Foxit Admin Console Administrator Guide

Microsoft Partner
Gold Independent Software Vendor (ISV)

Anti-Grain Geometry - Version 2.4

Contents

About Foxit® Admin Console™ Administrator Guide

This guide covers features and functions that are only available to administrators.

Foxit Admin Console Overview

Foxit Admin Console add-on is a Cloud-based portal that serves as a central location for administrators to manage Foxit products/services and entitled users across their entire organizations. After setting up and activating Admin Console based on the organization environment, the administrator can open the URL provided by Foxit and sign up an account to get started. The Admin Console allows administrators to do the following:

- View the summary of the licenses and products
- Configure the license keys
- Assign license keys to users
- Manage Foxit products
- Configure the internal update of packages (on-premise environments only)
- Configure mail server
- View the detailed reports on the uses and statistics of Foxit products
- Customize enterprise brand information
- View the administrator's action logs

Set up and activate

Foxit Admin Console can be deployed on AWS and hosted by Foxit (i.e. single-tenant), or located on the Enterprise's servers and available through an internal network (i.e. on-premise) and entirely maintained by the enterprise's staff. Single-tenant (Foxit-hosted) Admin Console is ready to use after the enterprise receives our email that contains the Admin Console URL and other configured information. For an on-premise Admin Console, the enterprise needs to deploy its on-premise environment, for which we provide the related deployment documentation and instructions in our email after your purchase of Foxit Admin Console.

After the deployment of the Admin Console, client configuration is required. The documentation and instructions on client configuration are also included in the email sent by Foxit.

When everything is ready, you (the enterprise administrator) need to activate Admin Console before getting started. To activate, do the following:

1. Open your web browser and visit the Admin Console URL. (For a single-tenant Admin Console, the URL has been provided in the email from Foxit after you purchased Foxit Admin Console. In an on-premise environment, the URL is created by your company during the deployment of Foxit Admin Console.)
2. Sign up an account and log in. ***Note**: For the account you signed up, if the email is the same with that of an SSO account (your LDAP or SAML account), you will need to use the SSO credential to log in after you set up LDAP or SAML in the Foxit Admin Console.*
3. There are two methods of activation: **Online Activation** and **Offline Activation**.
   - **Online Activation** requires an internet connection, and you can click **Connect** and activate by logging in to the account you purchased Foxit Admin Console with.
   - If your computer is offline, you need to complete an Offline Activation with your purchased license key file by clicking **Browse**. (If you haven't got a key file yet, click **Get One**. Then you will obtain the server ID of the Admin Console in the pop-up dialog box. You need to send the server ID to Foxit by email and Foxit's team will send the key file to you later.)
4. After successful activation, click **Get Started**. Then a wizard (a small green message box with on-screen instructions) for some items in Admin Console prompts to help you get started. There are a series of items in the left part of the Admin Console window, including **Dashboard**, **User ID Management**, **License Management**, **Mail Servers**, and more. Select an item or a sub item to open the associated page on the right side and do the settings as needed.
5. (Optional) To log out of your Foxit Admin Console, move the cursor over the administrator avatar in the top-right corner of the Admin Console window and a menu drops down. Click the **Log Out** command in the menu to log out.

Dashboard

The Dashboard displays the summary of data such as product licenses and users, which allows you to take a glance at the usage of Foxit products plans within your organization. To view the report for the number of assigned and activated licenses, you can choose **Last 7 days** or **Last 30 days** to display the data only for the latest week/month. The Dashboard also shows the enterprise data including the number of employees, groups, and logged-in users.

User ID Management

Depending on the requirements or circumstances in your enterprise, you may manage users (and groups) individually or in batch by uploading CSV files in the Admin Console, or by connecting Admin Console to your enterprise account system (user directory system) by configuring Single Sign-On.

Directory settings

Single Sign-On (SSO) is a session and user authentication service that permits a user to use one set of login credentials (e.g., the authenticated user ID and password provided in a company) to access multiple applications. Currently, Foxit Admin Console supports two popular SSO methods: LDAP and SAML. After you set up LDAP or SAML in Foxit Admin Console for performing Single Sign-On, all users in your company can directly sign in with their authenticated accounts to access Foxit applications.

To connect Admin Console to an LDAP or an SAML directory, you need to configure the user directory first in the **Directory setting** page under **User ID Management**.

Manage users with LDAP

LDAP, Lightweight Directory Access Protocol, is an Internet protocol that email and other programs use to look up information such as users, from an LDAP server. An LDAP directory stores a collection of data about users and groups.

For companies that use LDAP to store employee information, follow the steps below to connect Foxit Admin Console to an LDAP directory for authentication, user and group management.

