have set status to "Enabled" and saved all your settings before running your first user sync.

All the Provider Tabs have a "Directory Settings" tab which allows you to configure the frequency of your User Sync and also select which groups of users should be synced from your user provisioning system.

Mail-enabled security groups in Azure / Entra connection: This setting allows the inclusion of groups managed via Microsoft Exchange or Microsoft 365.

> IMPORTANT! For Okta and Azure/Entra directories, we recommend that you select a test security group with **a small number of users** to test the sync before selecting the group intended for production. This will avoid creating duplicate accounts.

Note: No users will sync from Okta or Azure/Entra directories if you do not select a group in the "Security groups" field of the User Sync module.

You will also see an auto generated "Directory Key". This is not a field that you need to configure and will be auto populated by Claromentis when you save the connection. It is just an internal reference to your Provider configuration.

Perform the first sync

Azure AD/ Entra: The Save and Sync button triggers an immediate synchronisation for the active connection profile. This does not affect other configured connections. Once clicked, a UI notification will appear to confirm that the synchronisation process has successfully initiated.

Okta / CSV: You can run a fresh sync manually from the People module's admin area under the `synchronize/Update users from user directory` tab. Here you can "Reset" the last run time of your chosen directory. This will cause a background task that runs every 1-2 minutes to trigger a new sync of your chosen directory.

You can also visit the audit logs in the Audit admin application to troubleshoot more about specific actions, syncs and users by selecting the "UserSync" category.

Once you are satisfied that the test users have been synced correctly, please set the User Sync status to disabled.

Configure production security groups

When you have tested the sync with a test group, please select the security group(s) with users you wish to sync into your production system.

Data Mapping

All the Provider Tabs also provide a section named "Claromentis Metadata" which allow you to map fields from your user provisioning provider to Claromentis User Metadata fields.

For Okta and Azure/Entra systems: Enabling the box "Populate Claromentis OrgChart based on the **AD Azure/Okta** manager field" will sync the value of the Manager attribute in Azure/Entra/Okta and populate the OrgChart information for each synced user. Therefore, please make sure that the attribute has values to share. When syncing the directory for the first time, please allow the system to sync for the second time before the Managers data is passed to Claromentis.

Groups sync

All the Provider Tabs also allow you to sync groups into your Claromentis intranet from your provisioning provider.

Groups must have at least one user in them in your external repository to be created in the Intranet on sync. Empty groups will be skipped by the sync.

You can limit the groups that should be synced by a regular expression so that, for example, only groups prefixed with "Intranet" will be synced in. Alternatively, you can sync all groups or disable the group sync altogether.

Please note: When limiting by an expression, enter its name into the User sync module field without any quotation marks or other special characters (that are not in the name), otherwise the groups will not be recognised (users will still be created in the Intranet)

When User directory sync is configured to map groups from the external directory, then the user's group membership will be updated according to how it is set up in that directory. For example, if groups are automatically provisioned from an external user directory and you manually add a user to a local group in Intranet, AD users will be removed from that local group.

Enable and schedule user sync

Once all of the above steps have been completed, you can enable and schedule the User Sync to perform its operation.

About Daily frequency. This is a schedule that runs once every 24 hours on the hour you specify in the "Time" field. However, if a manual sync is run within the 24 hours window, then the next scheduled sync will be skipped until the next day.

Troubleshooting

Basic requirements. Users must have a Username, First Name, Last Name and Email address in order for the Claromentis system to create them during the sync. If one user in particular is not syncing correctly, this is a good thing to check in your directory provider.

Limitation. In our tests the user sync performs well when syncing up to 7000 - 8000 users from Azure and Okta directories. Performance may be reduced when syncing over 10000 users.

System config. Typically, when syncing over 10000 users, you may find that the system times out before completing the sync. If this happens, please contact the Claromentis support team to configure the system timeout settings.

Existing user directory. If you already have a directory configured on your intranet, please contact Claromentis support team for assistance with migrating your existing directory to work with the User Directory Sync application. Configuring the sync prior to migration may result in duplicate users. Please see the deployment guide for more details.

Claromentis systems 8.13 or prior. Please set the Frequency on Daily, with Time setting to 12 pm - mid-day.

Audit logs. You can check the results of the sync by reviewing the logs via Admin > Audit > View Logs and then filtering for "System", "Users" categories. Here is a typical log file.

In this case you can solve the Local account issue by contacting Claromentis team to migrate the directory from existing to the new one. Or if this applies to only a few users, you can manually update them by going to Admin > People > select the user and change their directory from Local to Azure

Missing email in the Azure user's profile. In order to create an account in Intranet, the user must have a valid email address field. Therefore, once you have updated the Azure profile with the email address, the user will be synced with the intranet.

FAQ

1. We already created users locally on Intranet. When we do the first user sync, existing users will get updated and not deleted/recreated if the username field is the same, correct?
Yes, that is correct, but only when we configured all existing users with the Okta/Azure directory. Currently, all your users are considered to be local, as far as the Intranet is concerned. So, after setting up your user directory on Intranet, you should disable the scheduled sync and let us know via a

change request, so that we can ensure that all users have been switched from local to Okta/Azure directory. Please see the deployment guide for more details.

