AvePoint® User Guide

AvePoint Perimeter Pro 1.9.1

Secured Share User Guide

Issued February 2018

Table of Contents

What’s New in this Guide

- Updated the Configuring Secured Share Settings section.

Overview

AvePoint Perimeter Pro includes the **AvePoint Perimeter Secured Share** feature, which allows users in your organization to share files, folders, or libraries within internal SharePoint sites with users inside and outside of your organization. Internal users can choose whether or not to verify permissions for the access of shared items, configure permission settings on shared files and set an expiration time for how long the files/folders/libraries will be available to other users. Additionally, internal users can configure watermark settings for the sites to protect the shared files.

Users with whom the files/folders/libraries are shared can view and download copies of the shared files/folders/libraries via the **AvePoint Perimeter External Portal** or AvePoint Perimeter mobile apps on enrolled iOS (iPhone, iPad, and iPod touch)/Android devices, edit shared files, and upload new files to shared folders/libraries at the **AvePoint Perimeter External Portal**. The shared files protected with watermark will be viewed and downloaded in PDF format on the External Portal.

Internal users can go to the **AvePoint Perimeter Internal Portal** to view and manage the files, folders, and libraries shared by them. Site collection administrators can view and manage all of the shared files, folders, and libraries within their site collections.

The architectural diagram below outlines the workflow process for access to the AvePoint Perimeter External/Internal Portal through AvePoint Perimeter Secured Share.

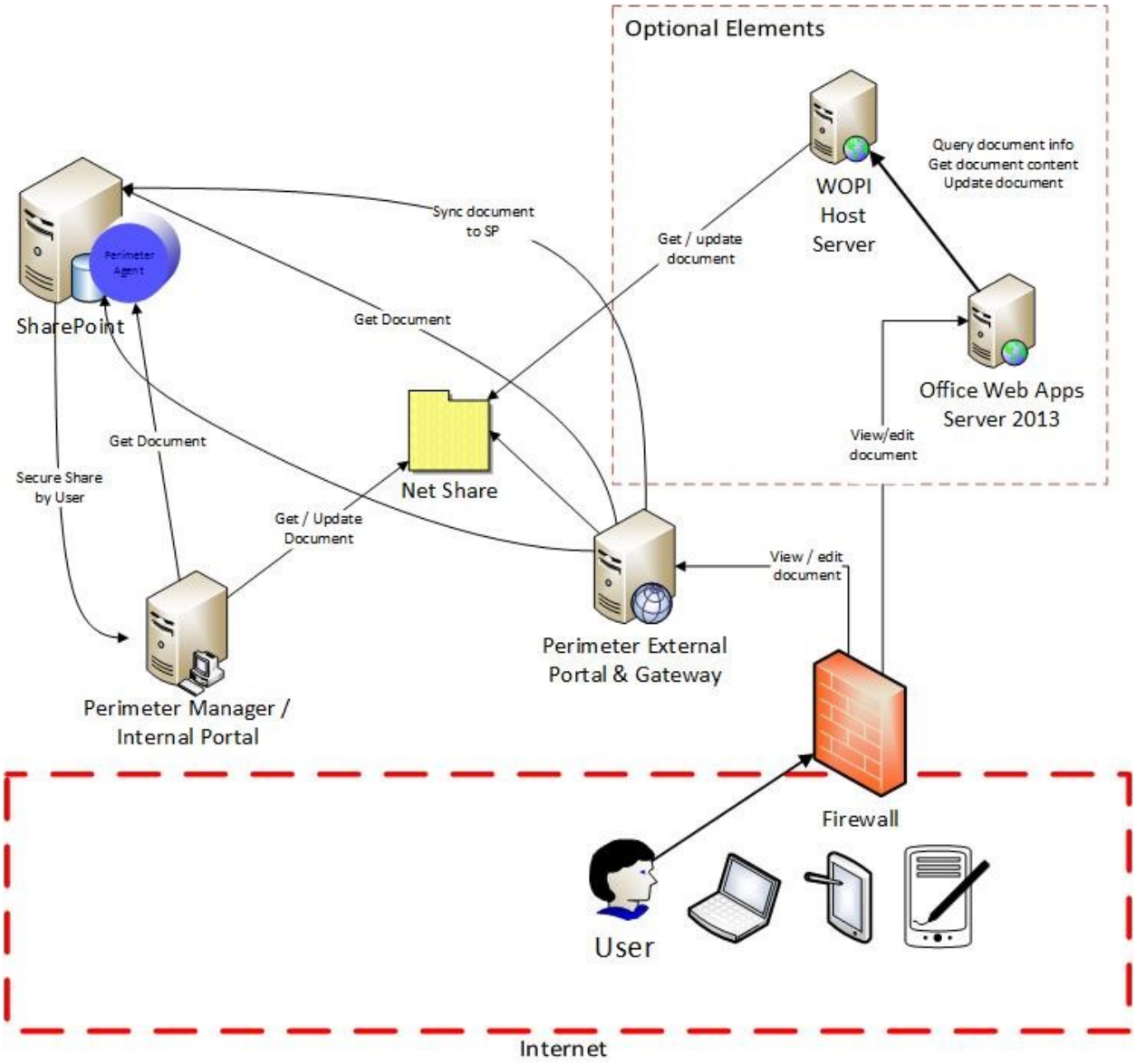

Figure 1: Architectural Diagram for Perimeter Secured Share feature

Internal Users

The following are tasks that every internal user can perform using the **AvePoint Perimeter Secured Share** feature and **AvePoint Perimeter Internal Portal**. Click the links to jump to the corresponding sections for detailed instructions.

Every internal user can perform the following tasks:

1. Sharing Files, Folders and Libraries via the AvePoint Perimeter Secured Share Feature

- Sharing Files or Folders via the AvePoint Perimeter Secured Share Feature
- Sharing a Library via the AvePoint Perimeter Secured Share Feature

2. Viewing Secure Share Details of a Shared File, Folder or Library in SharePoint
3. Logging into AvePoint Perimeter Internal Portal for the First Time
4. Managing My Shared Files
    - Opening shared files/folders/libraries in a browser
    - Accessing shared files/folders/libraries in SharePoint
    - Managing the Notification and Permission Settings for Shared Files, Folders and Libraries
        - Managing the Notification and Permission Settings for Shared Files, Folders and Libraries
        - Deleting Users' Permissions for Shared Files/Folder/Libraries
    - Viewing document usage for shared files
    - Downloading shared files

Site Collection Administrators

In addition to the tasks available for every internal user mentioned above, site collection administrators can perform the following advanced tasks:

1. Adding Managed Site Collections
2. Configuring Unique Watermark Settings for the Sites Within a Site Collection
3. The following operations manage all of the shared files, folders, and libraries within managed site collections:
    - Configuring Unique Watermark Settings for the Sites Within a Site Collection
    - Managing all shared files
        - Opening shared files/folders/libraries in browser
        - Accessing shared files/folders/libraries in SharePoint
        - Managing the Notification and Permission Settings for Shared Files, Folders and Libraries
            - Deleting Users' Permissions for Shared Files
        - Viewing History of Shared Files/Folders/Libraries
        - Viewing document usage for shared files
        - Downloading shared files

- Viewing the Dashboard
    - Viewing Secure Share Details

External Portal Users

After files/folders/libraries are shared via the Secured Share feature, the users (internal users and external users) with whom the files/folders/libraries are shared will receive an e-mail notification that includes the links for the shared content on the AvePoint Perimeter External Portal. Users can click the links in the e-mail to sign into the AvePoint Perimeter External Portal and access the content that has been shared with them.

***Note**: If a user logs into the AvePoint Perimeter External Portal via a browser whose display language is Japanese, French, or Italian, the AvePoint Perimeter External Portal will be displayed in Japanese, French, or Italian. For all other browsers whose display language is not Japanese, French, or Italian, the AvePoint Perimeter External Portal will be displayed in English.

Follow the procedures below to use the AvePoint Perimeter External Portal.

1. Before You Use the AvePoint Perimeter External Portal
2. Registering to the AvePoint Perimeter External Portal
    - Logging into the AvePoint Perimeter External Portal
    - Setting a Password in the AvePoint Perimeter External Portal
3. Users can perform the following tasks on the AvePoint Perimeter External Portal based on the permissions they have for the shared content and user type:
    - Using the My Files Interface
        - Accessing Shared Files from the My Files Interface
            - Opening a shared file in browser
            - Editing a shared file using Office Web Apps
            - Downloading shared files
            - Editing a Shared File by Overwriting it
        - Accessing Shared Folders and Libraries from the My Files Interface
            - Opening a shared file included in a shared folder/library in browser
            - Editing a shared file using Office Web Apps
            - Downloading shared files
            - Editing a Shared File by Overwriting it
            - Uploading a New File to a Shared Folder or Library
    - Operations Available on the Username Menu

- Managing enrolled devices
- Enrolling a new device

If an external user with whom the SharePoint folders are shared through the Secure Share feature wants to share the folder with others, this user can configure a SAP Jam group integrated with the AvePoint Perimeter External Portal to assign the shared folders to all of the members in that group. For detailed instructions, refer to Appendix A: Integrating the AvePoint Perimeter External Portal with SAP Jam.