1. Click **Add directory** in the **Directory setting** page.
2. Enter the values for the LDAP user directory settings.

Server Settings:

Setting	Description
Name	Enter a name to help you identify the LDAP directory server, such as “Company Staff Directory” or “Company Corporate LDAP”.
Directory Type	Select the type of LDAP directory that you will connect to.
Hostname	Enter the host name of the server running LDAP, such as “ldap.example.com”.

Port	The port your LDAP directory server is listening on, such as “389”.
Use SSL	If the connection to the directory server is an SSL (Secure Sockets Layer) connection, select this option. And you will need to configure an SSL certificate to use this setting.
Username	Enter the name of the user that will log in to LDAP. Here are some examples: • cn=user, dc=domain, dc=name • user@domain name
Password	Enter the password of the user.

LDAP Schema:

Setting	Description
Base DN	The Root node in an LDAP directory server when searching for users and groups from the server, such as “cn=users, dc=example, dc=com”.

User Schema Settings:

Setting	Description
User Object Filter	The attribute field to use when loading the username. Examples: • cn • sAMAccountName
User Name Attribute Field	The attribute field to use when loading the username. Examples: • cn • sAMAccountName
User DN Attribute Field	The attribute field to use when loading the user’s distinguished name. Examples: • entryDN • distinguishedName
User First Name Attribute Field	The attribute field to use when loading the user's first name, such as “givenName”.
User Last Name Attribute Field	The attribute field to use when loading the

	user's last name, such as “sn”.
User Display Name Attribute Field	The attribute field to use when loading the user's full name, such as “displayName”.
User Email Attribute Field	The attribute field to use when loading the user's email address, such as “mail”.

Group Schema Settings:

Setting	Description
Group Object Filter	The filter to use when searching for group objects, such as “(&(objectClass=group)(cn=*))”.
Group DN Attribute Field	The attribute field to use when loading the group’s distinguished name. Examples: • entryDN • distinguishedName
Group Name Attributes	The attribute field to use when loading the group's name, such as “cn”.
Group Description Attribute Field	The attribute field to use when loading the group's description, such as “description”.

Membership Schema Settings:

Setting	Description
Group Members Attribute	The attribute field to use when loading the group’s members, such as “member”.
User Membership Attribute	The attribute field to use when loading the user's groups, such as “memberOf”.

3. After configuration, click **Save** to apply the LDAP directory settings. (Or click **Reset** to clear all the data you input in the settings above.)
4. You can see the configured LDAP directory has been successfully added to the directories list. You can add more directories as needed after clicking the **Add directory** button above the directories list.
5. (Optional) In the **Action** column, you can do any of the following:
    - Disable or enable an LDAP directory by clicking **Disable** or **Enable**. After an LDAP directory is disabled, a “(inactive)” suffix will be added to the directory name and you can click **Remove** to delete the directory as needed. ***Tip****: To disable or enable one or more LDAP directories, you can select them and click the* ***Disable*** *or* ***Enable*** *button above the directories list.*

- Modify the LDAP directory information after clicking **Edit**.
- Click **Test** to test the connection to the selected LDAP directory by logging in. In the pop-up dialog box, enter the email and password of a user in the LDAP directory and click **Test Settings**. And then you will be prompted the login is successful, which means the LDAP connection is successful.
- Click **Sync now** to synchronize the LDAP directory immediately. The **Status** column shows the last synchronization of the directories. ***Tip****: You can also specify how often LDAP directories are synchronized. To do this, select one or more directories, click the* ***Synchronize*** *button above the directories list, and then a list box appears next to the button. From the list, select* ***Now*** *or set a specific time every day/week/month/year, and click* ***OK****.*

6. (Optional) If you have added multiple directories, you need to define the directory order by clicking the yellow up and down arrows next to each directory. If the same user exists in multiple directories, the user can only use the credentials (password) of the first occurrence in the directories when logging in.

Manage users with SAML

SAML, Security Assertion Markup Language, is an open standard for exchanging authentication and authorization data between parties, in particular, an identity provider and a service provider. SAML single sign-on allows your users to log in using your organization's identity provider to access all your Foxit applications.

This section describes how to set up SAML single sign-on.

1. The SAML configuration requires the user's username and email attributes to be configured in your identity provider. Follow the on-screen instructions to add the user attributes to your identity provider.
2. Click **Add SAML configuration**.
3. After adding your identity provider details to the "Directory setting" page in the Admin Console, you'll see new fields and values (about Service Provider's Entity ID and Assertion Consumer Service URL) appear. Copy those values and paste to your identity provider.
4. Copy your identity provider details to the following fields, and then click **Save configuration**.

