ManageEngine
Identity Manager Plus

Admin Guide

Contents

About Identity Manager Plus

Identity Manager Plus is a cloud-based, single sign-on (SSO) solution for enterprises. It delivers SSO to cloud-based and on-premises applications, and provides intelligence on application usage and access.

Features

Enterprise SSO: Provide one-click access to enterprise applications by enabling SSO. With Enterprise SSO, users can access all their corporate applications in one click just by signing in once using one set of credentials.

Access management: Ensure that the right employees have access to the right applications by assigning or revoking application access to users in bulk.

User life cycle management: Automate user life cycle management by provisioning and deprovisioning users across various applications and services using the System for Cross-domain Identity Management (SCIM).

Reporting and analytics: See comprehensive reports detailing when a given user accessed an application. Audit administrators' activities with an exclusive report that gives details on modifications made to directories, users, and applications.

Supported directories

Identity Manager Plus provides out-of-the-box integrations with the following directories and applications:

* Azure Active Directory (AD)
* Salesforce
* G Suite Directory
* Zendesk
* Zoho Directory
* Slack

You can also import users from other directories or systems, including on-premises AD, manually. This makes it easy to provide users with access to the applications they need.

Supported applications

Identity Manager Plus supports any application—cloud-based or on-premises—that is SAML, OAuth, or OpenID Connect-enabled. If you have a custom application that supports any of these protocols, it can be configured for SSO in Identity Manager Plus.

Getting started

Signing up

Signing up for Identity Manager Plus is quite easy.

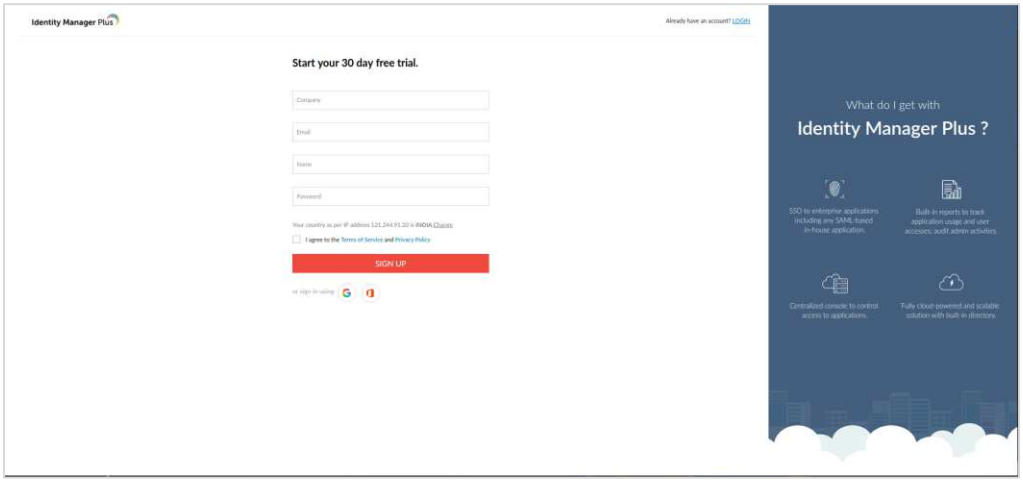
1. Visit https://identitymanager.manageengine.com/signup.

2. Enter your company name, your email address, your name, a password, and click SIGN UP.

You can also use your existing Office 365, Google, or Zoho account to sign up.

Once you sign up, a confirmation email will be sent to your email address. Click the link in that email to activate your Identity Manager Plus account and continue with the login process.

For end users, the admin has to either send an invitation email or verify the domain they are part of. Refer to the Managing Users section for more information on how to enable Identity Manager Plus for end users.



Logging in

Administrators can log in to Identity Manager Plus using the account they used to sign up.

End users can use either their existing directory account or the Zoho account they activated through email invitation to log into Identity Manger Plus. Refer the Logon Settings to know more.

Admin portal and user portal

The admin portal provides access to all the functionalities of Identity Manager Plus. It contains the dashboard, application settings, directory settings, and reports. Only users with Admin or Super Admin roles can log in to the admin portal.

The user portal provides access to the SSO-enabled enterprise applications. All types of users can log in to the user portal.

User roles

Identity Manager Plus employs three types of user roles to control the privilege a user has within the service.

User role	Admin portal							User portal
	Dashboard	**Add, modify, remove applications and directories**	**Access to reports**	**Add and modify users**	**Remove users**	**License management**	**Authenticator Settings (Logon Settings)**	
Super Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Admin	Yes	Yes	Yes	Yes	No	No	No	Yes
User	No							Yes

To learn how to change a user's role, click here.

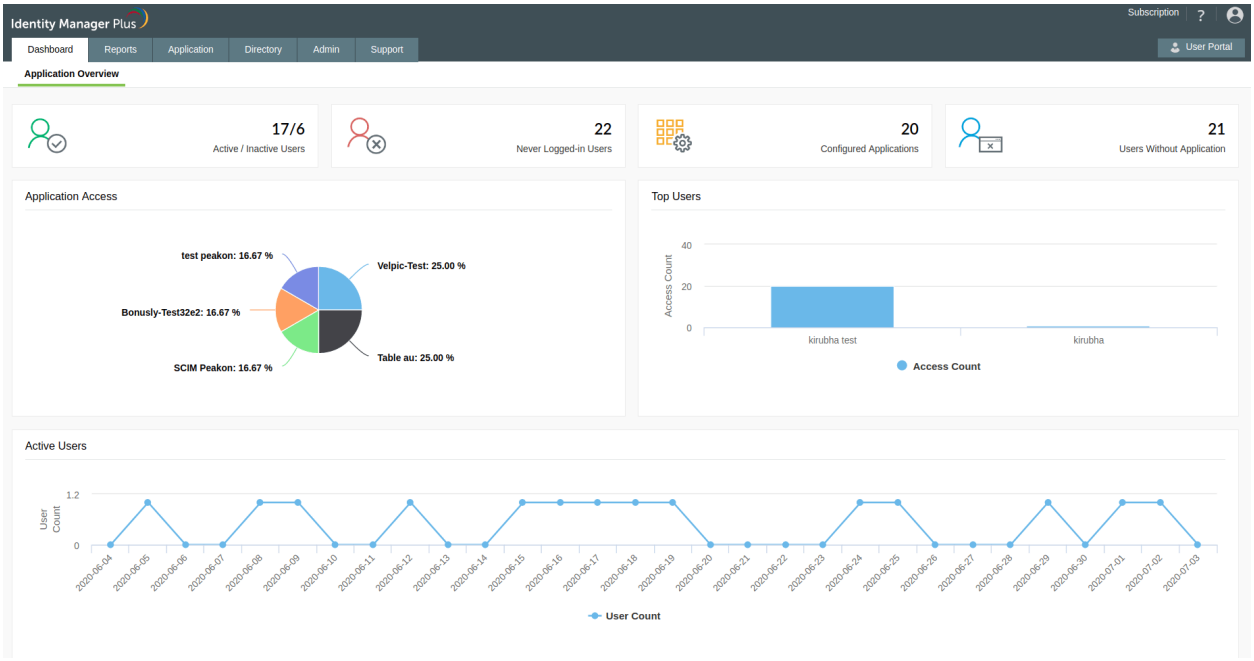
Subscription

Identity Manager Plus subscription costs are based on the number of users using the service for single sign-on. Pricing starts at $1 per user, per year.

Dashboard

When you log in to Identity Manager Plus as an Admin, the dashboard is the first page you see. The dashboard shows you key metrics related to users and applications, in neat graphical charts, including:

- Active and inactive users
- Users who have never logged in
- Users without application access
- The most frequently used applications
- Top users



Reports

The Reports menu provides insight into application access and usage. If you log in as a Super Admin, you can also view the actions performed by other users with Admin or Super Admin privilege.

The reports can be exported in various file formats, which includes CSV, PDF, HTML, and XLS. You can also customize the reports by adding or removing fields in the reports to view only the data that is relevant to you.

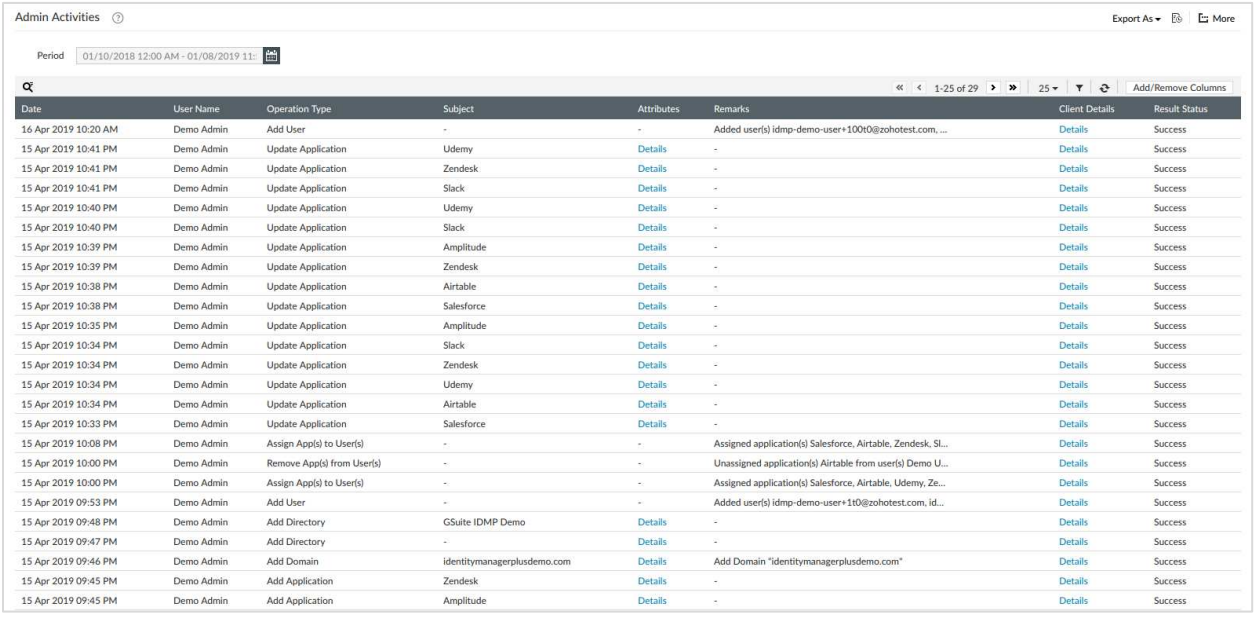
The reports are grouped into the following categories:

- Activities Reports
- Application Reports
- User Reports
- Logon Activity Reports

Activities Reports

The following reports are available under this category:

Admin activities report: Provides a detailed audit trail of actions performed by users with Admin and Super Admin roles for a specified period. With this report, you can view the operation performed, who performed it, when it was performed, and more.