Supported Browser Versions for AvePoint Perimeter Internal Portal and External Portal

See below for AvePoint Perimeter Internal Portal and External Portal browser support:

***Note**: It is recommended to use the latest versions of the browsers listed in the sections below.

Browser	Version
Internet Explorer	IE 9 or later
Google Chrome	49.0.2623.112 m or later
Mozilla Firefox	44.0.2 or later
Safari	Installed on iOS 9 or later

Supported File Types for Online Viewing on AvePoint Perimeter Internal Portal and External Portal

See the table below for the supported file types for online viewing on the AvePoint Perimeter Internal Portal and External Portal:

File Type	File Extension
Microsoft Word Document	.doc, .docx
Microsoft Excel Workbook	.xls, .xlsx
Microsoft PowerPoint Presentation	.ppt, .pptx
PDF file	.pdf
Microsoft Project file	.mpp
Microsoft Visio Drawing	.vsd, .vsdx
Image	.jpg, .png, .gif, .svg
AutoCAD file*	.dwg
Web page	.html, .htm
Text document	.txt
XML Paper Specification file	.xps
Printer Command Language Document	.pcl

***Note**: The AvePoint Perimeter Internal Portal and External Portal only support the online viewing of the AutoCAD 2004 **.dwg** files with no 3D effects.

Sharing Files, Folders and Libraries via the AvePoint Perimeter Secured Share Feature

Using the **AvePoint Perimeter Secured Share** feature within a specific SharePoint site, internal users can share files and folders in bulk and libraries individually with users within or outside your organization. The sections below offer detailed instructions on sharing files, folders and libraries through the **AvePoint Perimeter Secured Share** feature.

***Note**: Prior to sharing files/folder/libraries in a SharePoint site, you must ensure the **AvePoint Perimeter Secured Share** feature is active in this site.

Sharing Files or Folders via the AvePoint Perimeter Secured Share Feature

To share files or folders through the **AvePoint Perimeter Secured Share** feature in a site, complete the steps below:

***Note**: You must ensure that you have configured an e-mail address in the Active Directory Domain Controller. All updates of files or folders shared by users will be sent from this e-mail address.

1. Navigate to the document library containing the files/folders you want to share.
2. Select the files/folders you want to share by checking the corresponding checkboxes.
3. Click **Secure Share** on the ribbon of the **FILES** tab (in SharePoint 2013 and SharePoint 2016) or the **Documents** tab (in SharePoint 2010). The **Secured Share** pop-up window appears.

   ***Note**: If your Perimeter administrator defined document attribute based restrictions for secure share, the files and folders that are blocked will be listed in a pop-up window. You must deselect those blocked files or folders before continuing with secure share.
4. Follow the instructions in Configuring Secured Share Settings to configure the settings for sharing the selected files/folders in the **Secured Share** window.
5. Click **OK** to save the settings and share the files/folders/library with the designated users.

Once the selected files/folders are successfully shared, the users with whom the files/folders are shared can view the shared files/folders via the AvePoint Perimeter External Portal and AvePoint Perimeter mobile apps. The internal user who shares the files/folders can go to the AvePoint Perimeter Internal Portal to view and manage the shared files/folders.

Sharing a Library via the AvePoint Perimeter Secured Share Feature

To share a library through the **AvePoint Perimeter Secured Share** feature in a site, complete the steps below:

1. Navigate to the site where the library you want to share resides.
2. Go to the **LIBRARY** tab (in SharePoint 2013) or the **Library** tab (in SharePoint 2010).
3. Click the **Share Library** button on the ribbon. The **Secured Share** window appears.

   ***Note**: You must ensure that you have configured an e-mail address in the Active Directory Domain Controller. The updates of files or folders shared by users will be sent by this e-mail address.

4. Follow the instructions in Configuring Secured Share Settings to configure the settings for sharing this library in the **Secured Share** window.
5. Click **OK** to save the settings and share the library with the designated users.

Once the library is successfully shared, the users with whom the library is shared can view the shared library via the AvePoint Perimeter External Portal and AvePoint Perimeter mobile apps. The internal user who shares this library can go to the AvePoint Perimeter Internal Portal to view and manage the shared library.

Configuring Secured Share Settings

In the **Secured Share** window, select a secure share type at first for this sharing:

***Note**: Your Perimeter administrator controls whether or not to allow you to share items using the **Accessible to anyone through links** type and the **Verify viewers via passcode** type. If the secure share types are disabled, they are not available in the **Secure Share** page.

- **Require registration and verify the shared permission** – With this option selected, the shared users must provide the login credentials on the Perimeter Portals to access the shared items and their activities on the shared items will be controlled within the granted permission level.
- **Accessible to anyone through links** – If you want to allow anonymous access for the shared items, select the **Accessible to anyone through links** option. The shared items' links will be sent to the users in e-mail and they can also share the links with others. Anyone who wants to access the shared items can use these links to view or download the shared files.
- **Verify viewers via passcode** – If you want to verify the viewers of the shared items via passcode, select the **Verify viewers via passcode** option. The shared items' links will be sent to the users in e-mail and they can share the links with others. The user who accesses a shared item via the link is required to provide the e-mail address for

verification. That e-mail address will receive a one-time passcode and the user must provide the passcode to access the shared item.

If you select the **Require registration and verify the shared permission** option, continue with the settings below; if you select the **Accessible to anyone through links** option or the **Verify viewers via passcode** option, refer to Secure Share Settings for Anonymous Access and Passcode Verification.

- **Share With** – Configure with whom you want to share the selected files/folders/library and select whether to send e-mail notifications to the users or AD groups for the sharing.
    - **Invite people** – To share files/folders/library with others, enter their e-mail addresses in the text box. You can also enter internal users' usernames or AD groups' names to share. The matched users or AD groups will be automatically displayed. The matched external users that have been shared with before will also be displayed in the search results. Select a user or AD group from the search results.

      ***Note**: If your Perimeter administrator has configured domain restriction to control where the shared with users or groups are from, you will be notified when the user or group you entered is from a blocked domain. Please contact your administrator in this case.

    - **Send e-mail notifications to the users above** – Select whether to send e-mail notifications to the users you are sharing files/folders/library with. If you share the items with an AD group, the members of this AD group will receive the e-mail notification.
        - To send e-mail notifications to these users, select the checkbox. If you want to include a personal message within the invitation, enter your message in the text box. When entering a message, you can press Enter on the keyboard to start a new line of text inside the box. The entered message will be displayed before the pre-defined message in the e-mail notifications.
        - If you do not want to send e-mail notifications to these users, keep this checkbox deselected.
- **Permission Level** – Select the permission level you want to grant these users for the selected files/folders/library from the drop-down list. If your administrator has enabled the permission control in Secure Share, the permission levels that you are allowed to grant to the shared with users depend on your own permissions to the files, folders, or the library.
    - If you have the **Edit Items** permission to the files, folders, or library, you can grant the users any of the provided permission levels.
    - If you have the **View Items** and **Open Items** permission to the files, folders, or library, you can grant the users the **Read Only** or **Download** permission level.

- If you only have the **View Items** permission to the files and the files can be opened by Office Web App, you can only grant the users the **Read Only** permission level. If you only have the **View Items** permission to the files and the files cannot be opened by Office Web App, you can grant the users the **Read Only** or **Download** permission level.
- If you only have **View Items** permission to the folders or library, you can only grant users the **Read Only** permission level.

***Note**: The Delete option is disabled when you share a library via Secure Share.

To view the specific permissions included in each permission level, click the **Learn more about permission levels** to access the **Permission Level Capabilities** table. For further explanations on the permission level capabilities, refer to [About Secured Share Permission Levels](#).

Permission Level Capabilities

	Read Only	Download	Edit	Edit in Browser Only	Delete
View Only	✓	✓	✓	✓	✓
Print		✓	✓		✓
Copy & Paste		✓	✓	✓	✓
Download Files		✓	✓		✓
Edit in Browser			✓	✓	✓
Upload New Files to Shared Folder/Library			✓		✓
Reupload Modified Files			✓		✓
View Files with Watermark	✓	✓			
Delete Items					✓

Figure 2: Permission Level Capabilities table.

- **Share Updates** – This section is only available in the **Secured Share** window when files are selected. Select whether to share the updates of the shared files with these users as well.

  ***Note**: If sharing a library or folder with these users, all of the updates of this library/folder will be automatically shared with them.

- If you select **Yes**, the updates of the selected files in SharePoint will be shared with these users via the AvePoint Perimeter External Portal or Perimeter mobile apps.
- If you select **No**, the updates of the selected files in SharePoint will not be shared with these users.

- **Expiration Time** – Select an expiration time from the calendar for how long you would like to share the selected files/folders/library with these users. To ensure that the sharing never expires, leave this field blank.
- **Share View** –Select a list view from the drop-down list to display the properties of the shared items on Perimeter Portals or mobile apps. The properties will be displayed according to the column settings of this list view and only available on Perimeter Portals or mobile apps when your Perimeter administrator has metadata display enabled in the Perimeter Management Console.
- **Share Within a Folder** – If you want to categorize the sharing for specific users, you can configure this field. Enter a name into the text box for the virtual folder, which will be displayed on the Perimeter Portals or mobile apps containing all of the shared items. The users that are shared with in this sharing event must open this virtual folder on the Perimeter Portals or mobile apps to access the shared items.
- **Send Notification** – Choose whether or not to send notifications.