Field	Description
Identity provider Entity ID	The URL for your identity provider where Foxit applications will accept authentication requests.
Identity provider SSO URL	The URL your users will be redirected to when logging in.

Public x509 certificate	The value for this field begins with '-----BEGIN CERTIFICATE-----'. The certificate contains the public key Foxit applications use to verify that your identity provider has issued all received SAML authentication requests.

5. If you need to edit the SAML configuration or if your company doesn't want to configure SAML for single sign-on, click **Edit Configuration** to edit the configuration settings, or click **Delete Configuration** to remove the SAML configuration.
6. Do the following steps for SAML user Sync Configuration.
   1) Select a connector and then follow the on-screen instructions to enter details for the connector settings.
   2) After complete settings, click **Authorize**.
   3) Click Sync Users next to the connector to synchronize user data.

Users

After you have successfully connected Foxit Admin Console to your account system, you can add, search, and manage user accounts in the **Users** page. These user accounts entitle the end users in your organization to Foxit applications.

The **Users** page contains three tabs: **Directory users**, **Added users**, and **Unsynced from Directory**.

User management with LDAP

The Directory users tab

All users listed in this tab are from the LDAP directories you configured. On the left side, the hierarchical structures of the LDAP directories in your enterprise are displayed in a tree view. Select a group in the LDAP directory, and all the users in that group are listed on the right side. You can search for a user by entering the user's name or email address in the Search box and clicking the **Search** icon.

You can view and edit details of each user after clicking the **View details** icon in the **Action** column. In the details page, do any the following:

- **Edit Details**: edits the user name.
- **Disable**: disables the user account to not allow the user to log in to access Foxit applications.
- **Back**: returns to the user list.

The Added users tab

For some users who are not in your account system and request access to Foxit applications, you can add them manually in the **Added users** tab.

- To add users, click the **Add user** button above the user list to open the drop-down list. Then do either of the following:
  - Choose **Add a user** to add one user.
  - Choose **Add users by CSV** to add multiple users by uploading a CSV file that contains the user accounts.
  - Choose **Bulk operation results** to show the results after adding users by CSV. If any users are not added successfully, they will be displayed in the results.
- To export users to a CSV file, select the users you need by checking the boxes next to the users and click the **Export Users** button above the user list. If no users are selected, clicking **Export Users** exports all users in the list automatically.
- To remove users from the Admin Console and revoke their licenses, select the users and click the **Remove** button above the user list.
- To search for a user, enter the user's name/email address, select a type of the account status (whether their licenses are available or revoked), or specify the time period the users logged in, and then click **Search**. Click **Clear** to remove the information you entered or selected, after which you can start a new search.
- Click the **Revoke** icon in the **Actions** column to remove the license from the user. Once the license is revoked, the user becomes unable to activate products by logging in with their accounts until they are assigned licenses again, and the **Revoke** icon in the **Actions** column changes to the **Access** icon. Click the **Access** icon to assign a license to the user again.
- Click the **Details** icon in the **Actions** column to view the details of the user and then do any of the following:
  - Click **Remove** to remove the user from Admin Console.
  - Click **Set Password** to change the password for the user account.
  - Click **Revoke** to remove the license from the user, or click **Access** to assign a license to the user.

The Unsynced from Directory tab

The LDAP user directories are synchronized regularly to ensure the user data in the Admin Console is most up-to-date. After synchronization, the unsynchronized users who may have left your organization will be listed in the **Unsynced from Directory** tab. To search for a user in this tab, enter the user's name/email address in the text boxes or select the license status (whether the user was authorized or not), and click **Search**. To delete a user, select the user and click **Delete**.

User management with SAML

The Directory users tab

The **Users** tab lists all users in the SAML directories in your organization and shows the details including the user email and the activation status. You can perform the following tasks:

- Select a user and click the **Edit** icon in the **Action** column to edit the user name.
- Select a user and click the **Revoke** icon in the **Action** column to disable the user. After an account is deactivated, the user will not be able to log in with the account anymore.
- Search for a user by specifying the user's name/email address or the type of the account status (whether the license is available or revoked) above the user list and clicking **Search**. Click **Reset** to remove the information you entered or selected, after which you can start a new search.

You can also export users to a CSV file using the **Export Users** button. If no users are selected, clicking **Export Users** exports all users in the list automatically.

The Added users tab

See also the **Added users** tab in the **User management with LDAP** section.

The Unsynced from Directory tab

See also the **Unsynced from Directory** tab in the **User management with LDAP** section.

Groups

You can manage multiple users in groups, such as departments and project teams, without having to specify and apply your configuration to each user individually. In the **Groups** page, you can create and manage groups.