If you run a sync before this switchover, only new users will be added to Intranet and existing users would not be updated.

2. Will implementing this sync impact anything else within our intranet site or is it just the People section?

Just the People app, but you must be aware of the licence limit. If your Okta/Azure group, which contains all users to be synced with the Intranet has more users than the licensed number of users on Intranet, then the sync will stop.

3. If a user is in the People section but no longer with the company (not in Okta/Azure) and we sync, will it get removed?

As long as the user is configured as Okta/Azure directory user in the intranet, then once it is deleted from Okta/Azure, it will get disabled in People (Intranet). Disabled users do not count towards licence. Disabled users do not appear anywhere else in the Intranet and have no permissions or access to it. You can then filter out disabled users in Admin > People and delete them permanently, if required.

4. If a user is accidentally removed, can you restore the object easily?

If you remove it from Okta/Azure, then user gets disabled in Intranet - see above. If you disable a user in Intranet, whilst it is still active in Okta/Azure, then it will come back as active in the next sync with Okta/Azure, or you can just re-enable it in Intranet. If you delete a user in Intranet, but it is still active in Okta, then the user will be recreated in Intranet after the next sync, but all references to the user's previous activities would be deleted. You may need to manually restore permissions for that user. It is possible to restore from backup, but we would restore the whole system, not just a single user.

5. We already set up Claromentis app in Okta for SSO. Do we need to create another one for User Sync?

Yes, you will need to create a separate app for user sync. The reason is because the SSO (Login Handler) uses SAML methods for it to work and User Sync requires API Services, which is a different app. Okta does not allow two methods / services to be included in a single app. This is different for Azure because it allows multiple services to be included in a single app.

6. We would like to use the csv file to import the users into the system but allow them to login to the system using SSO via another Identity Provider. Is this possible? Are there additional steps to make this happen?

Yes, this is possible.

By default, all users in your People application are created as 'local' accounts. Therefore any user provisioned by the SSO will be created as local user in the intranet.

When you enable a User Sync application and set up a new source of users such as CSV/Azure/Okta, you will create a new directory to which local users can be switched. Currently you can do this manually, or you can ask Claromentis to do it for you, as long as we know which users need switching.
You can use the User Sync via csv to update the existing user profiles, as long as the usernames match. You can also create new users and SSO will be used to log them in, as long as the usernames match.

To be super-clear, the csv file must contain all users which must exist within CSV directory. If users are missing from the CSV file, then those users will be blocked in your Intranet.

7. Ok, I synced the users from Azure / Okta directory and I can see their profiles in the Intranet. However, they cannot access the intranet using their Azure / Okta credentials.

This is expected behaviour, because the User Sync application is used to create / manage users and their profiles in the Intranet. It is not used for authentication and therefore does not store passwords on the system. User sync works with in tandem with Login Handler application, which is responsible for user authentication and SSO.

8. What happens if groups are automatically provisioned from an external user directory, but then I manually add a user to a local group in Intranet?

A: Directory users will be removed from that local group. Therefore we recommend using Roles for managing users locally during onboarding of the new system. Roles membership is not affected by user synchronisation from an external directory

When User directory sync is configured to map groups from the external directory, then the user's group membership will be updated according to how it is set up in that directory.

For example, 'user a' is a member of 'AD-Intranet' group, which is a group set in an AD directory. 'User a' has also been added to 'Local-Intranet' group, which is created and managed manually on Intranet. Here are possible scenarios:

If Group mapping is enabled, then 'user a' will no longer be a member of 'Local-Intranet' group after the next user sync.

If Group mapping is then disabled, then 'user a' will stay in 'AD-Intranet' group and 'Local-Intranet' group after the next sync. It is important to note that group mapping from external directory will no longer take place in this scenario

9. What user attributes can be synced from an external user directory?

A: By default the application can sync the following standard user attributes from Azure / Entra:

aboutMe
ageGroup
birthday
businessPhones
city
consentProvidedForMinor
country
createdDateTime
creationType
department
displayName
employeeHireDate
employeeId
employeeType
faxNumber
hireDate
imAddresses
interests
legalAgeGroupClassification
mailNickname
mobilePhone
mySite
officeLocation
otherMails
pastProjects
postalCode
preferredLanguage
preferredName
proxyAddresses
responsibilities
schools
skills
state
streetAddress
usageLocation
userType

and the following attributes from Okta:

middleName
honorificPrefix
honorificSuffix
displayName
nickName
profileUrl
secondEmail
mobilePhone
primaryPhone
streetAddress
city
state
zipCode
countryCode
postalAddress
preferredLanguage
locale
timezone
userType
employeeNumber
costCenter
division
department
managerId

manager

Related Article

[Claromentis marketplace](#)

[User sync deployment guide](#)

[User management FAQ](#)

Last modified on 14 May 2026 by Hannah Door

Created on 4 August 2023 by Stas Dreiling
Tags: user guide