  ***Note**: The update notification will not work if your Perimeter administrator does not enable update notification. Please contact your administrator to confirm if update notifications have been enabled.

  - **Notify me when this item is viewed by anyone** – With this option selected, you will receive an e-mail notification once this item is viewed by anyone else.
  - **Notify everyone this item is shared with if the item is updated or deleted** – With this option selected, an e-mail notification will be sent to everyone with whom this item is currently shared once anyone updated or deleted this item.
  - **Notify me once this item is downloaded by anyone** – With this option selected, you will receive an e-mail notification once this item is downloaded by anyone else.

Secure Share Settings for Anonymous Access and Passcode Verification

If you select the **Accessible to anyone through links** option or the **Verify viewers via passcode** option, refer to the instructions below to complete the settings:

- **Send Link To** – Enter the users to whom you want to send the links of the share items via e-mail. Select the **Send e-mail notifications to the users above** option to send the e-mail notifications to the users you entered. If you want to include a personal message within the e-mail, enter you message in the text box. The entered message will be displayed before the pre-defined message in the e-mail notifications.

- **Permission Level** – Select the **Read Only** or **Download** option as the permission level. You can click the **Learn more about permission level** link to view the capabilities of the permission levels.
- **Expiration Time** – Select an expiration time from the calendar for when the links will expire. To ensure that the sharing never expires, leave this field blank.
- **Send Notification** – This field is unavailable when the **Accessible to anyone through links** option is selected.
    - **Notify me when this item is viewed by anyone** – With this option selected, you will receive an e-mail notification once this item is viewed by anyone else.
    - **Notify me once this item is downloaded by anyone** – With this option selected, you will receive an e-mail notification once this item is downloaded by anyone else.

About Secured Share Permission Levels

To share a file/folder/library via the AvePoint Perimeter **Secured Share** feature with external/internal users, it is necessary to assign these users permission to access the shared file/folder/library that will be stored in the AvePoint Perimeter External Portal. To assign these users permissions, select a permission level in the **Secured Share** window. Even after the files are shared, you can change the permission levels for specific files via the **Manage Permissions** feature in the AvePoint Perimeter Internal Portal. Refer to the table below for the specific permissions to include in each permission level that can be assigned to users for the shared file/folder/library.

Permission Level / Permission	Read Only	Download	Edit	Edit in Browser Only	Delete
Open in Browser	√	√	√	√	√
Print		√	√		√
Copy & Paste		√	√	√	√
Download Files		√	√		√
Edit in Browser			√	√	√
Upload New Files to Shared Folder/Library			√		√
Re-upload Modified Files			√		√
View Files with Watermark	√	√			
Delete Items					√

***Note**: The users granted the **Delete** permission level can delete the files and subfolders within the shared folders.

***Note**: Only the files of the following file types listed in the Supported File Types for Online Viewing on AvePoint Perimeter Internal Portal and External Portal section can be opened online in the AvePoint Perimeter External Portal and Internal Portal. If you are about to share a file or a folder/library that contains files that cannot be opened online, AvePoint recommends granting the users **Download**, **Edit**, or **Delete** permission level to ensure that the users can download the shared files.

Viewing Secure Share Details of a Shared File, Folder or Library in SharePoint

After a file/folder/library is shared with users through the AvePoint Perimeter **Secured Share** feature in a SharePoint site, internal users can use the following features to view the secured share details of the shared content:

- The **Modified By (External)** column in each library that contains shared files that have been modified by users on the AvePoint Perimeter External Portal. When a shared file is edited by a user on the AvePoint Perimeter External Portal for the first time, the **Modified By (External)** column is added to the library where this file resides.
    - If a shared file has been last modified by a user on the AvePoint Perimeter External Portal, the username of the user is displayed in the **Modified By (External)** column of this file.
    - If a shared file has been last modified by a user in SharePoint, the value in the **Modified By (External)** column of this file is automatically cleared and left blank.

  ***Note**: If a shared file's **Modified By (External)** column value cannot be automatically cleared after it is modified by a SharePoint user, contact your site administrator to resolve this issue by deactivating the **AvePoint Perimeter Secured Share** site feature and then re-activating the feature.

- The **Secured Share Details** feature on the ribbon of each shared library and each library that contains shared files or folders. Using this feature, internal users can view the detailed information of the sharing settings of each shared object (file/folder/library), including the users who shared this object, users who were shared with, the permission level assigned for the shared object, and the expiration date of the share. For detailed instructions on using this feature, see the steps below.

To view the secure share details of a file/folder/library using the **Secured Share Details** feature, complete the steps below:

1. Access the **Secure Share Details** interface by either of the following methods, according to the object level of the shared object whose secure share details you want to view:
    - To access the **Secure Share Details** interface of a shared file or folder, complete the steps below:
        i. Go to the library where the desired file or folder resides and select the desired file or folder.
        ii. Go to the **FILES** tab (in SharePoint 2013) or the **Documents** tab (in SharePoint 2010).
        iii. Click **Secure Share Details** on the ribbon. The **Secure Share Details** pop-up window appears.

- To access the **Secure Share Details** interface of a shared library, complete the steps below:
    i. Go to the library whose secure share details you want to view.
    ii. Go to the **LIBRARY** tab (in SharePoint 2013) or the **Library** tab (in SharePoint 2010).
    iii. Click **Secure Share Details** on the ribbon. The **Secure Share Details** pop-up window appears.

2. In the **Secure Share Details** interface, you can view the detailed information of all sharing settings of the shared object and perform the following operations:
    - **INVITE PEOPLE** – To share this object with more people, click this link to open the **Secured Share** window.
    - **MANAGE SHARED FILES** – To manage all of the files, folders, and libraries shared by you, click this link to access the AvePoint Perimeter Internal Portal.
    - **Resend Notification** – To send an e-mail notification again to the user with whom this item is shared, click this button.

Logging into AvePoint Perimeter Internal Portal for the First Time

Refer to the section below for the steps for logging into the AvePoint Perimeter Internal Portal.

1. In a SharePoint site where you have shared files through the AvePoint Perimeter Pro **Secured Share** feature, go to a document library and click the **FILES** tab (in SharePoint 2013) or the **Documents** tab (in SharePoint 2010).
2. Click the **Manage Shared Files** button on the ribbon. The login page of the AvePoint Perimeter Internal Portal appears.
3. Log into the AvePoint Perimeter Internal Portal with your Active Directory credentials or your registered e-mail address and password.

***Note**: If your Perimeter administrator has set the **Windows Authentication** as the default authentication type for signing into the Internal Portal, internal users will automatically sign into the Internal Portal using Windows accounts.

Using the AvePoint Perimeter Internal Portal

The sections below offer instructions on using the AvePoint Perimeter Internal Portal. To access the Internal Portal, click **Manage Shared Files** in the ribbon for any document library where the **AvePoint Perimeter Secured Share** feature has been enabled.

Managing My Shared Files

In the **My Shared Files** interface, you can view and manage all of the files, folders, and libraries you have shared through the **AvePoint Perimeter Secured Share** feature, download shared files, and view the usage details of each shared file.

In the display pane of the **My Shared Files** interface, you can view all of the files, folders, and libraries you have shared via the **AvePoint Perimeter Secured Share** feature, including the shared object name, and original URL in SharePoint.

With the Search box on the **My Shared Files** page, you can select the **Current Folder** search criteria for searching items among the shared files, folders, or libraries or select the **All Folders** search criteria for searching items among the shared items and within the shared folders and libraries. In a specific shared library or folder, you can also use the Search box to search items in the root folder or its entire hierarchy by selecting **Current Folder** or **All Folders**.

You can also perform the following operations on a desired shared object:

- Open the shared object by clicking the object name in the **NAME** column.
  - If you click a file name, the file will be opened in the browser.
  - If you click a folder name or library name, you can open this folder/library to view the content inside.
- Access the original URL of this shared object by clicking the link in the **URL** column.
- Click the settings ( ) button for a shared object in the **ACTION** column, a drop-down menu appears. The following actions are available:
  - **Manage Sharing** – To manage the notification settings for downloading or updating the shared file and the permission settings of a shared file/folder/library, select this option. The **Manage Sharing** interface for this object appears. For detailed instructions on operations in this interface, refer to Managing the Notification and Permission Settings for Shared Files, Folders and Libraries.
  - **View Document Usage** – To view the usage of a shared file or the files included in a shared folder/library performed by users via the AvePoint Perimeter External Portal and AvePoint Perimeter mobile apps, select this option to access the **View Document Usage** interface for this file. In this interface, you can view details of all of the activities on the selected shared file or files in the shared

folder/library, including the access time, the user who accessed the file, the action performed, the source of the access, and the shared file's URL in each activity.

- **Download** – This option is used to download a copy of a shared file.
  - To download a shared file in the **My Shared Files** interface, click the settings ( ) button for this file and then select **Download** from the drop-down menu.
  - To download a file inside a share folder or library, expand the folder or library to display desired file, click the settings ( ) button for this file, and then select **Download** from the drop-down menu.
- **Unlock** – This option is only available for site collection administrators, and it only appears when anyone is editing this file or has checked out this file. Site collection administrators can unlock the shared file to allow the others to make edits.
- **Properties** – Select this option to view the properties of the file. The **Properties Information** area will appear, displaying the properties of the item.