Date	User Name	Operation Type	Subject	Attributes	Remarks	Client Details	Result Status
16 Apr 2019 10:20 AM	Demo Admin	Add User	-	-	Added user(s) idmp-demo-user+100t0@zohotest.com, ...	Details	Success
15 Apr 2019 10:41 PM	Demo Admin	Update Application	Udemy	Details	-	Details	Success
15 Apr 2019 10:41 PM	Demo Admin	Update Application	Zendesk	Details	-	Details	Success
15 Apr 2019 10:41 PM	Demo Admin	Update Application	Slack	Details	-	Details	Success
15 Apr 2019 10:40 PM	Demo Admin	Update Application	Udemy	Details	-	Details	Success
15 Apr 2019 10:40 PM	Demo Admin	Update Application	Slack	Details	-	Details	Success
15 Apr 2019 10:39 PM	Demo Admin	Update Application	Amplitude	Details	-	Details	Success
15 Apr 2019 10:39 PM	Demo Admin	Update Application	Zendesk	Details	-	Details	Success
15 Apr 2019 10:38 PM	Demo Admin	Update Application	Airtable	Details	-	Details	Success
15 Apr 2019 10:38 PM	Demo Admin	Update Application	Salesforce	Details	-	Details	Success
15 Apr 2019 10:35 PM	Demo Admin	Update Application	Amplitude	Details	-	Details	Success
15 Apr 2019 10:34 PM	Demo Admin	Update Application	Slack	Details	-	Details	Success
15 Apr 2019 10:34 PM	Demo Admin	Update Application	Zendesk	Details	-	Details	Success
15 Apr 2019 10:34 PM	Demo Admin	Update Application	Udemy	Details	-	Details	Success
15 Apr 2019 10:34 PM	Demo Admin	Update Application	Airtable	Details	-	Details	Success
15 Apr 2019 10:33 PM	Demo Admin	Update Application	Salesforce	Details	-	Details	Success
15 Apr 2019 10:08 PM	Demo Admin	Assign App(s) to User(s)	-	-	Assigned application(s) Salesforce, Airtable, Zendesk, Sl...	Details	Success
15 Apr 2019 10:00 PM	Demo Admin	Remove App(s) from User(s)	-	-	Unassigned application(s) Airtable from user(s) Demo U...	Details	Success
15 Apr 2019 10:00 PM	Demo Admin	Assign App(s) to User(s)	-	-	Assigned application(s) Salesforce, Airtable, Udemy, Ze...	Details	Success
15 Apr 2019 09:53 PM	Demo Admin	Add User	-	-	Added user(s) idmp-demo-user+1t0@zohotest.com, id...	Details	Success
15 Apr 2019 09:48 PM	Demo Admin	Add Directory	GSuite IDMP Demo	Details	-	Details	Success
15 Apr 2019 09:47 PM	Demo Admin	Add Directory	-	Details	-	Details	Success
15 Apr 2019 09:46 PM	Demo Admin	Add Domain	identitymanagerplusdemo.com	Details	Add Domain "identitymanagerplusdemo.com"	Details	Success
15 Apr 2019 09:45 PM	Demo Admin	Add Application	Zendesk	Details	-	Details	Success
15 Apr 2019 09:45 PM	Demo Admin	Add Application	Amplitude	Details	-	Details	Success

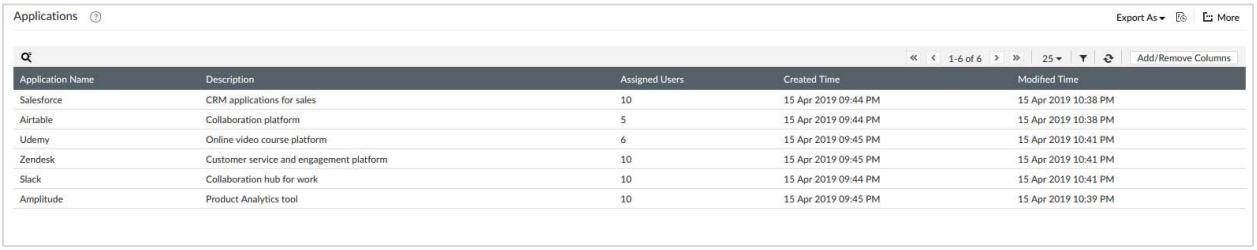
Application Access report: Reveals when an application was accessed, who accessed it, the client IP, and the agent used to access the application during the specified period.

Unmanaged Users report: Lists the users whose accounts have been unmanaged.

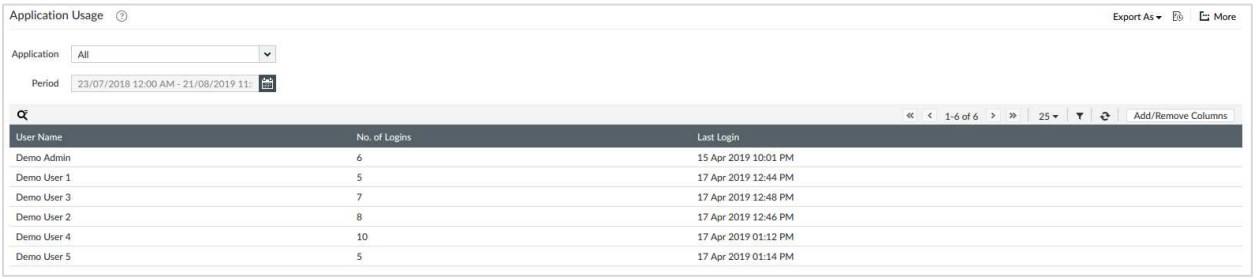
Applications Reports

The following reports are available under this category:

Applications report: Shows the details of the applications added in Identity Manager Plus, such as the name, description, assigned users, created time, and modified time.



Application Usage report: Shows how many times a user has logged in to an application during a specific period. You can also see the last time an application was used by a user.



Assigned Applications report: Lists the users assigned to the selected application.

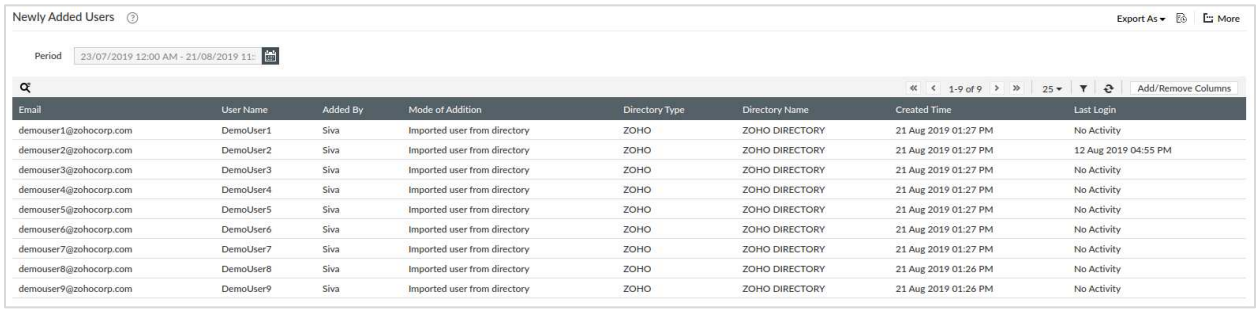
User Reports

The following reports are available under this category:

Inactive Users report: Lists the users who haven't logged in or whose sessions are idle over the past specified number of days.

Disabled Users report: Lists the users who are disabled over the past specified number of days.

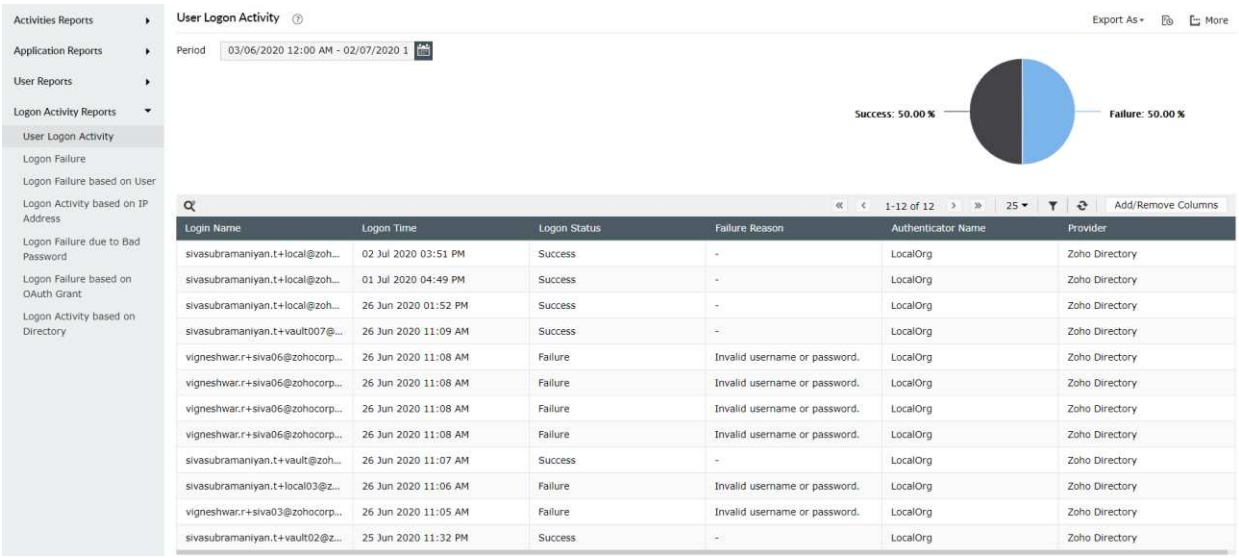
Newly Added Users report: Lists the users who were added during the specified period.