To create a group, do the following:

1. Click **Create Group**. Type the name and description for the group in the pop-up dialog box, and click **Next**.
2. Select a user in the **User List** box, and click the sign next to the user's email address. Then the user will be added to the **Added Users** box, and the sign next to the user's email address in the **User List** box changes into the sign. Repeat until you add all users you want to add.

3. (Optional) in the **Added Users** box, put your cursor over a user's email address, and the ⊗ sign appears. Click the ⊗ sign to remove the user from the **Added Users** box, if needed.
4. Click **Save**. The group will be added to the groups list.
5. (Optional) Click on the icons in the **Actions** column to perform the following tasks as needed:

    - To delete the group, click the **Delete** icon.
    - To view user list in the group, click the **View users** icon in the corresponding group.
    - To edit the group, click the **Edit** icon. You can edit the group's name/description, and add/remove users in the group.

Do any of the following to manage groups:

- To export groups of users to a CSV file, select the group(s) you need and click the **Export Users** button above the groups list.
- To remove groups, select the groups and click the **Delete** button above the groups list.
- To search for a group, enter the group's name or specify the time period when the group is created, and then click **Search**. Click **Clear** to remove the information you entered or selected, after which you can start a new search.

Customize Organization

All users in Foxit Admin Console, including LDAP/SAML users and added users, belong to an organizational unit (or "OU" for short). In the **Customize Organization** page, administrators (except sub-administrators) can create and manage departments for their organizational units. And the super administrator can set department admins (i.e. sub-administrators) to manage the members, licenses, and settings for that department. See also Admin Role Management. This feature is useful for an organization that is divided into smaller departments or sub-organizations that work independently, such as a university with different colleges.

If you are the super administrator or a general administrator, click on the OU name in the left part of the **Customize Organization** page, and all users are listed on the right. The default name of the OU is the company name provided when you purchase Foxit Admin Console. You can edit the OU name the same way you edit department names (described below). To create a department under the OU as a child, do the following:

1. Click the **Add Department** button in the left part of the page, where all the

departments are listed. Or move the cursor over the vertical three-dot icon next to any department, and choose **Add Department**. (***Note**: Before adding departments, make sure you have connected to your LDAP or SAML directories or added users in the **Users** page.*)

2. In the pop-up dialog box, enter the department name and select a parent department that the new department will be listed below as a child department. Click **OK** to continue.
3. Then the new department will be listed in the department list. Click on the department and click **Add members** in the right part of the page.
4. In the pop-up dialog box, select a user in the **User List** box, and click the sign next to the user's email address. Then the user will be added to the **Selected user** box, and the sign next to the user's email address in the **User List** box changes into the sign. Repeat until you add all users you want to add. ***Tip**: You can add all the users in a group of your LDAP or SAML directories by clicking the sign next to the group in the **Directory users**.*
5. (Optional) In the **Selected user** box, put your cursor over a user's email address, and the sign appears. Click the sign to remove the user from the box, if needed.
6. When you're done, click **OK**. You can click the **Add members** button to add more users to the department if needed.

After creating a department, the super administrator or a general administrator can perform more actions:

- To edit a department name or delete a department, move the cursor over the vertical three-dot icon next to the department, and choose **Edit Department** or Delete.
- To remove a user from a department, select the department, navigate to the user and click the **Delete** icon in the **Actions** column. To remove multiple users, select the users by checking the boxes in front of the user name and click the **Delete** button above the user list.
- To move users to other departments, select the users and click the **Move to** button above the user list. In the pop-up dialog box, select the desired department and click **OK**.
- To adjust the order of the departments, drag the department you want to move to the desired place. You can also put a department under another department (the parent department). For example, to put Department A under Department B, drag Department A onto Department B and release the mouse button when the pointer is directly over Department B.

If you are a sub-administrator:

- You can see an assigned OU displayed in the left part of the **Customize**

Organization page, which only contains the departments assigned by your super administrator. The assigned OU's name is specified when the super administrator assigns the OU. See also Add a sub-administrator.

- Any changes to the department (including changing the department name and adding/deleting department members) made by the super administrator will be synched into the departments in the assigned OU.
- You are allowed to add users to the departments in the assigned OU. For details on how to add users, see also the **Added users** tab in the **Users** section. The users you add will also be synced into the OU managed by the super administrator. And you are allowed to delete a user you added by clicking the **Delete** icon in the **Actions** column.

License Management

Foxit Admin Console supports **Account Mode** for you to perform license management in your organization. **Account Mode** is a licensing mode that enables each end user to activate Foxit applications once they log in to their accounts, and allows administrators to apply precise and flexible control such as who are allowed to activate the application and what application they can activate.