Managing the Notification and Permission Settings for Shared Files, Folders, and Libraries

The **Manage Sharing** interface displays notification settings for shared files being updated or downloaded and the detailed information on all of the permissions assigned for a shared file/folder/library, including the user who shares this object, the user with whom this object is shared, permission level, share update settings, and expiration time of each sharing event. Refer to the sections below to manage notifications and permissions for a shared object.

Complete the steps below to configure the notification and permission settings of sharing:

1. In the **Mange Sharing** interface, find the **Configure Notification** section. You can choose the notifications the shared by user will receive by selecting the **Notify users who shared the item once it is viewed** option, **Notify users who shared the item when it is updated** option or the **Notify users who shared the item when it is downloaded** option.
2. In the **Manage Permissions** section, select one or more sharing records in the table and click **Edit** to modify the permission level, expiration time, share update, or the notification settings for.
3. In the **Edit** window, configure the following settings:
   - **Permission Level** – Select the permission level you want to grant the user for this shared file/folder/library from the drop-down list. For details on selecting the permission level, refer to About Secured Share Permission Levels.

If your administrator has enabled the permission control for Secure Share, the permission levels that you are allowed to grant to the shared with users depend on your own permissions to the files, folders, or the library.

- If you have the **Edit Items** permission to the files, folders, or library, you can grant the users any of the provided permission levels.
- If you have the **View Items** and **Open Items** permission to the files, folders, or library, you can grant the users the **Read Only** or **Download** permission level.
- If you only have the **View Items** permission to the files and the files can be opened by Office Web App, you can only grant the users the **Read Only** permission level. If you only have the **View Items** permission to the files and the files cannot be opened by Office Web App, you can grant the users the **Read Only** or **Download** permission level.
- If you only have **View Items** permission to the folders or library, you can only grant users the **Read Only** permission level.

- **Share Updates** – Select whether or not to share the updates of the shared file with the users who have Download permission or Read-Only permission.

  Note: This field is only editable for files.
- **Expiration Time** – Specify the expiration time of a file/folder/library share by selecting an expiration time using the calendar.
- **Notification** – Choose whether or not to notify the shared with users when this file is updated.

4. Click **Save** on the window to save the changes, or click **Cancel** on the window to exit the window without saving the changes.

Deleting Permissions to Shared Files/Folder/Libraries

To delete a user or group's permissions for a shared file, folder, or library, complete the following steps:

1. In the **Manage Sharing** interface, go to the **Manage Permission** section.
2. Locate the sharing record for the user or group whose permission you want to delete through the **SHARED WITH** column, click the Delete ( ) button on the ribbon. The confirmation window appears.
3. Click **OK** to delete a user or group's permission to this shared file/folder/library, or click **Cancel** to exit this window without revoking the sharing.
4. Click **Save** to save the configurations and exit the **Manage Sharing** interface, or click **Cancel**.

If a user or group's permissions for this shared file/folder/library have been revoked, this user or the users in this group cannot access this object via the AvePoint Perimeter External Portal or AvePoint Perimeter mobile apps.

Managing All Shared Files in Site Collections

If you are a site collection administrator of SharePoint site collections that have the **Secured Share** feature deployed on them, the AvePoint Perimeter Internal Portal provides you with features to view and manage all of the shared files, folders, and libraries within your site collections.

To manage all of the shared files, folders, and libraries within your site collections, you must first add your site collections into **Manage Site Collections**. After you add site collections into the managed site collections, the **All Shared Files** and **Dashboard** interfaces become available. You can view and manage all of the shared files, folders, and libraries within your managed site collections.

Adding Managed Site Collections

To add a site collection into **Manage Site Collections**, click the settings ( ) button in the upper-right corner and click **Manage Site Collections** to access the **Managed Site Collections** interface. Complete the following steps to add site collections into managed site collections:

1. Click **Add Site Collection**.
2. In the **Site Collection URL** column, enter the URL of the site collection you want to add into the text box.
3. In the **Authentication Method** column, select the authentication method used by the SharePoint zone where the site collection resides.
4. In the **Password** column, click **Click to Edit** and enter the password of your current login account into the text box.
5. After adding a site collection, you can click **Add Site Collection** to add another site collection or click the **Delete** ( ) button following each site collection to delete the site collection. You can also click the **Go to SharePoint** ( ) button to access the site collection in SharePoint.
6. Click **Save** to add the site collections or click **Cancel** to exit this interface without adding the site collections.

Configuring Unique Watermark Settings for the Sites Within a Site Collection

In the **Manage Site Collections** interface, you can expand the added site collections to configure watermark settings for the sites within. If the Web application where the added site collection resides has watermark settings configured in Perimeter Manager, the watermark settings of the site collection inherits that from the Web application by default. You can configure unique watermark settings for the sites within the site collection from the Perimeter Internal Portal, as well as for the sites in the site collection that do not have watermark settings configured.

After you have added the site collection, expand the tree displayed under the **SCOPE**. You can view all of the sites within the site collection and their watermark settings inheritance status.

If the Web application where this site resides has watermark settings enabled, complete the steps below:

1. Click **Configure** next to the site where you want to configure unique watermark settings. The **Configure** interface appears.
2. In the **Watermark** section, deselect the **Inherit configuration from Perimeter Manager** option to configure the unique watermark settings for this site.

   ***Note**: If you want to disable the watermark settings on this site, deselect the **Enable watermarking** option, and then click **Save**.

3. In the **Watermark Settings** section, complete the settings below:
   - **Text** – Select the **Current User Account** option from the drop-down list to display the username of the account who is accessing the shared file as the watermark text, or select **Customized** to enter the desired text or select a value from the drop-down list as the watermark text.
   - Configure the font, size, color, and layout for the watermark text.
   - **Repeat** – Choose whether or not to repeat the text on the same page.
4. Click **Save**.

If the Web application where this site resides does not have watermark settings enabled, the **WATERMARK SETTINGS INHERITANCE** column is not applicable in this case. Complete the steps below to enable and configure the watermark settings for the site within:

1. Click **Configure** next to the site where you want to configure watermark settings. The **Configure** interface appears.
2. In the **Watermark** section, select the **Enable watermarking** option.
3. In the **Watermark Settings** section, complete the settings below:
   - **Text** – Select the **Current User Account** option from the drop-down list to display the username of the account who is accessing the shared file as the watermark text, or select **Customized** to enter the desired text or select a value from the drop-down list as the watermark text.
   - Configure the font, size, color, and layout for the watermark text.
   - **Repeat** – Choose whether or not to repeat the text on the same page.
4. Click **Save**.

If you want to remove the unique watermark settings configured on a site, click **Remove Configurations** next to the site, and then click **OK** to proceed.

Managing All Shared Files

After you add site collections into the Managed Site Collections, the **All Shared Files** interface becomes available. In **All Shared Files**, you can view and manage all of the files, folders, and libraries shared via the **AvePoint Perimeter Secured Share** feature within your managed site collections.

With the Search box on the **All Shared Files** page, you can select the **Current Folder** search criteria for searching items among the shared files, folders, or libraries or select the **All Folders** search criteria for searching items among the shared items and within the shared folders and libraries. In a specific shared library or folder, you can also use the Search box to search items in the root folder or its entire hierarchy by selecting **Current Folder** or **All Folders**.

In the display pane of **All Shared Files**, you can view all of the files, folders, and libraries shared via the Secured Share feature within your managed site collections, including the name and original URL of each shared object in SharePoint, and perform the following operations on a desired shared object:

- Open the shared object by clicking the object name in the **NAME** column.
    - If you click a file name, the file will be opened in the browse and can be read.
    - If you click a folder name or library name, you can open this folder/library to view the content inside.
- Access the original URL of this shared object by clicking the link in the **URL** column.
- If you click the settings ( ) button for a shared object in the **ACTION** column, the following actions are available:
    - **Manage Sharing** – To manage the notification settings for downloading or updating the shared file and the permission settings of a shared file/folder/library, select this option. The **Manage Sharing** interface for this object appears. For detailed instructions on using this interface, refer to Managing the Notification and Permission Settings for Shared Files, Folders and Libraries.
    - **View History** – To view the sharing history of a shared file/folder/library, select this option. The **View History** interface for this object appears. For detailed information on using this interface, refer to Viewing History of Shared Files/Folders/Libraries.
    - **View Document Usage** – To view the usage of a shared file or the files included in a shared folder/library accessed by users via the AvePoint Perimeter External Portal and AvePoint Perimeter mobile apps, select this option to access the **View Document Usage** interface for this file. In this interface, you can view details of all of the activities on the selected shared file or files in the selected shared folder/library, including the access time, the user who accessed the file, the action performed, the source of the access, and the shared file's URL in each activity.
    - **Download** – This option is used to download a copy of a shared file.

- To download a shared file in the **All Shared Files** interface, click the settings ( ) button for this file and then select **Download** from the drop-down menu.
- To download a file inside a share folder or library, expand the folder or library to display the desired file, click the settings ( ) button for this file, and then select **Download** from the drop-down menu.

Viewing History of Shared Files/Folders/Libraries

In the **View History** interface, you can view the detailed information of all of a shared object's sharing events, including the user who shared the object, the user who is shared with, the time when this object was shared, permission level and expiration time of each sharing event. To export a **.csv** report of these sharing events, click **Export** on the ribbon. Your browser will prompt you to open or save the CSV file. Click **Save** or **Save as** to save it to a designated location.