Email	User Name	Added By	Mode of Addition	Directory Type	Directory Name	Created Time	Last Login
demouser1@zohocorp.com	DemoUser1	Siva	Imported user from directory	ZOHO	ZOHO DIRECTORY	21 Aug 2019 01:27 PM	No Activity
demouser2@zohocorp.com	DemoUser2	Siva	Imported user from directory	ZOHO	ZOHO DIRECTORY	21 Aug 2019 01:27 PM	12 Aug 2019 04:55 PM
demouser3@zohocorp.com	DemoUser3	Siva	Imported user from directory	ZOHO	ZOHO DIRECTORY	21 Aug 2019 01:27 PM	No Activity
demouser4@zohocorp.com	DemoUser4	Siva	Imported user from directory	ZOHO	ZOHO DIRECTORY	21 Aug 2019 01:27 PM	No Activity
demouser5@zohocorp.com	DemoUser5	Siva	Imported user from directory	ZOHO	ZOHO DIRECTORY	21 Aug 2019 01:27 PM	No Activity
demouser6@zohocorp.com	DemoUser6	Siva	Imported user from directory	ZOHO	ZOHO DIRECTORY	21 Aug 2019 01:27 PM	No Activity
demouser7@zohocorp.com	DemoUser7	Siva	Imported user from directory	ZOHO	ZOHO DIRECTORY	21 Aug 2019 01:27 PM	No Activity
demouser8@zohocorp.com	DemoUser8	Siva	Imported user from directory	ZOHO	ZOHO DIRECTORY	21 Aug 2019 01:26 PM	No Activity
demouser9@zohocorp.com	DemoUser9	Siva	Imported user from directory	ZOHO	ZOHO DIRECTORY	21 Aug 2019 01:26 PM	No Activity

Logon Activity Reports

The following reports are available under this category:



Login Name	Logon Time	Logon Status	Failure Reason	Authenticator Name	Provider
sivasubramaniyan.t+local@zoh...	02 Jul 2020 03:51 PM	Success	-	LocalOrg	Zoho Directory
sivasubramaniyan.t+local@zoh...	01 Jul 2020 04:49 PM	Success	-	LocalOrg	Zoho Directory
sivasubramaniyan.t+local@zoh...	26 Jun 2020 01:52 PM	Success	-	LocalOrg	Zoho Directory
sivasubramaniyan.t+vault007@...	26 Jun 2020 11:09 AM	Success	-	LocalOrg	Zoho Directory
vigneshwar.r+siva06@zohocorp...	26 Jun 2020 11:08 AM	Failure	Invalid username or password.	LocalOrg	Zoho Directory
vigneshwar.r+siva06@zohocorp...	26 Jun 2020 11:08 AM	Failure	Invalid username or password.	LocalOrg	Zoho Directory
vigneshwar.r+siva06@zohocorp...	26 Jun 2020 11:08 AM	Failure	Invalid username or password.	LocalOrg	Zoho Directory
vigneshwar.r+siva06@zohocorp...	26 Jun 2020 11:08 AM	Failure	Invalid username or password.	LocalOrg	Zoho Directory
sivasubramaniyan.t+vault@zoh...	26 Jun 2020 11:07 AM	Success	-	LocalOrg	Zoho Directory
sivasubramaniyan.t+local03@z...	26 Jun 2020 11:06 AM	Failure	Invalid username or password.	LocalOrg	Zoho Directory
vigneshwar.r+siva03@zohocorp...	26 Jun 2020 11:05 AM	Failure	Invalid username or password.	LocalOrg	Zoho Directory
sivasubramaniyan.t+vault02@z...	25 Jun 2020 11:32 PM	Success	-	LocalOrg	Zoho Directory

User Logon Activity report: Shows the logon activity of all users.

Logon Activity Based on Directory: Shows the logon activity of users based on directory.

Logon Activity Based on IP Address: Shows the logon activity of users based on IP address.

Logon Failure report: Shows the number of failed logons along with their details.

Logon Failure Based on User report: Shows the details of failed logons based on users.

Logon Failure Due to Bad Password: Shows the details of failed logons due to bad passwords.

Logon Failure Based on OAuth Grant: Shows the details of failed logons due to OAuth Grant.

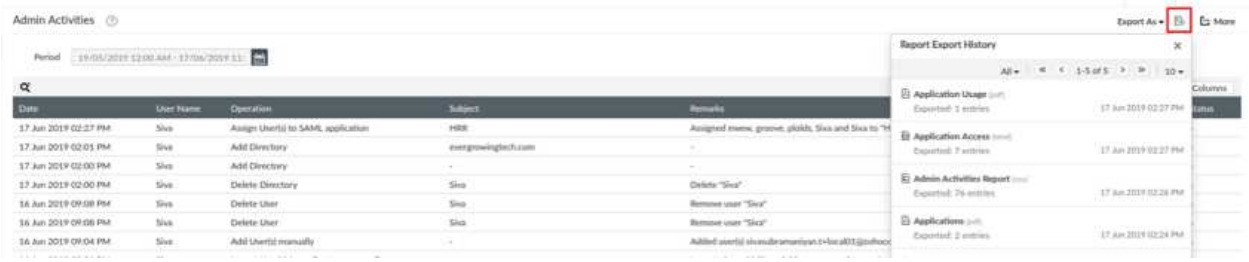
Exporting the reports

1. Select the desired report, and in the top-right corner, click the **Export As** menu.

2. Select the file format. Supported formats: CSV, PDF, HTML, and XLS.

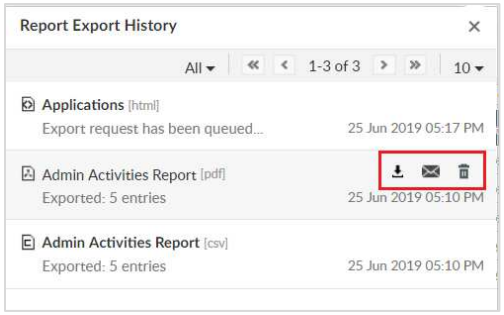
3. The report will be queued for export.

4. Click the **Report Export History** icon that is present next to the Export As menu.



5. Hover over the report that you exported. You'll get three options.

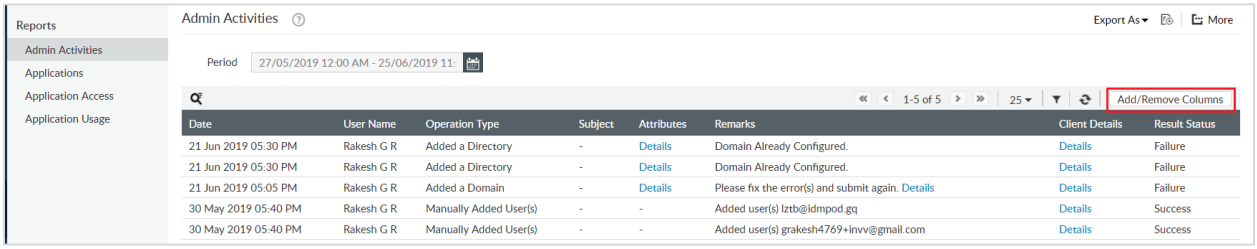
    - Click the **Download** icon to download and save the report.
    - Click the **Mail** icon to send the report via email.
    - Click the **Delete** icon to remove the report form the Report Export History list.



6. Click **More** to view the **Export Settings**. Here you can modify the **description** of the report and also choose to **include the product logo** in the report header.

Customizing the reports

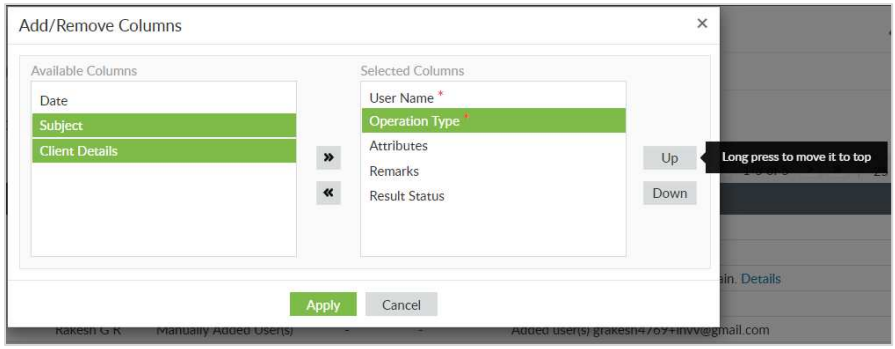
1. Select the desired report and click the **Add/Remove Columns** button.



2. **To add a field**, select the field from the **Available Columns** list and click the **>>** arrow to move it to the **Selected Columns**.

3. **To remove a field**, select the field from the **Selected Columns** list and click the **<<** arrow to move it to the **Available Columns**.

4. You can also select the order in which the fields appear by selecting a field and clicking the **Up** or **Down** buttons.



Note: Fields marked as mandatory cannot be removed.

Application

The application menu allows you to configure and enable SSO and automated provisioning and deprovisioning for your enterprise applications. Identity Manager Plus comes pre-integrated with over 300 popular enterprise applications. If your application is missing from the list, use the custom application option to add it manually.

Enabling SSO for an application

ManageEngine Identity Manager Plus single sign-on (SSO) simplifies application access using a secure portal. This provides better security and makes applications accessible with just one click.

ManageEngine Identity Manager Plus supports two widely used SSO protocols:

- SAML
- OAuth/OpenID Connect

SAML SSO

Security Assertion Markup Language (SAML) is an open standard that links authentication and authorization services to access-protected resources. Identity Manager Plus supports the secure and widely adopted industry standard SAML 2.0.

Identity Manager Plus SAML SSO eliminates the need for multiple user IDs and passwords, streamlines the login experience of users, and improves security.

With SAML authentication, we have an identity provider (IdP) and a service provider (SP). The IdP verifies the user's login credentials and sends a claim to the SP as proof of verification. Here, the IdP is Identity Manager Plus and the SP is the cloud application or service that a user wants to access.

How SAML works

There are two types of flows in SAML SSO.