***Notes**:*

1. *Only the clients whose IP addresses and MAC addresses are in the specified ranges are allowed to activate Foxit applications. See also Client Activation Policy.*
2. *When assigning licenses, you will be prompted if the number of licenses you want to assign exceeds the number of purchased licenses.*

Manage Licensing

In the **License Management** page, you can assign/change/unassign licenses, and view the details of assigned users. (***Tip**: You can click the **Columns** button above the user list to specify what details to be displayed in the list of assigned users, including users' email addresses, licenses, activation status, assigned time, MAC addresses, and more.*)

You can specify criteria to search for specific users. To export users to a CSV file, select the users you need and click the **Export** button above the user list.

Assign licenses to users

1. Click the **Assign License** button. Choose **Assign License** to select users and assign licenses to the selected users.
2. In the pop-up dialog box, select a user in the **User List** box, and click the sign

next to the user's email address. Then the user will be added to the **Selected user** box, and the sign next to the user's email address in the **User List** box changes into the sign. Repeat until you add all users you want to add. ***Tip****: You can add all the users in a group of your LDAP or SAML directories by clicking the sign next to the group in the* ***Directory users****.*

3. (Optional) in the **Selected user** box, put your cursor over a user's email address, and the sign appears. Click the sign to remove the user from the **Selected user** box, if needed.
4. Select the license you want to assign to the selected users.
5. (Optional) Enterprises are enabled to purchase licenses that allow a user to activate Foxit products in multiple devices. For this type of licenses, the **Number of allowed devices** item appears in the dialog box, allowing you to specify the number of the devices that are allowed to log in.
6. Click **OK**.

You can also assign licenses to multiple users with a CSV file by doing the following:

1. Click the **Assign License** button. Choose **Assign licenses with CSV file** to assign licenses to user listed in a CSV file.
2. In the pop-up dialog box, drag a CSV file to the box or click **Browse** to select a CSV file. The CSV file includes the users you want to assign licenses to and the corresponding licenses for each user. How to create the CSV file, click **Download the sample CSV file to see the required format** for reference.)
3. Click **Assign**.

Change product licenses for users

To change the product license for a user, click the sign in the Actions column. In the pop-up dialog box, select a desired product license and choose **Save**.

Unassign licenses from users

Select the users you want to unassign licenses from and click the **Remove License** button above the user list. Optionally, you can unassign licenses from multiple users with a CSV file. When a license is unassigned from a user, the user will no longer be able to activate Foxit applications by logging in with their accounts.

Restore activation

If an end user has activated Foxit products successfully in Device 1 and needs to activate the products in Device 2 for some reason (maybe Device 1 is broken), you can restore the activation to enable the user to sign in to activate the product again. To do this, select the user and click the **Restore Activation** button above the user list.

Internal Update Configuration (On-premise environments only)

In an on-premise enterprise environment, the internal update server sends requests to the Foxit web server to get the latest versions of Foxit products, and the clients in the enterprise only get updates from the internal update server. The **Internal Update Configuration** item in Foxit Admin Console allows you to configure how to get the latest installation packages from the Foxit web server and how to deploy the package updates to the end users in your enterprise.

Configuration

In the **Configuration** page, you can specify the packages to be downloaded from the Foxit web server and the update configuration in your enterprise. After finishing the settings, click **Save** at the bottom of the page. If you want to erase all the specified settings, click **Reset**.

- **Packages to download**: Select the packages to be downloaded automatically from Foxit server. Downloaded packages can be viewed and managed in Version Management.
- **Automatic update check interval**: Specify how often the internal update server automatically checks for new product packages from the Foxit web server.
- **Automatically approve downloaded packages**: Turn on the switch to enable **Approved automatically** option to allow all end users in your enterprise to download all available packages that have been downloaded from Foxit server. This setting only applies to the packages that are downloaded from Foxit server after you specify the setting. By default, this option is disabled and you need to manually approve downloads for all packages.
- **Scheduled Update Settings**: Select the **Set a scheduled time to update specific users or groups** option to set different times for different users to install updates, which can help to relieve some of the pressure on server and bandwidth.
    - Click **Add** and select **Add user**, **Add IP Address**, or **Add MAC address** to add emails, IP, or Mac addresses you want to set a scheduled time for. All the users you added will be included in the list below. (If you choose **Add MAC address**, you can click **Add multiple MAC addresses** in the pop-up dialog box to add multiple MAC addresses at once by importing a CSV file with a list of MAC addresses you want to add.)
    - Click **Edit time** to select the scheduled time for selected users.
    - To delete the scheduled update settings for users, select the users from the list and click **Delete**.
- **Roll Back Setting**: Sometimes you might find issues in an update or the end users

are having problems with it. In these cases, administrators can configure rollback settings to force clients to temporarily roll back one or more versions to an earlier version. For example, check the **Roll back PhantomPDF versions** option, and select the rolled back versions and the available versions to roll back to. ***Note**: Only main packages support rollback. Rolling back to an earlier version installs the version and the default components, but the data in the registry and the GPO template will be retained.*

- **Network proxy configuration**: Set up a proxy server to connect to Foxit server as needed.