Viewing the Dashboard

After you add site collections into the managed site collections, the **Dashboard** interface becomes available. In **Dashboard**, you can get an overview of the number of the shared objects within each managed site collection in a more intuitive way.

To generate a graph displaying the numbers of shared objects within a specific managed site collection, complete the following steps:

1. Select the site collection where the shared objects you want to view are located from the **Site Collection** drop-down list
2. Select the report type you want to view from the drop-down list next to the site collection:
    - **Total Shared Files** – With this option selected, the number of the total shared objects within the selected site collection is displayed in the graph below.
    - **Recently Shared Files** – With this option selected, the numbers of the shared objects within the selected site collection during each day/week/month are displayed in the graph below.
3. Select the time interval of the data displayed in the **Shared Files** graph by clicking **Daily/Weekly/Monthly**.

In the generated **Shared Files** graph, the X-axis is the date, week or month. The Y-axis is the number of the shared objects. You perform the following operations on the graph:

- By hovering the mouse over a specific node, you can view the number of **Total Shared Files** within the selected site collection up to the specific time point or the number of **Recently Shared Files** within the selected site collection during the specific time range.
- By clicking a specific node, you can access the **Sharing Details** interface to view the detailed information of the **Total Shared Files** within the selected site collection up to the selected time point or the **Recently Shared Files** within the selected site collection

of the selected time range. For detailed instructions on the operations in the **Sharing Details** interface, refer to Viewing Secure Share Details.

Viewing Secure Share Details

In the **Secure Share Details** interface, you can view the detailed information of the **Total Shared Files** within the selected site collection up to the selected time point, or the **Recently Shared Files** within the selected site collection for the selected time range, including the shared object name, and original URL in SharePoint. You can also perform the following operations on a shared object:

- Open the shared object by clicking the object name in the **NAME** column.
  - If you click a file name, the file will be opened in the browser and can be read.
  - If you click a folder name or library name, you can open this folder/library to view the content inside.
- Access the original URL of this shared object by clicking the link in the **URL** column.
- Click the settings ( ) button for a shared object in the **ACTION** column. The following actions are available:
  - **Manage Permissions** – To manage the permission settings of a shared file/folder/library, select this option. The **Manage Permissions** interface for this object appears. For detailed instructions on the operations in this interface, refer to Managing the Notification and Permission Settings for Shared Files, Folders and Libraries.
  - **View History** – To view the sharing history of a shared file/folder/library, select this option. The **View History** interface for this object appears. For details information on the operations in this interface, refer to Viewing History of Shared Files/Folders/Libraries.
  - **View Document Usage** – To view the usage of a shared file/folder/library by users via the AvePoint Perimeter External Portal and AvePoint Perimeter mobile apps, select this option to access the **View Document Usage** interface for the file/folder/library. In this interface, you can view activity details of the selected shared file or the files in the selected shared folder/library, including the time the user accessed the file, the action performed, the source of the access, and the shared file's URL in each activity.
  - **Download** – This option is used to download a copy of a shared file.
    - To download a shared file in the **Secure Share Details** interface, click the settings ( ) button for this file and then select **Download** from the drop-down menu.
    - To download a file inside a share folder or library, expand the folder or library to display the desired file, click the settings ( ) button for this file, and then select **Download** from the drop-down menu.

Managing Shared Links

You can manage the links of the shared items in Perimeter Internal Portal, if you have shared items for anonymous access or passcode access verification. In the **Manage Shared Links** page, you can stop sharing a link, update the expiration time of the links, and track the links' usage.

Follow the instructions below:

1. Click the settings ( ) button in the upper-right corner and then select **Manage Shared Links**. The table displays all of the items and their links you shared for the **Accessible to anyone through links** secure share type and the **Verify viewers via passcode** secure share type.
2. You can perform the following actions:
    - Edit the expiration time – Select the checkbox ahead of the item name, and then click **Edit** on the ribbon. In the **Edit** window, the expiration time of this link is displayed. You can change the expiration time by selecting another date from the calendar. Click **Save** to save your changes, or click **Cancel** to exit this window without saving any changes.
    - Remove the link – If you want to stop the sharing of a link, select the checkbox ahead of the item name, click **Remove** on the ribbon, and then click **OK** in the confirmation window.
    - Track the link usage – You can track when the shared link was accessed and by whom. Select the checkbox ahead of the item name, and then click **Link Usage Tracking** on the ribbon.

Managing Virtual Folders

If you use virtual folders to categorize the sharing for specific users, you can manage the virtual folders you share with them in the Internal Portal.

Follow the instructions below:

1. Click the settings ( ) button in the upper-right corner and then select **Manage Virtual Folders**.
2. In the **Manage Virtual Folders** page, all of the virtual folders you shared are listed in the table. You can view the virtual folder name and the users or groups that shared with the corresponding folder.
3. You can perform the following actions on a virtual folder by clicking the action ( ) button in the **ACTION** column.
    - Rename a virtual folder. Select **Rename** from the **ACTION** list. In the **Rename** window, enter the new folder name into the **New Name** box. Click **Rename** to save your changes.
    - Remove a virtual folder. Select **Remove** from the **ACTION** list and then confirm your deletion.

Managing Pending Access Requests

The users who do not have permission to the items that you shared can submit an access request to you while accessing the secure share link of that item. Complete the steps below to view and process the your pending access requests:

1. Click the settings ( ) button in the upper-right corner and then select **Manage Pending Access Requests**. All of your pending access requests are listed in the table.
2. Select one or more requests and click **Approve** or **Reject**.

   ***Note**: You cannot select the access requests for the folders and files at the same time to approve.

   - If you want to reject the access request, leave your comments in the pop-up window and click **Reject**. An e-mail with your comments will be sent to the requester for notification.
   - If you want to approve the access request, configure the Secure Share settings in the pop-up window and click **Approve**. For details on each setting, refer to Managing the Notification and Permission Settings for Shared Files, Folders, and Libraries.

Before You Use the AvePoint Perimeter External Portal

Before you use the AvePoint Perimeter External Portal, read the instructions below.

- For the secure shares that do not require permission and passcode verification, anyone with the link to the shared items can access the shared items anonymously. If the secure share requires a passcode verification, you must provide your e-mail address to receive a passcode, and then provide the passcode to the Perimeter External Portal within 30 minutes for verification.
- If you are using the AvePoint Perimeter system as an external user and you are required to sign into the External Portal to access the shared items, see Registering to the AvePoint Perimeter External Portal to register a user account for the AvePoint Perimeter External Portal.
- If you have already enrolled mobile devices into the AvePoint Perimeter system as an external user, the **Organization E-mail Address** included in the **AvePoint Perimeter Device Enrollment** e-mail sent by your AvePoint Perimeter administrator is your AvePoint Perimeter user account. This account can be used to access the AvePoint Perimeter External Portal after you set a password for this account by following the instructions in Setting a Password in the AvePoint Perimeter External Portal.
- If you are an internal user of the AvePoint Perimeter system or an external user already registered to the AvePoint Perimeter External Portal, see Logging into the AvePoint Perimeter External Portal.

Registering to the AvePoint Perimeter External Portal

To register a new AvePoint Perimeter External Portal account, complete the following steps:

1. Click the **SIGN UP** link in the **AvePoint Perimeter Secured Shared Notification** e-mail or access any Secure Share links of the shared items. The **Sign In** page of the AvePoint Perimeter External Portal appears.

   ***Note**: External users that do not have Secure Share items shared with them can also sign up to the Perimeter External Portal if the Perimeter administrator has enabled it through the configuration file.

   If an external user sends the secure share links of the shared items they received in the Secure Share e-mail to another external user and the user who wants to access the items does not have permission, this user can submit an access request for the shared item. An e-mail notification will be sent to the internal user who shared this item with the external user to process the access request. If more than one internal user has shared this item, the internal user who most recently shared this item will receive this task.

2. Click **Sign Up** to access the **Account Registration** interface.

3. Configure the following settings for the new account:
    - **Create a User ID** – Set up a user ID that will be used to access the AvePoint Perimeter External Portal.
        i. Enter a valid e-mail address or a username in the **User ID/E-mail Address** text box. This e-mail address or username will become your login ID for accessing the AvePoint Perimeter External Portal.
        ii. Enter the password for this user ID in the **Password** text box and enter it again to confirm the password in the **Confirm Password** text box.
    - **Contact Information** – Configure the related contact information for the user account in the following fields:
        - **First Name** – Enter your first name.
        - **Last Name** – Enter your last name.
        - **Country/Region** – Select your country or region. When selecting **United States**, the **State/Province** field will appear, from which you also need to select your state or province.
        - **Phone Number** – Enter your phone number.
        - **Organization** – Enter your organization name.
        - **Address** – Enter your address.
        - **City** – Enter the name of your city.
        - **Postal Code** – Enter your postal code.
4. Enter the verification code into the **Verification** text box. Click **Refresh** to refresh the verification code if there is no image.
5. Click the **terms and conditions** link to review the AvePoint Website Terms and Conditions. Click the **privacy policy** link to review the AvePoint Website Privacy Policy. After you have read the terms and conditions/privacy policy, select **I have read and accept the terms and conditions and privacy policy** checkbox.
6. Click **Register** to register a new user account. Upon registering, a registration confirmation e-mail is sent to the e-mail entered in the **User ID (e-mail address)** section. Once you receive the e-mail message, click the supplied link to activate your account. After clicking the link, you will be redirected to the AvePoint Perimeter External Portal **Sign In** page.