SP-initiated SSO

1. A user attempts to log in to the SP.
2. The user is redirected to the Identity Manager Plus login page. The user enters their directory login credentials here.

3. Identity Manager Plus verifies the user login, and if successful, it issues an authentication claim, which is handed to the SP along with the redirection link to the SP. The claim does not contain the password. It has other personal attributes like the last name, first name, email address, and more.

4. The SP accepts this claim after verifying the digital signature of IdP and logs the user in.

IdP-initiated SSO

1. A user logs in to the Identity Manager Plus portal.

2. To access an application, they can simply click on the corresponding application's icon in the Applications tab.

3. Identity Manager Plus sends the authentication claim to the SP directly, as they are already logged in to Identity Manager Plus.

4. The SP accepts this claim after verifying the digital signature of IdP and logs the user in.

Learn how to configure SAML SSO in Identity Manager Plus for:

- Predefined applications
- Custom application

Predefined applications

Add an application for SSO

1. Log in to Identity Manager Plus as an Admin or Super Admin.

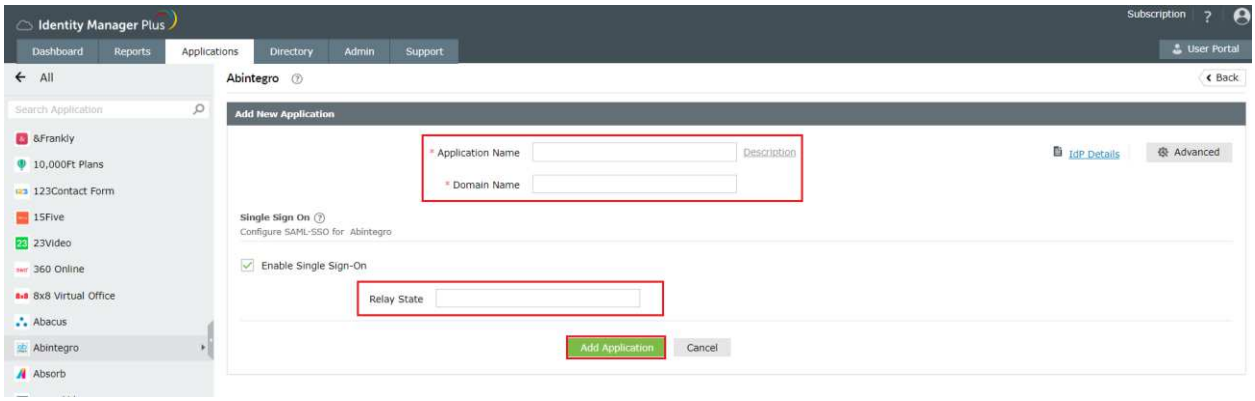
2. Navigate to Application and click **Add Application** or select one of the applications from the list displayed.

   Tip: Use the search option or click on a category to quickly get to the application you want to add.

3. Enter the **Application Name** and **Domain Name**.

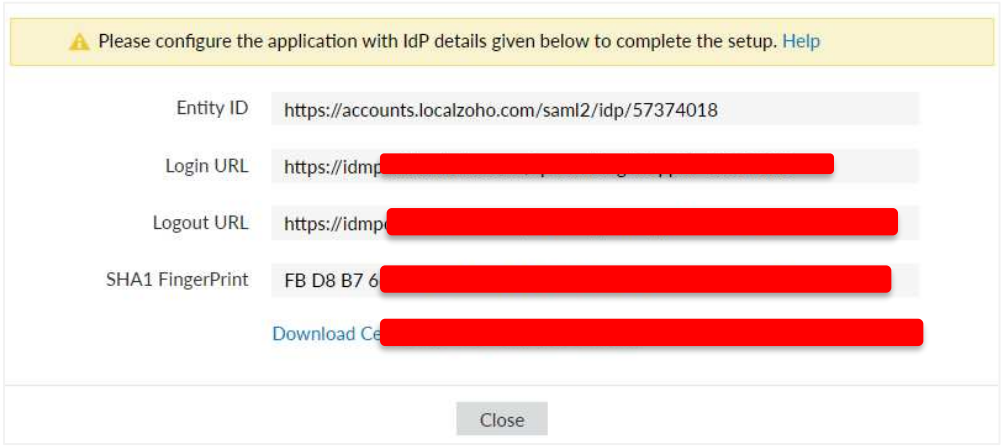
4. Select the **Enable Single Sign-On** checkbox.

5. Enter the **Relay State** and any other application-specific information as required.



6. Click **Add Application**.

7. A pop-up containing the IdP details for that application will be shown as soon as you add the application.



8. Copy the **Login URL** and **Logout URL**, and copy the **SHA1 Fingerprint**; or just download the **metadata file** based on the requirements set by your application.

9. Follow the procedure mentioned in your application to enable SAML SSO and finish the setup.

Custom application

Adding a custom SAML application

1. In the **Application** menu, click the **Add Custom Application** link in the bottom of the left-side panel.

2. Enter the **Application Name** and **Domain Name**.

3. Upload the icons for the application if available.

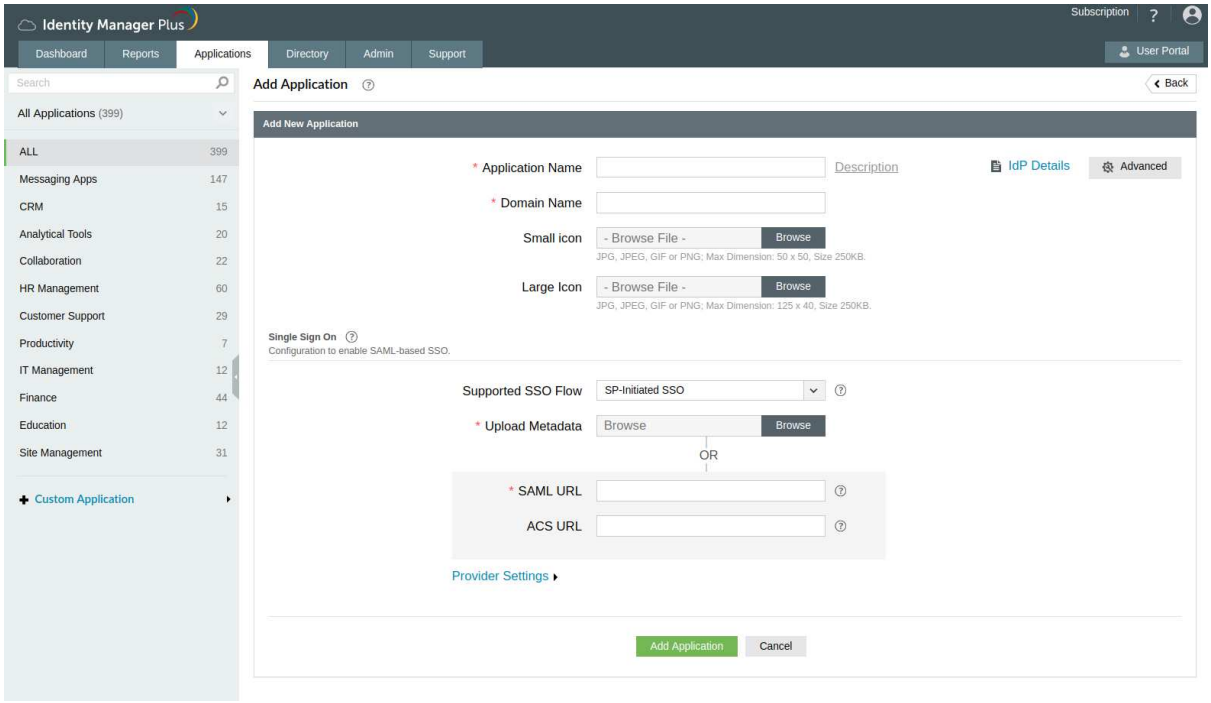
4. Select the supported SSO flow.

    a. **SP-initiated SSO:** In a SP-initiated SSO, when users click on an application link, they will be taken to the login page of the SP. After entering their username or selecting the SAML SSO option, the SP will redirect the users to the IdP. Users then need to log in to the IdP to be able to access the SP.

    b. **IdP-initiated SSO:** In an IdP-initiated SSO, users log in to the ADSelfService Plus page, and click an application. The application will open in a new tab and the users will be logged in automatically.

Here, the IdP refers to Identity Manager Plus and the SP refers to the SAML application.

5. If the application has a **Metadata file**, click **Browse** and **select the XML file**.



6. If you don’t have a metadata file, enter the following details:

    a. In the **SAML Redirect URL** field, enter the SAML redirect URL your application service provider supplies. The URL value can be found in the application’s default login page or in the SSO configuration page.

    b. Enter the **Assertion Consumer Service (ACS) URL** your application service provider provides in the ACS URL field. This value can also be found in the application's SSO configuration page.

c. If the application you are trying to add supports only IdP-initiated SSO, then you must enter the **Entity ID** value of the application.

7. Click **Add Application**.
8. A pop-up containing the IdP details for that application will be shown as soon as you add the application.
9. Copy the **Login URL** and **Logout URL**, and download the **metadata file** or **certificate file**, or copy the **SHA1 FingerPrint** based on the requirements set by your application.
10. Follow the procedure mentioned in your application to enable SAML SSO to finish the setup.

Assigning applications to users

To assign or unassign applications to users:

1. Log in to Identity Manager Plus as an Admin or Super Admin.
2. Navigate to **Application**. You'll see a list of applications configured for SSO.
3. Select the applications you want to manage.
4. In the **Manage** drop-down at the top of the table:
    a. Select **Assign Application** to choose users and grant them access to the selected applications.
    b. Select **Unassign Application** to revoke the access a user or users have to the selected applications.
5. You can also click the link under the Assigned Users column to assign or revoke the access users have to an application.

Managing applications

You can enable, disable, or delete applications from Identity Manager Plus.

- **Disabling an application** will block users from accessing that application. In this case, the configuration details of the application will be retained. You can re-enable the application to allow users to access it through SSO.
- **Deleting an application** will completely remove the application information from Identity Manager Plus. If you want to enable SSO for a deleted application, you need to configure the application from scratch by uploading the metadata file or other necessary information.