Version Management

The **Version Management** page in Admin Console lists all main packages and plug-in packages that have been downloaded, are being downloaded, and were not downloaded successfully from Foxit server. You can filter/delete packages, and restrict which packages are available to end users by approving distribution.

- To view the details of a package, click the **Details** icon in the **Action** column. The details panel appears in the right of the Admin Console window. Click the button in the upper right corner of the panel to close the panel.
- To filter packages, enter the package's name/version/size, or select the approval status or Download Completion Time in the boxes above the packages list as needed.
- To delete packages, select the package(s) and click the **Delete** button above the packages list.
- To give users access to packages or if the approval status is unapproved currently, select the package(s) and click the **Approve** icon in the **Action** column (or click the **Approve** button above the packages list). In the pop-up dialog box, do any the following:
    - Select **Approve package for all clients to update** to allow all clients in the organization to download the package, and click **Approve**.
    - To allow some specific clients to download the package, select **Approve package for specific clients to update** to add specific clients by selecting user emails, IP address ranges, or MAC addresses (You can also add multiple MAC addresses at once by importing a CSV file with a list of MAC addresses you want to add.). Then click **Approve**.
    - (Optional) For a package with significant changes or security updates, you can select the **Force clients to install update package** option for a mandatory update. Then the package status shows **Pushed** and all the selected clients have to download and install the package.
- To not allow users to download a package, select the package and click the **Cancel** icon in the **Actions** column. Or select the package(s) and click the **Unapprove** button above the packages list to disable downloading. After a package is approved/unapproved, **Approved** or **Unapproved** is shown respectively in the **Status**

column.

- (Optional) For a package whose approval status is **Approved** or **Pushed**, you can click the **Edit** icon in the **Action** column to modify the approval settings.

Both main packages and add-on packages are categorized into three tabs: **Downloaded**, **Download failed**, and **Downloading**. Here take main packages for example:

- In the **Downloaded** tab, you can view each package's name, version number, Download completion time, size, approval status, and the actions you can perform. Depending on the package's approval status, the available actions vary in the **Action** column.
- The **Download failed** tab lists the packages that were not downloaded successfully, and the time and reason for the failure. To delete a package, select it and click **Delete**; to start the download again, select the package and click **Retry**.
- The **Downloading** tab displays the list of packages that are being downloaded at present. You can view the details of each package including the package name, version number, and Start Time (when the download began).

Mail Servers

Enterprise administrators can configure an SMTP mail server used by Foxit Admin Console to send end users email messages such as update notifications and reports. Generally in an on-premise environment where the enterprise itself is responsible for any notifications, it is a must to configure an SMTP mail server. In the **Mail Servers** page, you can configure a mail server and then test the configured mail server.

Configure a mail server

To configure a mail server, edit the following fields as required and click **Save** after you complete editing. After a mail server is added, you can click the **Edit** icon in the **Actions** column to modify the server information, or click the **Delete** icon to remove the mail server.

SMTP server details

- Name – Enter a name to identify the mail server in Foxit Admin Console.
- From address – Enter the email address that will be used by Foxit Admin Console to send notification emails.
- From name – Enter the name that will be displayed in notification emails.
- Subject prefix – Enter the text that you want to appear at the beginning of the subject line of notification emails.

***Tip**: You can customize more information for email templates. See also Enterprise Brand Customization.*

Server hostname

- Server hostname - Enter the host name of the mail server or the JNDI location of a javax.mail Session object.
- Server port – Enter the port the mail server.
- User Name – Enter the username that will be used to connect to the mail server, and then specify the password below.
- Use TLS - Select this option if the SMTP server uses the Transport Layer Security (TLS) protocol.

Test a mail server

To ensure the mail server is correctly configured, you can click the  sign to send a test email. In the pop-up **Send test email** dialog box, specify the recipient, and enter the subject, message type, and messages. Then click **OK** to send the email. A text message will appear in the **Log** box in the **Send test email** dialog box, telling you whether the email has been sent successfully.

Products

The **Products** page lists all the products and licenses your company has purchased. If your company has purchased more licenses or products, you can update the licenses and products by doing the following:

1. Click **Update Licenses** at the top of the **Products** page.
2. In the pop-up dialog box, choose **Online updating** or **Offline updating**.