Logging into the AvePoint Perimeter External Portal

To log into AvePoint Perimeter External Portal, complete the following steps:

1. Open the URL for the shared content in the **AvePoint Perimeter Secured Share Notification** e-mail using the browser. The **Sign In** page for AvePoint Perimeter External Portal appears.
2. Enter your login information:

- If you have registered an AvePoint Perimeter External Portal account, the user ID is automatically populated in the **Username** field. Enter the password into the **Password** field to log into the External Portal.
- If you are an internal user, you can either enter your Active Directory credentials or enter the e-mail address and password to log into the External Portal.

***Note**: If the default authentication type for signing into the External Portal is **Windows Authentication**, internal users can automatically sign in with their Windows account and external users must change the authentication type to **Form Based Authentication** and enter their username and password for login.

***Note**: Click the **Forgot password?** link in the following conditions:

- If you already have an external user account for the AvePoint Perimeter system by enrolling mobile devices but haven't set a password for your account, click the **Forgot password?** link to set a password for your account.
- If you already registered a user account for AvePoint Perimeter External Portal but forget your password, click the **Forgot password?** to set your password.

  For detailed instructions, see Setting a Password in the AvePoint Perimeter External Portal.

3. Click **Sign in** to access the AvePoint Perimeter External Portal.

Setting a Password in the AvePoint Perimeter External Portal

To set a password for an AvePoint Perimeter external user account for the first time, or reset the password for an AvePoint Perimeter External Portal account, complete the steps below:

1. Go to the **Sign In** page of AvePoint Perimeter External Portal and click **Forgot password?** The **Reset Your Password** interface appears.
2. Enter the following information:
   a. **User ID** – Enter the e-mail address or username that you used for logging into the AvePoint Perimeter External Portal.
      - If you already have an external user account for the AvePoint Perimeter system by enrolling mobile devices but haven't set a password for your account, enter the **Organization E-mail Address** included in the **AvePoint Perimeter Device Enrollment** e-mail sent by AvePoint Perimeter administrator.
      - If you already registered an AvePoint Perimeter External Portal account, enter the **User ID** you configured in the **Account Registration** page.

   b. **Verification** – Enter the verification code. Click **Refresh** to refresh the verification graphic if no image is displayed.

3. Click **Submit**. After submitting, an **AvePoint Perimeter External Portal - Reset Password Confirmation** e-mail is sent to the e-mail address you entered.

4. Retrieve the e-mail message and click the supplied link to set a new password. After clicking the link, you will be redirected to the **Reset Your Password** page. Enter the following information in this page:

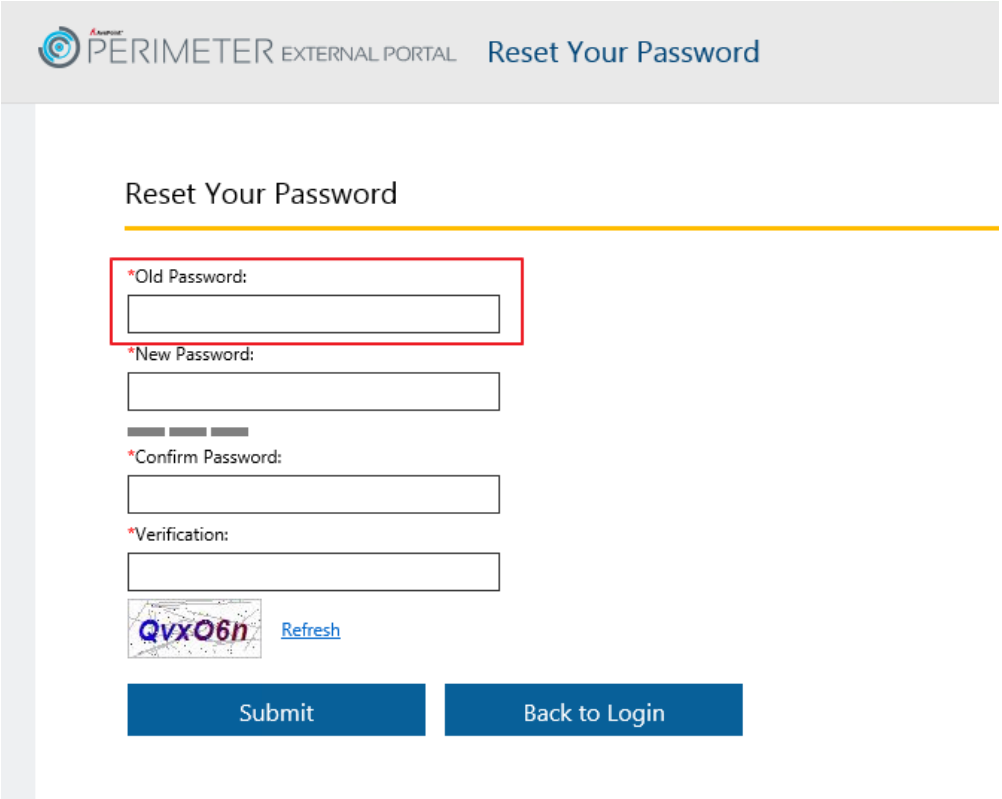

Figure 3: The Reset Your Password page.

   a. **Old Password** – enter your old password.

   b. **New Password** – Enter a new password.

   c. **Confirm Password** – Enter the new password again for confirmation.

   d. **Verification** – Enter the verification code. Click **Refresh** to refresh the verification graphic if no image is displayed.

5. After setting up the new password, click **Submit** to save your new password, and then click **OK** in the pop-up window. You are redirected to the **Sign In** page. Log into the AvePoint Perimeter External Portal with the new password.

Using the AvePoint Perimeter External Portal

In the AvePoint Perimeter External Portal, both the internal users and external users can access the content shared with them using the **My Files** interface, manage their enrolled devices, enroll new devices into the AvePoint Perimeter system, and external users can reset their password. See the sections below for instructions on using the AvePoint Perimeter External Portal.

***Note**: If the **Enroll New Device** feature is disabled by the Perimeter administrator, it will be not available for users in the External Portal.

Using the My Files Interface

In the **My Files** interface, you can perform the following:

- View the **NAME**, **LAST MODIFIED TIME**, and **EXPIRATION TIME** of each shared file/folder/library in the display pane.
- Search for shared files/folders/libraries by keywords using the **Search** box with the search criteria of **All Folders** or **Current Folder**.
- Access the shared files/folders/libraries, and perform additional operations on the shared content according to the permission you have.

Follow the instructions below to access the shared file/folder/library.

Accessing Shared Files from the My Files Interface

In the **My Files** interface, you can access the files that have been shared with you and perform additional operations on the shared content according to the permissions you have by following the instructions below:

***Note**: If the site or the Web application where the site resides has watermark settings configured, the files shared to the external users with Read-Only or Download permission level will be protected with watermark. If the shared file protected with watermark settings is viewed or downloaded, the file will be converted to PDF with the watermark settings applied.

- To open a file in your browser, click the desired file name in the **NAME** column.
    - If the file is opened in a web page after it is converted to a PDF file, see Viewing Files with the Online PDF Viewer for detailed instructions on the operations on this page.
    - If the file is opened in an Office Web App (Word Web App, Excel Web App, PowerPoint Web App), you can view the original file in the App. According to the level of permission that you are assigned, you will be able to download, print, and/or edit the file using the App.

***Note**: If you open an XLSX file in Internet Explorer 11 using the Microsoft Excel Web App, the **EDIT IN BROWSER** button used for enabling editing of the file may not work due to an Internet Explorer 11 compatibility issue with the Microsoft Excel Web App. To resolve this issue, contact your AvePoint Perimeter system administrator to follow the instructions in Enabling the EDIT IN BROWSER Feature of the Microsoft Excel Web App in Internet Explorer 11.

- To perform additional operations on a shared file, expand the action menu by clicking the settings ( ) button for the desired file in the **ACTION** column. A drop-down menu appears, including the options for the actions that you can perform on this file based on your permissions.
    - **Download** – This option is available when you have permission to download this file. To download a copy of this file, select this option and then use the download bar or download window to download this file to your local computer.
    - **Download & Lock for Editing** – This option is available when you have permission to edit the file and enables you to download the file, lock it for editing, and upload the modified file to overwrite the existing file. For more details, follow the instructions in Editing a Shared File by Overwriting it.
    - **Unlock** – This option is available when the file is locked for editing by you. To unlock this file, select this option.
    - **Upload Edited File** – This option is available when you have permission to edit the file and enables you to upload an edited version to overwrite this file. For more details, follow the instructions in Overwriting an Existing Shared File.
    - **Delete** – This option is available when you have the permission to delete the file. If you delete a file from the External Portal, that file will be automatically removed from SharePoint. Note that the locked file cannot be deleted.
    - **Properties** – This option is available to all users the file is shared with. Select this option to view the properties of the file. The **Properties Information** area will appear, displaying the properties of the item shared with you.