To disable or delete applications:

1. Log in to Identity Manager Plus as an Admin or Super Admin.
2. Navigate to **Application**. You'll see a list of applications configured for SSO, the users assigned to each, and the IdP details for each application.
3. Select the applications you want to manage.
4. In the **Manage** drop-down at the top of the table, select **Enable, Disable, or Delete** based on the action you want to perform.
5. Click the **Details** link under the **IdP Details** column to view the identity provider details. Copy these details and configure them in the application (service provider) to enable SSO.

OAuth and OpenID Connect SSO

OAuth is an authorization protocol that allows authenticated resource accesses between servers and services without sharing any logon credentials. OpenID Connect is an identity layer on top of OAuth's framework.

The basic components in OAuth and OpenID Connect's working are:

- **Server**: This entity is going to verify the user credentials and provide the key to log them in. In our case, Identity Manager Plus acts as a server.
- **Client application**: This application depends on the server to verify the user's identity.
- **User**: This is the account that is attempting to log in to the client application.

OAuth

This is how OAuth enables SSO:

1. A user tries to log in to an application. The application sends an **authorization request** to Identity Manager Plus. The user is redirected to the Identity Manager Plus login page.
2. The user enters their logon credentials here. After successful verification, an **authorization code** is sent to the application from Identity Manager Plus.
3. The application sends the authorization code back to Identity Manager Plus to receive the **access token** and the **refresh token**. The access token acts as a time-bound key for the user to access the application's protected resources. The refresh token is a permanent key that can be used to request a new access token after the old one expires.
4. Now, the application sends a **user info request** along with the access token as proof of identity to Identity Manager Plus. The response to this request returns the user profile details required to complete the login process.
5. After successful verification of user details on the application's end, the user is logged in to the application.

OpenID Connect

OpenID Connect is similar OAuth SSO, but an ID token is used here.The ID token contains the signature of Identity Manager Plus and the user details.There are two scenarios that are possible here. Let's understand the workflow in both these cases:

Application-initiated login

1. A user tries to log in to an application. The application sends an authorization request to Identity Manager Plus. The user is redirected to the Identity Manager Plus login page.
2. The user enters their logon credentials here. After successful verification, an authorization code is sent to the application from Identity Manager Plus.
3. The application sends the authorization code back to Identity Manager Plus to receive the ID token. This token contains the user details required to complete the login process.
4. After verifying the signature of Identity Manager Plus in the ID token, the application retrieves the user details from the ID token.
5. Finally, after the successful verification of user details on the application's end, the user is logged in to the application.

Identity Manager Plus-initiated login

1. A user logs in to Identity Manager Plus successfully. They go to the Applications tab and click on the desired application.
2. In this case, Identity Manager Plus sends an ID token to the application directly.
3. After verifying the signature of Identity Manager Plus in the ID token, the application retrieves the user details from the ID token.
4. After the successful verification of user details on the application's end, the user is logged in to the application.

Supported Scopes

Scopes define the level of access that can be requested by the service provider to access a resource. These have to be enabled suitably by the Admin. Identity Manager Plus supports the following scopes:

- **openid**: Establishes that this is an OpenID Connect request. This is a mandatory scope for OpenID authentication request.
- **profile**: Requests the user's profile claims (FirstName and LastName).
- **email**: Requests the user's email attribute.
- **offline_access**: Requests the refresh token that can be used to receive new access tokens.

Supported applications

- Freshdesk
- Freshservice
- Okta
- PingOne
- Salesforce
- TalentLMS

Managing applications

This section explains how to assign, unassign, delete, and disable the added applications.

Assigning applications to users

1. Login to Identity Manager Plus as Administrator or Super administrator.
2. Go to the **Applications** tab.
3. Go to the row of the application you want to assign users to, and click the value under the column Assigned Users.
4. In the screen that appears, click the **Assign Users** button in the top-left corner.
5. Now, you can search for users and select them to assign the application.
6. Click **Assign** to save the settings.

Disabling and deleting applications

1. Login to Identity Manager Plus as Admin or Super Admin.
2. Go to the **Applications** tab.
3. In the row of the application you want to disable, click the icon.

4. To delete an application, click the icon. In the Confirm Box that pops up, click **Yes** if you are sure about deleting the application.

SCIM-based automated user provisioning

With the proliferation of cloud applications, it's imperative that enterprises ensure employees gain access to applications they need as soon as they join the organization or move to a new position, as well as have their access permissions revoked when they leave. System for Cross-domain Identity Management (SCIM) is an open standard that facilitates automated provisioning and deprovisioning of user accounts in cloud applications.

Identity Manager Plus supports SCIM-based automated user provisioning. It can be configured to automatically provision users to a cloud application when they're assigned to that application. For example, when users are imported from Azure Active Directory and assigned to the Slack application, user accounts will be automatically created for each of these users in Slack.

Identity Manager Plus supports two provisioning features:

- **Create user:** A new account will be automatically created in the cloud application when a user is assigned to that application in Identity Manager Plus. If there is an existing disabled account for that user, the account will be enabled.
- **Delete user:** Deletes or disables the user account in the cloud application when the user is deleted or unassigned from the application in Identity Manager Plus.

The following applications are supported for automated user provisioning:

- Bonusly
- Monday.com
- Peakon
- Pingboard
- Proxyclick
- ScreenSteps

- Slack
- Tableau Online
- ThousandEyes
- Velpic

Directory

The directory menu allows you to integrate directories with Identity Manager Plus and manage the users in those directories.

Important: When you sign up for Identity Manager Plus, a Zoho directory will be automatically created and added as the default directory. If you sign up using your enterprise's existing Zoho admin account, your enterprise's Zoho directory will be added as the default directory.

Users from the directories that you add, such as Azure AD or G Suite, will be added to the default Zoho directory, once your domains associated with those directories are verified. Click here to learn about domain verification.

Directory settings

Here you can add, modify, and delete directories.

- Adding an Azure Active Directory
- Adding a G Suite directory
- Adding Slack
- Adding Salesforce
- Adding Zendesk
- Modifying the directory settings

Adding an Azure Active Directory

1. Log in to Identity Manager Plus as an Admin or Super Admin.
2. Go to the **Directory** tab and click **Add Directory**.
3. Select **Azure Active Directory**.
4. Click **Authorize Identity Manager Plus**. You will be shown a couple of instructions on how to proceed.
5. Click **Proceed**. You will be redirected to the Azure AD login page.

6. Enter the **Email** address and **Password** of an account that has **Global Administrator permissions** and login.
7. Once you are logged in, you will be prompted to grant Identity Manager Plus access to user domain details from your Azure AD environment. Click **Accept**.
8. You will be redirected back to the Identity Manger Plus portal.
9. The Azure AD tenant is now integrated with Identity Manager Plus.

To import the users from your Azure AD tenant into Identity Manager Plus, use the Manage Users option.

Adding a G Suite Directory

1. Log in to Identity Manager Plus as an Admin or Super Admin.
2. Go to the **Directory** tab and click **Add Directory**.
3. Select **G Suite**.
4. Click **Authorize Identity Manager Plus**. You will be shown a couple of instructions on how to proceed.
5. Click **Proceed**. You will be redirected to the G Suite login page.
6. Enter the **Email** address and **Password** of an account that has **Super Admin role** and login.
7. Once you are logged in, you will be prompted to grant Identity Manager Plus access to your Google account. Click **Allow**.
8. You will be redirected back to the Identity Manger Plus portal.
9. The G Suite directory is now integrated with Identity Manager Plus.

To import the users from your G Suite directory into Identity Manager Plus, use the Manage Users option.

Adding Slack

1. Log in to Identity Manager Plus as an Admin or Super Admin.
2. Go to the **Directory** tab and click **Add Directory**.
3. Select **Slack**.
4. Click **Authorize Identity Manager Plus**. You will be shown a couple of instructions on how to proceed.

5. Click **Proceed**. You will be redirected to the Azure AD login page.
6. Enter your **Slack Workspace URL**.
7. Enter the **Email** address and **Password** of an account that has **Administrator role** and login.
8. Once you are logged in, you will be prompted to grant Identity Manager Plus access to content in the workspace. Click **Allow**.
9. You will be redirected back to the Identity Manger Plus portal.
10. The Slack workspace is now integrated with Identity Manager Plus.

To import the users from your Slack workspace into Identity Manager Plus, use the Manage Users option.

Adding Salesforce

1. Log in to Identity Manager Plus as an Admin or Super Admin.
2. Go to the **Directory** tab and click **Add Directory**.
3. Select **Salesforce**.
4. Enter your Salesforce Organization Name and Domain Name.

   Note: If you don't enter the Domain Name, you'll be redirected to the standard login page (https://login.salesforce.com) instead of your Salesforce domain's login page.
5. Click **Authorize**. You will be shown a couple of instructions on how to proceed.
6. Click **Proceed**. You will be redirected to the Salesforce login page.
7. Enter the **Username** and **Password** of an account that has **Administrator role.** Click **Log In**.
8. Once you are logged in, you will be prompted to grant Identity Manager Plus access to your Salesforce organization. Click **Allow**.
9. You will be redirected back to the Identity Manger Plus portal.
10. The Salesforce organization is now integrated with Identity Manager Plus.

To import the users from your Salesforce organization into Identity Manager Plus, use the Manage Users option.

Adding Zendesk

1. Log in to Identity Manager Plus as an Admin or Super Admin.
2. Go to the **Directory** tab and click **Add Directory**.
3. Select **Zendesk**.
4. Enter your Zendesk **Subdomain** name.

   Note: Your subdomain can be identified from your Zendesk account's URL: https://[yoursubdomain].zendesk.com.
5. Click **Authorize**. You will be shown a couple of instructions on how to proceed.
6. Click **Proceed**. You will be redirected to the Salesforce login page.
7. Enter the **Email** and **Password** of an account that has **Administrator role.** Click **Sign In**.
8. Once you are logged in, you will be prompted to grant Identity Manager Plus access to your Zendesk subdomain. Click **Allow**.
9. You will be redirected back to the Identity Manger Plus portal.
10. The Zendesk subdomain is now integrated with Identity Manager Plus.

To import the users from your Zendesk subdomain into Identity Manager Plus, use the Manage Users option.

Modifying directory settings

You might need to modify the directory settings for three reasons.