    - For **Online updating**, an internet connection is required. Click **Connect** to sign in with your account to update licenses.
    - If you don't have internet access, click **Browse** to select key files for the products. (If you haven't got a key file yet, click **Get One**. Then you will obtain the server ID of the Admin Console in the pop-up dialog box. You need to send the server ID to Foxit by email and Foxit's team will send the key file to you later.)

Reports

The **Reports** page shows a chart about the enterprise statistics including the number of

total licenses, assigned licenses, activated licenses, and active users. Administrators can specify what statistics to be displayed or export desired data as needed.

- To display specific statistics you need in the chart, do any of the following:

  - ✧ Select **All Statistics** or specific products to specify what products' statistics to be displayed.
  - ✧ Select the time period for which you want to view statistics.
  - ✧ Select the statistics you need: the number of total licenses, assigned licenses, activated licenses, and active users.

- To export data (summarized or detailed) you specified to a CSV file, do any of the following:

  - ✧ To export summarized data to a CSV file, put your cursor over **Export Data** (choose **Export User Data** to export data with detailed user information such as user names and emails), choose **Export Data Locally,** and specify a local location to download the file.
  - ✧ To send the exported CSV file with summarized data to your account by email, put your cursor over **Export Data** (choose **Export User Data** to export and send the detailed data), and choose **Send Data via Email**.

  ***Note**: When you export detailed user data, all instances of users that meet the specified criteria will be exported, including the users that have been removed from the Admin Console.*

Admin Role Management

An enterprise can have one super administrator and multiple general administrators and sub-administrators to perform management in Foxit Admin Console. In the **Admin Role Management** page, the super administrator can add general administrators and sub-administrators (assign the admin role to other users), remove general administrators and sub-administrators (revoke admin permissions), and change the super administrator.

***Note**: Different types of admins have different permissions.*

- *Super administrator – has all permissions to perform all tasks in the Admin Console.*
- *General administrator – has the same permissions as the super administrator, except the ability to add and remove administrators/sub-administrators.*
- *Sub-administrator – has the permissions to add/remove users and manage licenses within the specific OU assigned by the super administrator.*

Assign admin roles

To add a general admin, do the following:

1. Click **Add Admin**.
2. In the pop-up dialog box, enter the user's email address, select **Administrator** from **Role**, and click **OK**.
3. The user will be added to the admin list.

To add a sub-administrator, do the following:

1. Click **Add Admin**.
2. In the pop-up dialog box, enter the user's email address and select **Sub-administrator** from **Role**. Then click **Next**.
3. Select the department you want the sub-administrator to manage, name the assignment, and assign licenses in the pop-up dialog box. ***Tip****: The name for the assignment will be the OU name displayed in the* ***Customize Organizations*** *page the sub-administrator can see after logging in to Admin Console. See also Customized Organization.*
4. When you're done, click **OK**. The user will be added to the admin list.

Remove admin roles

To remove a general administrator or a sub-administrator, navigate to the administrator in the admin list and click on the **Delete** icon in the **Actions** column. Removing an administrator only revokes the admin privileges from the administrator, without deleting the user from the Admin Console.

Transfer the super admin privileges

As the super administrator, you can transfer your administrative privileges to another user.

1. Click the **Transfer ownership** icon in the **Actions** column.
2. In the pop-up dialog box, enter the email address of the new super admin and click **OK**.

If you are not only the super admin but also a user in Admin Console, this operation only revokes all of the administrative control and access to the Admin Console, without removing your user account from Admin Console.

Enterprise Brand Customization

In the **Enterprise Brand Customization** page, administrators can customize or modify the logo of PhantomPDF's login window on clients and email templates that are used for sending emails to end users, to match your company's brand.

Customize the client's login page:

Click **Browse** to select an image for the logo and enter the server name in the box. Both the logo and the server name will appear on the PhantomPDF's login window on clients.

Customize email templates:

Click **Browse** to select an image for the logo in emails and enter the company name that appears at the bottom of the email messages sent to your end users.

After completing the settings, click **Save**. Or click **Reset** to return to the default settings.

Settings

Password Setting

The **Password Setting** page under **Settings** allows administrators to modify the password for their own accounts to log in to Admin Console.

Windows Authentication

Integrated Windows authentication enables users to log in applications with their Windows credentials. For companies that have enabled Active Directory (AD) domains, administrators can configure their AD domain information in the Admin Console to allow the AD users to automatically activate products by logging in with their AD accounts.

Overall, two key steps are needed for Windows authentication: configuring settings in the Admin Console and on clients.

Configure settings in the Admin Console

In Step 1, navigate to the **Windows Authentication** page under **Settings**, and enter the information of the AD domain your organization uses.