Accessing Shared Folders and Libraries from the My Files Interface

Shared folders and libraries are all displayed as folders in the **My Files** interface. To access a shared folder or library, click the corresponding folder/library name in the **NAME** column. Within the expanded folder/library, you can view all of the files and sub folders included in this shared folder/library, and open sub folders to view the included files by clicking the sub folder names in the **NAME** column.

Within an expanded shared folder/library, you can access each individual file and perform further operations on the files or the folder/library according to the permissions you have by following the instructions below:

- To open a file in your browser, click the desired file name in the **NAME** column.

- If the file is opened in a web page after it is converted to a PDF file, see Viewing Files with the Online PDF Viewer for detailed instructions on the operations on this page.
- If the file is open in an Office Web App (Word Web App, Excel Web App, PowerPoint Web App), you can view the original file in the App. According to the level of permission that you are assigned, you will be able to download, print, and/or edit the file using the App.

***Note**: If you open an XLSX file in Internet Explorer 11 using the Microsoft Excel Web App, the **EDIT IN BROWSER** button used for enabling editing of the file may not work due to an Internet Explorer 11 compatibility issue with the Microsoft Excel Web App. To resolve this problem, contact your AvePoint Perimeter system administrator to follow the instructions in Enabling the EDIT IN BROWSER Feature of the Microsoft Excel Web App in Internet Explorer 11.

- To perform further operations on a shared file, expand its action menu by clicking the settings ( ) button for the desired file in the **ACTION** column. A drop-down menu appears, including the options for the actions that you can perform on this file based on your permissions.
  - **Download** – This option is available when you have permission to download files from the shared folder/library. To download a copy of the file, select this option and then use the download bar or download window to download this file.
  - **Download & Lock for Editing** – This option is available when you have permission to edit files in the shared folder/library and enables you to download the file, lock it for editing, and upload the modified file to overwrite the existing file. For more details, follow the instructions in Editing a Shared File by Overwriting it.
  - **Unlock** – This option is available when the file is locked for editing by you. To unlock this file, select this option.
  - **Upload Edited File** – This option is available when you have permission to edit this file and enables you to upload an edited version to overwrite this file. For more details, follow the instructions in Overwriting an Existing Shared File.
  - **Delete** – This option is available when you have permission to delete the file. If you delete a file from External Portal, that file will be automatically removed from SharePoint. Note that a locked file cannot be deleted.
  - **Properties** – This option is available to every user with whom this folder/library is shared. To view the properties of this file, select this option, the **Properties Information** area will appear below, displaying the properties shared with you.
- **Upload** – This link is available on the ribbon when you have permission to edit the currently opened folder/library. Using the **Upload** link on the ribbon, you can upload files in the following two methods:
  - Uploading a New File to a Shared Folder or Library

- Overwriting an Existing Shared File

- **New Folder** – If you have the Edit permission to a shared folder or library, the **New Folder** feature is available to you within the shared folder or library. For details on creating a new folder within a shared folder or library, refer to Creating a New Folder in a Shared Folder or Library.

Enabling the EDIT IN BROWSER Feature of the Microsoft Excel Web App in Internet Explorer 11

If you open an XLSX file in Internet Explorer 11 using the Microsoft Excel Web App, the **EDIT IN BROWSER** button used for enabling editing of the file may not work due to an Internet Explorer 11 compatibility issue with the Microsoft Excel Web App. To resolve this issue complete the following steps:

1. Go to the *…\Microsoft Office Web Apps\ExcelServicesWfe_layouts* directory on the Office Web Apps server of your AvePoint Perimeter system.
2. Copy and paste the **XLViewerInternal.aspx** file to another location as a backup.
3. Open the **XLViewerInternal.aspx** file using Notepad under the *…\Microsoft Office Web Apps\ExcelServicesWfe_layouts* directory.
4. Within the **<head>** node, locate the **<meta>** sub node that contains the **http-equiv** and **content** attributes.
5. Change the value of the **content** attribute to **IE=10**.

```
<%-- Copyright (c) Microsoft Corporation. All rights reserved. --%>

<%@ Register Tagprefix="Ewa" Namespace="Microsoft.Office.Excel.WebUI"
Assembly="Microsoft.Office.Excel.WebUI.Internal, Version=15.0.0.0, Culture=neutral,
PublicKeyToken=71e9bce111e9429c" %>

<%@ Assembly Name="Microsoft.Office.Excel.WebUI.Internal, Version=15.0.0.0,
Culture=neutral, PublicKeyToken=71e9bce111e9429c" %>
<%@ Page language="C#" Codebehind="XlViewerInternal.aspx.cs" AutoEventWireup="false"
Inherits="Microsoft.Office.Excel.WebUI.XlViewerInternal,Microsoft.Office.Excel.WebUI.Intern
al,Version=15.0.0.0,Culture=neutral,PublicKeyToken=71e9bce111e9429c" %>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" dir="<%= HtmlDirection%>">
        <head runat="server">
                <meta http-equiv="X-UA-Compatible" content="IE=10" />
                <meta name='viewport' content='width=device-width, initial-scale=1' />
                <link rel="shortcut icon" type="image/vnd.microsoft.icon"
id="m_shortcutIcon"/>
```

Figure 3: Changing the value of the content attribute to IE=10.

6. Save the change and close the file.

Viewing Files with the Online PDF Viewer

If you open a file in a web page, it is converted to a PDF file and displayed in the online PDF viewer. If the site where the shared file resides has applied the watermark settings, the configured watermark text will

be displayed on each page for document protection. You can view the file from the display area and perform the following operations:

- Change page scaling – To change the page scaling, click the **Fit Width** ( ) button or the **Fit Height** ( ) button, or use the scale bar.
- Rotate page – To rotate the page, click the **Rotate** ( ) button.
- Change page display mode – To change the page display mode, click one of the following buttons: **Single Page** ( ) button, **Two Pages** ( ) button, and **Thumb Views** ( ) button.
- **Print** – To print the opened file, click the **Print** ( ) button, select the print range from the **Select print range** pop-up window, and then click **Print**.

  ***Note:** This button is only available when you have permission to print this file.

- **Download** – To download the opened file, click the **Download** ( ) button and then use the pop-up download bar or download window to download this file to your local computer.

  ***Note:** This button is only available when you have permission to download this file. Additionally, if the site where the shared file resides has configured watermark settings, the file will be automatically converted to PDF with watermark settings applied.

Editing a Shared File by Overwriting it

To edit a file by downloading the file, editing the downloaded file, and uploading the modified file back to the External Portal, complete the following steps:

1. Go to the **My Files** interface or the shared folder/library where the file resides and click the settings ( ) button for this file in the **ACTION** column. A drop-down menu appears.
2. Select the **Download & Lock for Editing** option, the file becomes locked for editing by you and cannot be edited by other users. The **(You are editing this file.)** message appears below the file name and a download bar or window appears.
3. Download a copy of the file, and edit the downloaded file on your local computer.
4. After you finish editing the downloaded file, follow the instructions Overwriting an Existing Shared File to upload the modified file to the **My Files** interface or shared folder/library to overwrite the existing shared file. The changes made to the shared file on the External Portal will be synchronized to the original file in SharePoint. If you do not want to make any changes to the locked shared file, you can unlock it by clicking the settings ( ) button of this file in the **ACTION** column and selecting **Unlock** from the drop-down menu.

Uploading a File

The sections below provide detailed instructions on using the **Upload** feature in a shared folder/library to upload files and the **Upload Edited File** feature to overwrite a shared file. These features above are only available to you when you have the Edit permission to a shared folder or library.

You can also use the drag-and-drop feature to drag one or more files from your local computer and drop them into the External Portal to upload the new file to a shared folder or library, or upload edited files for replacement.

***Note**: this drag-and-drop feature only works when you browse the AvePoint Perimeter External Portal using Internet Explorer 10 or later, Google Chrome, or Firefox.

Uploading Files to a Shared Folder or Library

To upload new files or edited files into a shared folder or library, complete the following steps:

1. Open the shared folder/library where you want to upload files.
2. Click **Upload** on the ribbon. The **Upload** window appears.
3. Click **Browse**, select the files that you want to upload from the **Open** window, and click **Open**.
4. Click **Upload** to upload the selected files. If there are existing files in the shared folder or library, a window will appear asking you whether or not to replace the existing file or skip the upload. You can click **Replace** to upload the selected file to replace the existing one or click **Skip** to cancel the upload.

The uploaded file will be added to the shared folder/library on the External Portal and then synchronized to the original folder/library in SharePoint. In this way, the newly uploaded file is shared with all of the users who have access to the original folder/library in SharePoint from the External Portal.

Overwriting an Existing Shared File

To overwrite an existing shared file, complete the following steps:

1. Go to the **My Files** interface or the folder/library that contains the shared file you want to overwrite.
2. Open the **Upload** window in either of the following methods:
    - Method **1**: In the **My Files** interface or the shared folder/library, click the settings ( ) button of the file you want to overwrite in the **ACTION** column and select **Upload Edited File** from the drop-down menu. Using this method, you can only upload an edited version of this file.
    - Method **2**: In the shared folder/library, click **Upload** on the ribbon. The **Upload** window appears. Using this method, you can upload an edited version of any existing file within the folder/library.