Reauthorization: If the user account you used to configure the directory has been deleted or the password has been changed, you must reauthorize the permissions required by Identity Manager Plus.

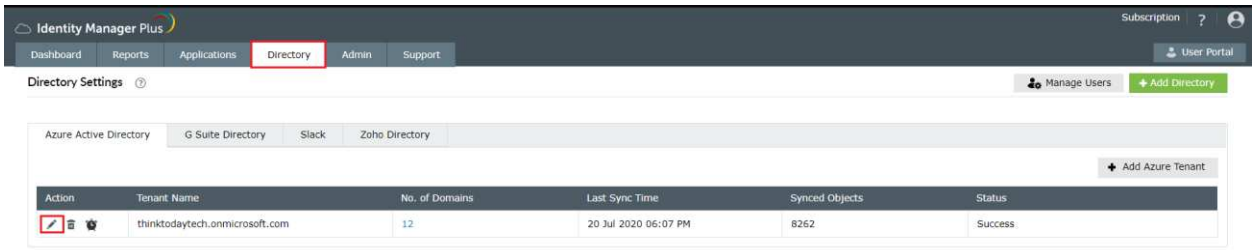
Sync directory settings: To synchronize objects between the directory services and Identity Manager Plus, and to update the status of users verified through domain verification, the directories need to be synced with

Identity Manager Plus. For example, during synchronization, any deleted user account in Azure AD or G Suite will be automatically removed in Identity Manager Plus.

Remove directory: If a directory is no longer in use or you have migrated to another directory, you can delete the unwanted directory. Removing a directory will remove all the licensed users from that directory and their licenses will be reclaimed.

To reauthorize a directory:

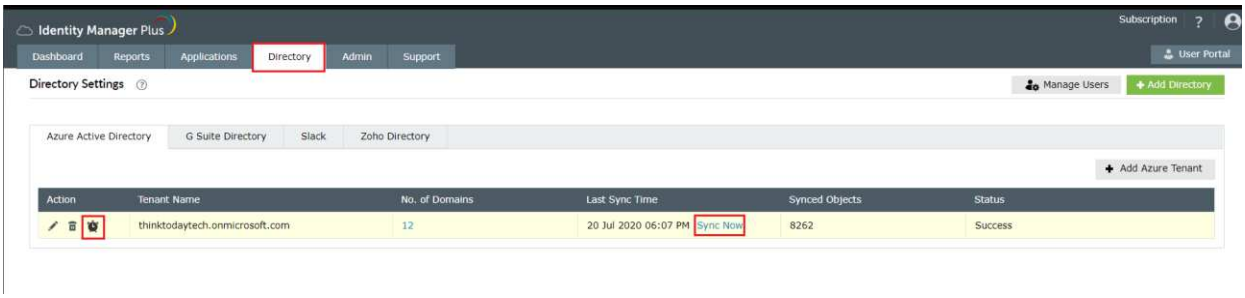
1. Log in to Identity Manager Plus as an Admin or Super Admin.
2. Go to the **Directory** tab.
3. Select the directory you want to modify.
4. You'll see a list of tenant or domain you've added from that directory type in a table.
5. Click the **edit icon** under the **Action** column corresponding to the tenant or domain you want to reauthorize.



6. Follow the authorization process again.

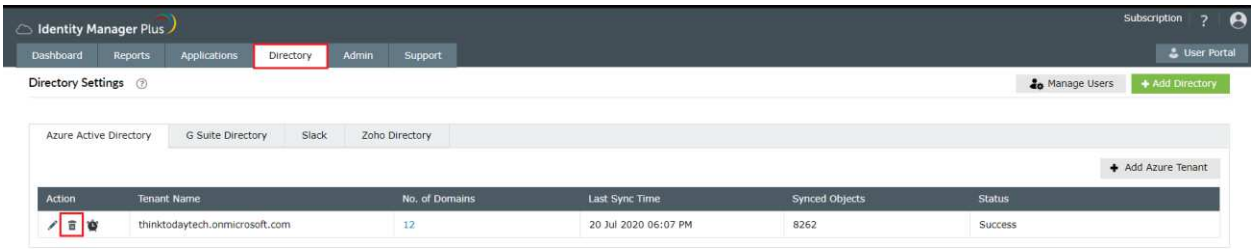
To synchronize objects

1. Log in to Identity Manager Plus as an Admin or Super Admin.
2. Go to the **Directory** tab.
3. You'll see a list of directories you've added in a table.
4. Click the **clock icon** under the **Action** column to schedule automatic sync.
5. Alternatively, hover the mouse over **Last Sync Time** column. Click the **Sync Now** link that appears to run the synchronization immediately.



To remove a directory:

1. Log in to Identity Manager Plus as an Admin or Super Admin.
2. Go to the **Directory** tab.
3. You'll see a list of directories you've added in a table.
4. Click the **delete icon** under the **Action** column.



User Management

Once directories are added to Identity Manager Plus, users from those directories can be added to the built-in directory of Identity Manager Plus. You can also disable, enable, or change users' roles.

- Adding users
- Managing users

Adding Users

To import users into the built-in directory, user accounts need to verified.

There are two ways to verify users and import them into the built-in directory:

- **Adding and verifying a domain:** In this method, you need to add and verify your domains associated with the directories that are integrated with Identity Manager Plus. Once the domains have been verified, users in those directories will be automatically added to the built-in directory.
- **Sending email invitation:** In this method, you send an email inviting users to activate their Identity Manager Plus account. Once they accept the invitation by clicking on the link in the email, they will be added to the built-in directory. This method can also be used to import users from any directory service including on-premises Active Directory.

Only when the users are verified, they will be added into the built-in directory, and applications can be assigned to them.

Adding and verifying a domain

Domain verification is an essential step to ensuring that the domain associated with your directories is valid (not expired), and that the user who added the domain has the required privileges to sync users in that particular domain with Identity Manager Plus. This step ensures that the domain is not a spoofed domain, and prevents any loss of service due to the misuse of domain names. You can choose from two different verification methods:

- **CNAME Method:** Add a unique 'CNAME' record in the domain's DNS Manager.
- **HTML Method:** Upload the given HTML file under the root of your website.

To add and verify a domain:

1) Go to the **Directory** tab.

2) Click **Manage Users**.

3) Click the **Verified/Unverified Domain** link at the top-right corner.

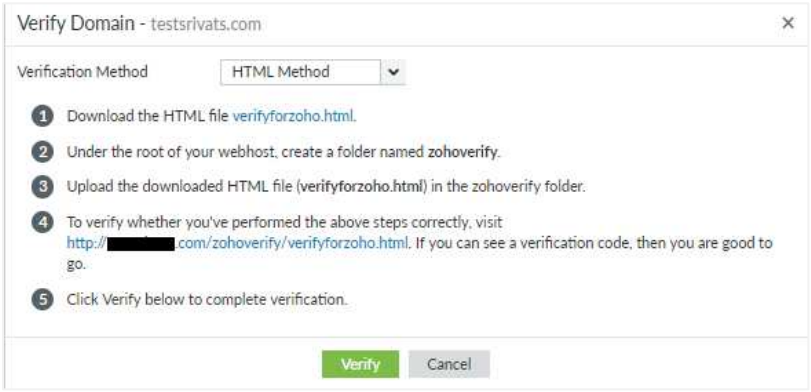
4) Click **Add Domain**.

5) Enter the **Domain Name** and click **Add Domain**.

6) The domain will be listed in a table with its details.

7) Under the **Status** column, click the **Click to Verify** link.

8) Select a **Verification Method** from the drop-down.



 # CNAME Method

I. Copy the CNAME code.

II. The code generated (which follows the format zb*****) is different for each domain added in Identity Manager Plus.

III. Log in to your account where your domain's DNS is hosted.

IV. Open your Domain Management Page to update the DNS Records.

V. Locate the option to add CNAME records. (Generally found under DNS Records. You can also consult the help page of your registrar.)

VI. In the Name/ Host/ Alias/ CNAME, add the CNAME code zb*****.

VII. In the Value/ Points To/ Destination field, add “domain.zoho.com”.

VIII. Click Save.

 # HTML Method

I. Download the HTML file verifyforzoho.html.

II. Under the root of your webhost, create a folder named “zohoverify”.

III. Upload the downloaded HTML file (verifyforzoho.html) in the zohoverify folder.

IV. To verify whether you've performed the above steps correctly, visit http://sree.zoho.com/zohoverify/verifyforzoho.html. If you can see a verification code, then you are good to go.

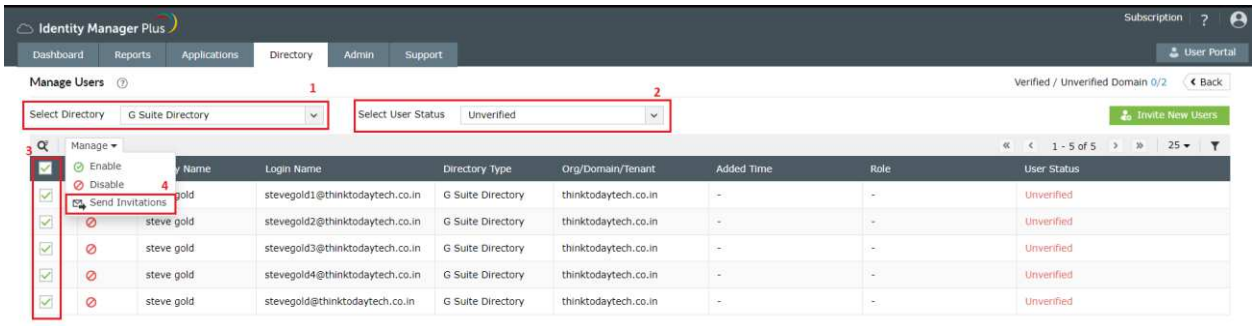
9) Click **Verify** to complete verification.

Important: Once the domain is verified, make sure you sync the directories with the built-in directory of Identity Manager Plus. Only after directory sync, users’ status will be changed to Verified in Identity Manager Plus, and they can start using its service.

Sending invitation emails to users

To invite users through email:

1) Go to the **Directory** tab.
2) Click **Manage Users**.
3) Select a directory from the **Select Directory** drop down.
4) From the **Select Users Status** drop down, select **Unverified**. A list of users who have not been verified will be displayed in a table.
5) Select all users or the users you want to import into Identity Manager Plus.
6) From the drop-down box at the top of the table, select **Send Invitation**.