- Domain name - The Windows AD domain name.
- IP Address - The IP address of the AD domain controller.
- Hostname - The hostname of the AD domain controller.
- Computer Account - The computer account of the domain controller. If you haven't created a computer account for the domain controller yet, click **How to get the above configuration** at the bottom of the page to create an account and password.
- Password – The password of the domain controller.
- Domain of Email – The domain of your email. If you leave this field empty, the system will use the domain name of the Computer Account.
- Reset – Click **Reset** at the bottom of the **Windows Authentication** page to clear all the data you entered above.

After completing the settings, click **Save and Test**. You will be prompted if the configuration is successful and then you can go to the next step to configure settings on clients.

Configure settings on clients

In Step 2, configure Internet Explorer on the client devices in your AD domain.

1. Open Internet Explorer.
2. Click Internet Options > Advanced > Settings > Security > select **Enable Integrated Windows Authentication**.
3. Restart Internet Explorer.
4. Click Internet Options > Security > Local Intranet > Sites > Advanced. Copy the URL provided in the **Windows Authentication** page to the **Websites** box. *(Note: The URL is generated automatically after the Admin Console is set up in your organization.*)
5. Internet Options > Intranet > Custom Level > User Authentication, select **Automatic login in intranet zone only**.

Content Logs

Keep track of administrators' actions on the Admin Console and the user data collected from clients. **Content Logs** contains four pages: Admin Operation Logs, Internal Update Operation Logs, Login Logs, and Rolled Back Logs.

Administrators' actions on the Admin Console are recorded in the tree pages: Admin Operation Logs, Internal Update Operation Logs, and Login Logs. From the lists in the pages, you can see when an action is performed, the action type (event type), the status (whether the action is performed successfully), the detailed results, and the operator (which administrator performs the action).

The Rolled Back Logs page records the events that users or devices roll back a version, including the rollback time, the user email, the associated product, the version they roll back to, the user's MAC address, and more.

- Admin Operation Logs - Records all the actions performed by the administrator.
- Internal Update Operation Logs - Records the administrator's operation history in internal update configuration.
- Login Logs - Records the administrator's login history.
- Rolled Back Logs – Records the events that users or devices rolled back a version successfully.

To filter log data, specify the criteria and click **Search**. You can also export and download log data to CSV files.

Product Configuration

To apply better and more precise control on the access to Foxit applications, you can do more configuration in the Admin Console such as the activation policy on clients.

Client Activation Policy

Licensing Model: shows the current licensing mode your company uses to control product licenses.

Authorization Model: Select an authorization model to assign licenses to users. This setting is only available for on-premise environments with LDAP set up in the Admin Console.

- **Manual authorization**: With this model selected, administrators can specify which users to assign licenses to. Only the assigned users can activate Foxit PhantomPDF successfully after logging in with their accounts. This model is selected by default.
- **Automatically authorize**: Select this model, and each user will be allowed to activate Foxit PhantomPDF once they log in with their accounts as long as there are available licenses.
  For the **Automatically authorize** model, if there are more than one license type for the same product, you need to specify the priority of how clients obtain authorization. Clients will automatically activate the product with the available licenses in the specified priority. Higher priority licenses are used before lower priority licenses.

IP address range restriction: Specify IP addresses or ranges to allow only the clients

whose IP addresses are in the specified ranges to activate Foxit PhantomPDF.

Offline activation period: Specify a period after which PhantomPDF on the devices will be automatically deactivated if those devices do not connect to the Admin Console server (e.g. devices are switched off or do not connect to the Internet). Generally, if deactivated because of the failure to connect to the server, PhantomPDF can be activated again once users connect their devices to the server, unless the licenses are revoked or expire.

Mac address range restriction: Specify MAC addresses to allow only the clients with the MAC addresses specified to activate Foxit PhantomPDF. You can also add multiple MAC addresses at once by importing a CSV file with a list of MAC addresses you want to add.

Contact Us

Feel free to contact us should you need any information or have any problems with our products. We are always here, ready to serve you better.

- *Office Address:*
  Foxit Software Incorporated
  41841 Albrae Street
  Fremont, CA 94538
  USA

- *Sales:*
  1-866-680-3668

- *Support & General:*
  1-866-MYFOXIT, 1-866-693-6948, or 1-510-438-9090

- *Fax:*
  1-510-405-9288

- *Website:*
  www.foxitsoftware.com

- *E-mail:*
  Sales - sales@foxitsoftware.com
  Marketing - marketing@foxitsoftware.com
  Technical Support - enter a trouble ticket via our Support Portal
  Business Development - bd@foxitsoftware.com