To import users from other directories such as on-premises Active Directory,

1) Go to the **Directory** tab.
2) Click **Manage Users**.
3) Click **Invite Users**.
4) Enter the **Email Address, First Name, Last Name,** and **Role** of the user.
5) Click **Send Invite**.

An account will be created in the built-in directory of Identity Manager Plus for all the invited users who accept the invitation.

To view the list of invited users:

1) Go to the **Directory** tab.
2) Click **Manage Users**.
3) Select a directory from the **Select Directory** drop down.
4) From the **Select Users Status** drop down, select **Invited.**
5) You can re-invite a user or cancel an invitation. If you choose to re-invite a user, an invitation will be sent again. If you choose to cancel an invitation, the invitation email that was sent will be invalidated and can no longer be used.

Activating the accounts of end users

Users who received an invitation email need to activate their account by clicking on the link in the email and by entering their details and setting a password for their account. Once they do, an account will be created for them in the built-in directory of Identity Manager Plus.

Users whose accounts were activated automatically through domain verification can log into Identity Manage Plus using their directory credentials. However, domain-verified users need to set their passwords to be able to login using their account in the built-in directory of Identity Manager Plus. To set their passwords, they can go to https://accounts.zoho.com.

Managing Users

Users added to Identity Manager Plus can be enabled, disabled, or have their roles changed. To learn more, click the respective links below:

- Enabling or disabling users
- Changing a user's role

Enabling or disabling users

You can enable or disable users from Identity Manager Plus. Disabling a user will block them from accessing the applications assigned to them. However, details of the applications assigned to the user will still be retained. You can enable the user to reinstate their access at a later point.

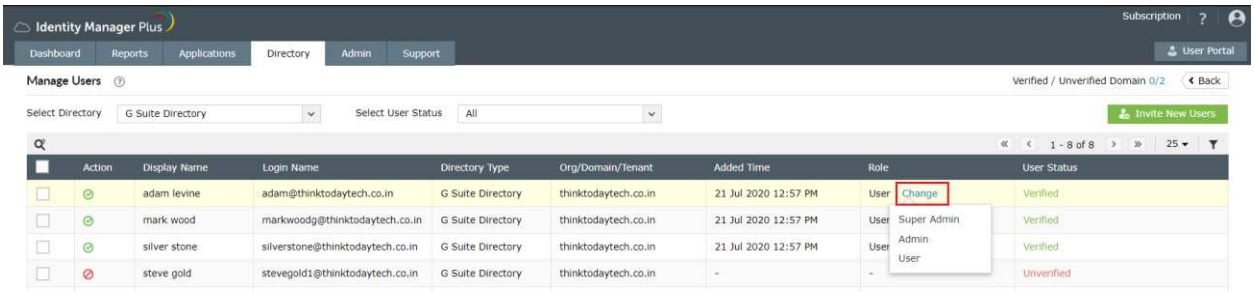
To manage users:

1. Log in to Identity Manager Plus as an Admin or Super Admin
2. Navigate to **Directory**, and click **Manage Users**.
3. Select the directory, and then, the users you want to enable or disable.
4. In the **Manage** drop-down at the top of the table, select **Enable** or **Disable** based on the action you want to perform.

Changing a user's role

User roles play an important role in determining what privilege a user has inside Identity Manager Plus. To change a user's role:

1. Select a user and hover the mouse under the **Role** column of the respective user.
2. A **Change** link will appear.



3. Click that link and select a role.

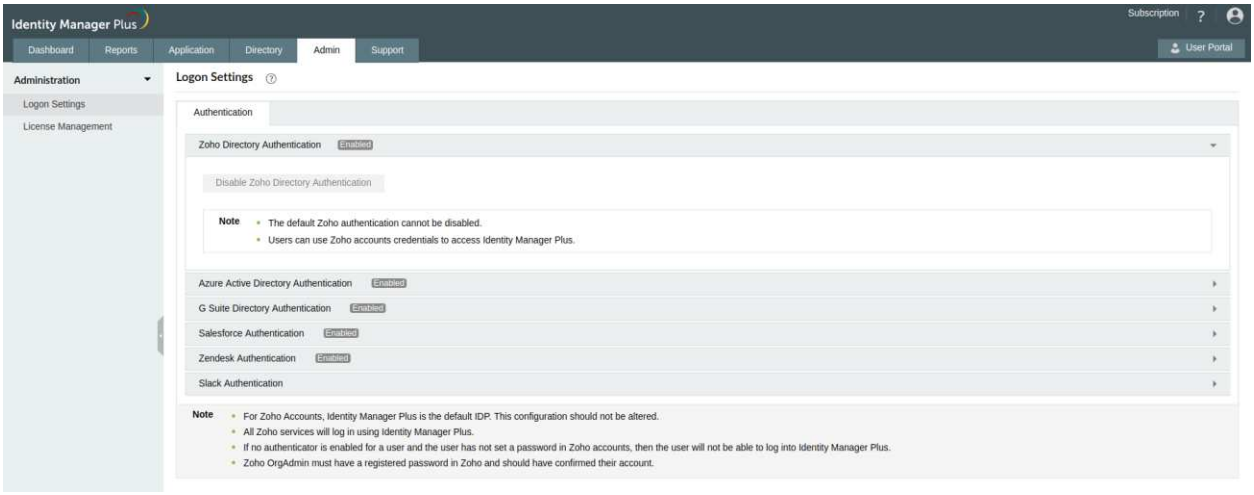
Note: There must always be at least one user assigned the Super Admin role.

Admin

The admin tab contains the logon settings and license management menus.

Configuring Logon Settings

The logon settings determine how users can log into Identity Manager Plus. Users can log in using either their Zoho credentials, which they created during account activation, or any of the directory credentials form which they were imported.



Zoho Authentication

Users who activated their account using the invitation email can use Zoho Authentication to log into Identity Manager Plus.

For Zoho Authentication:

1) Users need to enter their email address and click *Click to Login* in the login page.

2) In the next page, they will be displayed all the authentication methods enabled for them.

3) If they select Zoho Authentication, they will be asked to enter their password.

Directory Authentication

Users can use their existing directory accounts to log into Identity Manager Plus. For example, a user imported from Azure AD can log into Identity Manager Plus by logging into Azure AD.

For Directory Authentication:

1) Users need to enter their email address and click *Click to Login* in the login page.

2) In the next page, they will be displayed all the authentication methods enabled for them.

3) Users need to select the directory they want to use for authentication. They will be redirected to the directory's login page. Once successfully authenticated, they will be redirected to Identity Manager Plus and logged in automatically.

To enable an authentication method:

1) Go to the **Admin > Logon Settings > Authentication**.

2) Click on an authentication method.

3) Toggle the button to **Enabled**.

Note:

i) Only directories integrated with Identity Manager Plus can be enabled for authentication.

ii) To use a particular directory for authentication, a user must have been added from that specific directory into Identity Manager Plus. For example, Azure AD Authentication can be enabled only for users who were imported from Azure AD into Identity Manager Plus.

License Management

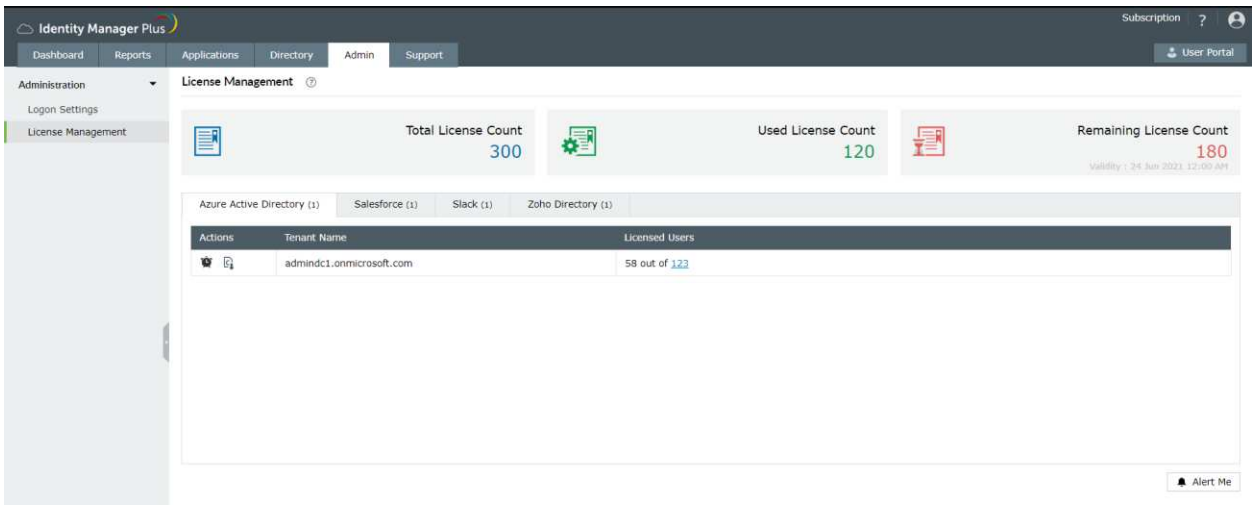
Identity Manager Plus is licensed based on the number of users. If you want to add a number of directories to Identity Manager Plus, but don't want all the users in those directories to access Identity Manger Plus, you can use the License Management option to assign licenses to only those users who need them, and thus save on license cost. This option allows you to assign licenses to or reclaim licenses from users based on your requirements.

To view the license usage:

1) Go to **Admin > License Management**.

2) The License Management screen displays the following information:

- **Total License Count**: This shows the number of licenses you have purchased.
- **Used License Count:** This shows the number of users who are consuming the license.
- **Remaining License Count:** This shows the number of unused licenses.



Assigning or reclaiming license

To assign a license or reclaim a license from a user, you need to configure the licensed users list.

Licensed Users: Users who have a valid license assigned to them.

Unlicensed Users: Users who don't have a valid license assigned to them, and hence, cannot access Identity Manager Plus.

To assign or reclaim license from users:

1) Go to **Admin > License Management**.

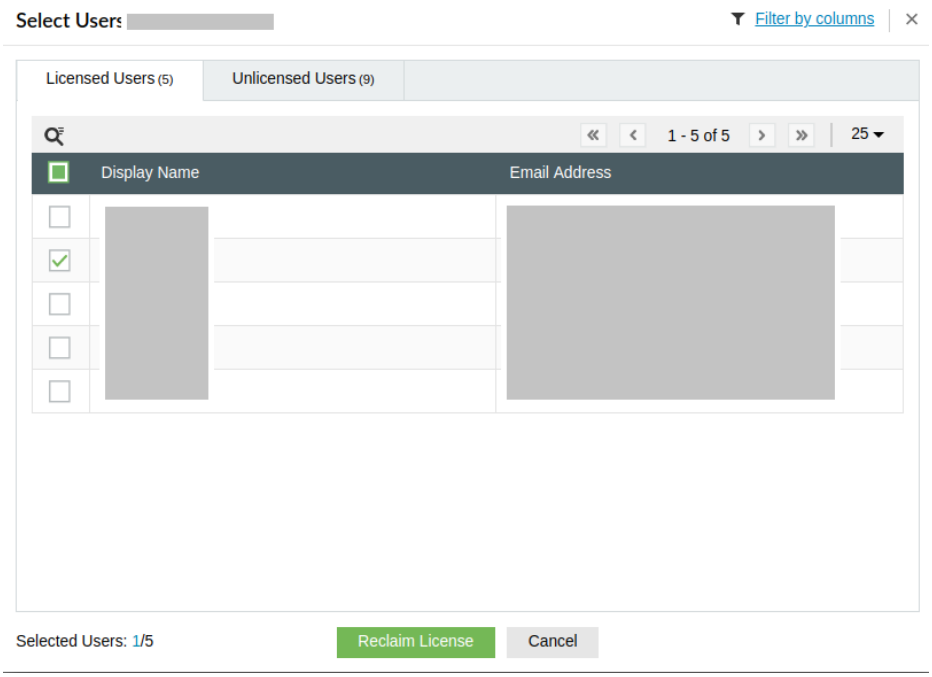
2) Select the directory you want to modify.

3) Under the **Licensed Users** column in the table, hover the mouse over the values.

4) Click on **Assign License** or **Reclaim License** as per your requirement.

5) There is also a **CSV Import** option under the **Actions** column, to assign or reclaim license from multiple users.

6) **To view the exact list of Licensed Users or Unlicensed Users,** click the **total users value** in the **Licensed Users** column. This will open a pop-up.



a. The entire list of Licensed Users and Unlicensed Users will be displayed under the respective tabs.

b. To reclaim license, select the users from the Licensed Users tab and click Reclaim License.

c. To assign license, select the users from the Unlicensed Users tab and click Assign License.

7) To automatically assign or reclaim licenses, enable the **Schedule** option under the **Actions** column.

a. Click the Schedule icon under the Actions column.

b. Select the **Enable Scheduler to manage licenses automatically** checkbox.

c. Configure the time period for the scheduler to run.

d. Under the Assign License and Reclaim License tabs, **set up criteria** as per your requirements. For example, you can configure a scheduler to reclaim licenses from users who have remained inactive for the past 30 days.

e. Click **Save** to save the scheduler, or **Save & Run** to save the scheduler and run it once immediately.

Note: The criteria configured under the Reclaim License tab will be applied first followed by the criteria configured under the Assign License tab.

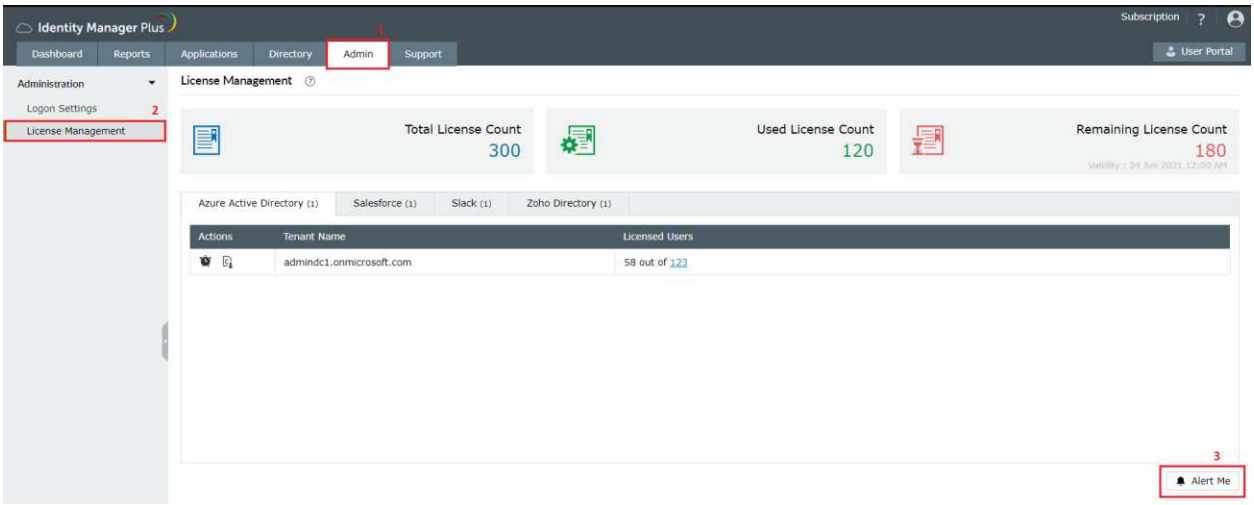
Configuring license notifications

The Alert Me option found at the bottom of the Manage License page contains settings to notify you when the license is about to expire or the license limit is about to be reached. This will help you proactively renew or upgrade your license so that end users are not prevented from accessing Identity Manager Plus.

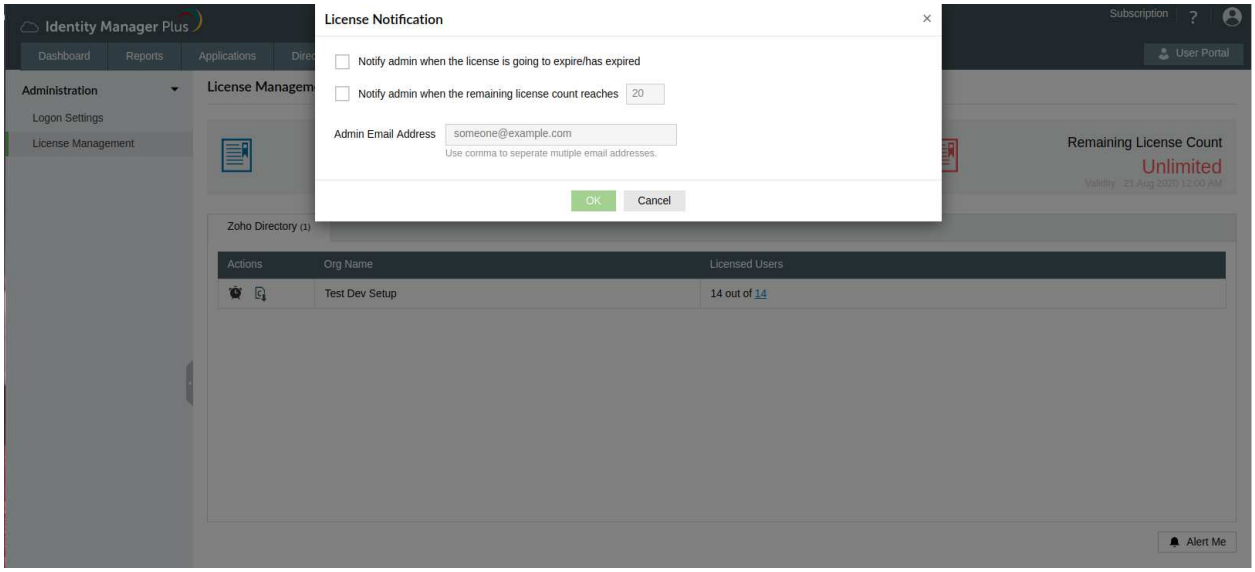
To configure license notifications:

1) Go to **Admin > License Management**.

2) Click on the **Alert Me** button present at the bottom-right corner of the page.



3) Enable the notifications as per your requirement.



a. **Notify admin when the license is going to expire/has expired:** When enabled, you will receive a notification when the license is about to expire. You can configure when exactly the notification is to be sent by entering the number of days before license expiration.

b. Notify admin when the remaining license count reaches: Enter a value in the box to receive a notification when the Remaining License Count reaches the entered value.

4) Enter the **Admin Email Address** to which the notifications are to be sent. If you want the notifications to be sent to multiple users, enter their email addresses separated by a comma.

5) Click **OK**.

Managing Subscription

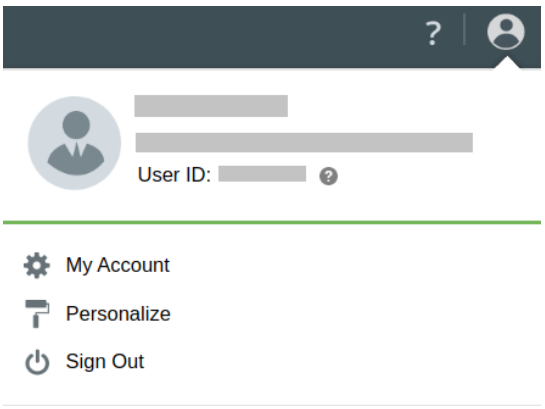
The subscription menu shows your current subscription plan, how long the subscription is valid, the total number of users included in your subscription, and how many users you currently have in Identity Manager Plus.

To upgrade or modify your subscription plan, click **Upgrade**.

To cancel your subscription, click **Close Account**.

Account Settings

You can modify your profile information, security settings, two-factor authentication options, and more using the **My Account** option available under the user profile in the top-right corner.



Support

If you have any questions or need technical assistance, contact support@identitymanagerplus.com or call +1-408-916-9890.

About Identity Manager Plus

Identity Manager Plus is a cloud-based, single sign-on (SSO) solution for enterprises. It provides end users secure, one-click access to their applications, allows admins to centrally manage access to applications, and delivers deep insights into application usage and accesses.

Get Quote | Start Free Trial | Personalized Demo