3. Click **Browse**, select the modified file that you want to upload from the **Open** window, and click **Open**.
4. Verify that the **Overwrite existing file** checkbox in the **Upload** window is selected.

   ***Note**: If you open the **Upload** window by selecting the **Upload Edited File** option, the **Overwrite existing file** is selected by default and cannot be deselected.

5. Click **Upload** to upload the selected file.

The existing shared file will be overwritten by the uploaded file, and the changes will be synchronized to the original file in SharePoint.

Creating a New Folder in a Shared Folder or Library

Within a shared folder or library, a user who has the **Edit** permission can create a new folder or a nested folder structure in the shared folder or library for grouping the new files to be uploaded.

To create a folder, open a folder or library and then click **New Folder** on the ribbon. Enter the folder name and click **Save**.

***Note**: If you browse the Perimeter External Portal via Google Chrome, you can drag and drop folders to upload the folders and the files and folders within them.

Operations Available on the Username Menu

When you click the username displayed in the upper-right corner, a drop-down menu opens. The following options are available in the drop-down menu:

- **Manage My Devices** – Click this option to access the **My Devices** interface to view information regarding the mobile devices you have enrolled in the AvePoint Perimeter system. You can perform the following tasks in this interface:
  - **View enrolled devices** – In the display pane, you can view all of your enrolled devices with the following detailed information: **DEVICE NAME**, **MODEL**, **OPERATING SYSTEM**, **REGISTRATION TIME**, and **STATUS**. With an enrolled device, you can view the files/folders/libraries on your iOS/Android device using the AvePoint Perimeter mobile app.
  - **Enroll New Device** – To enroll a new device into the AvePoint Perimeter system, click the **Enroll New Device** link on the ribbon, and click **OK** in the pop-up confirmation window. The Perimeter system will send a device enrollment request e-mail to the e-mail address that is used as your user ID (if you are an external user) or your e-mail address that is stored in the Active Directory Domain Controller (if you are an internal user). You can enroll your mobile device by following the instructions in the request e-mail.

    ***Note**: If the **Enroll New Device** feature is disabled by the Perimeter administrator, this link will be not available for users in the External Portal.

- **Back to Files** – To return to the **My Files** interface, click **Back to Files** on the ribbon.

- **Enroll New Device** – The function of this option is the same as that of the **Enroll New Device** link in the **My Devices** interface.

  ***Note**: If the **Enroll New Device** feature is disabled by the Perimeter administrator, this link will be not available for users in the External Portal.

- **Reset Password** – Select this option to change your password. The **Reset Your Password** page will appear. If your Perimeter administrator enabled the External User Password Policy and applied password complexity requirements, you must enter a password meeting those requirements.

- **Log Out** – To log out of the AvePoint Perimeter External Portal, select this option and click **OK** in the pop-up confirmation window.

Appendix A: Integrating the AvePoint Perimeter External Portal with SAP Jam

With an XML file applied to a SAP Jam group, SAP Jam group can integrate with AvePoint Perimeter External Portal to allow the following features:

- SAP Jam group owners with whom the SharePoint folders are shared can assign the SharePoint folders to all of the members in that SAP Jam group. For detailed instructions, refer to SAP Jam Group Owners.
- The SAP Jam group members can access the files or folders within the assigned folders in the AvePoint Perimeter External Portal after the group members registered and logged into the External Portal. The group members can perform additional actions to the files in the assigned folder, since they have the same permission as the group owner. For detailed instructions, refer to Jam Group Members.

***Note**: In the integrated AvePoint Perimeter External Portal, group members can only view or operate the files in the folders assigned by the group owner. If there are other items that are shared with a group member through the AvePoint Perimeter Secure Share feature, the group member must log into the organizations' Perimeter External Portal as an external user to view and operate the shared items.

***Note**: This feature is not supported on AvePoint Perimeter Mobile app.

Before you get started, note the following:

- Check whether or not the XML file is ready to be used. The default URL of this XML file is *http://[ExternalPortal:port]/portal/home/SAPJAMXML*. If the XML file cannot be accessed, contact the Perimeter administrator for help.
- If you use Google Chrome, make sure the **Block third-party cookies and site data** option is deselected.

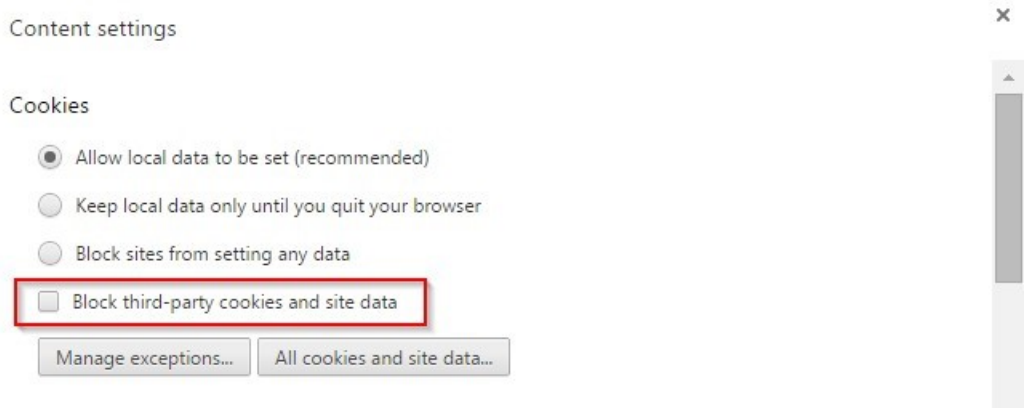

Figure 4: Ensuring that the Block third-party cookies and site data option is deselected.

- If you narrow the browser window, the **Sign In** section in the Perimeter login page may move down on the page, which may partially block the credentials form.

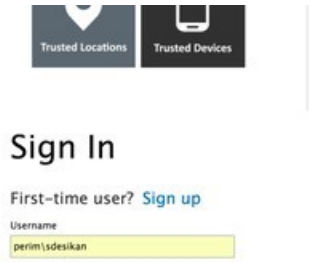

Figure 5: The Password box is blocked.

SAP Jam Group Owners

SAP Jam users can create a group to integrate with AvePoint Perimeter. For details, refer to Creating a SAP Jam Group Integrated with Perimeter.

The user who created a group in SAP Jam will be the owner of this group. The owner of a group that is integrated with AvePoint Perimeter will have access to the following feature:

- If anyone shares SharePoint folders with SAP Jam group owners via AvePoint Perimeter Secure Share, the group owner can assign the shared folder to all of the members in this group through the integrated AvePoint Perimeter External Portal. For details on assigning a shared folder on the AvePoint Perimeter External Portal, refer to Assigning Folders.

Creating a SAP Jam Group Integrated with Perimeter

Complete the steps below to create a SAP Jam group that is integrated with AvePoint Perimeter:

1. After you log into SAP Jam, click **Groups** on the ribbon, and then select **Create a Group** from the drop-down list to create a new group.

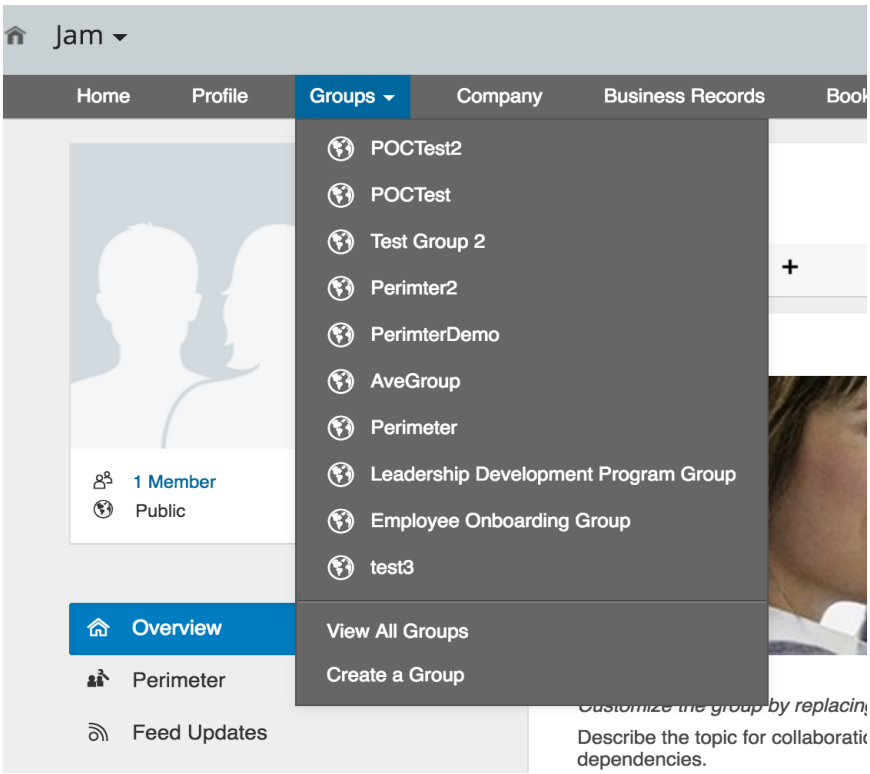

Figure 6: Clicking Groups.

2. Follow the instructions on the **Create a Group** window to create and activate your group.
3. Click your login name on the top menu, and select **Jam Admin** from the drop-down list.

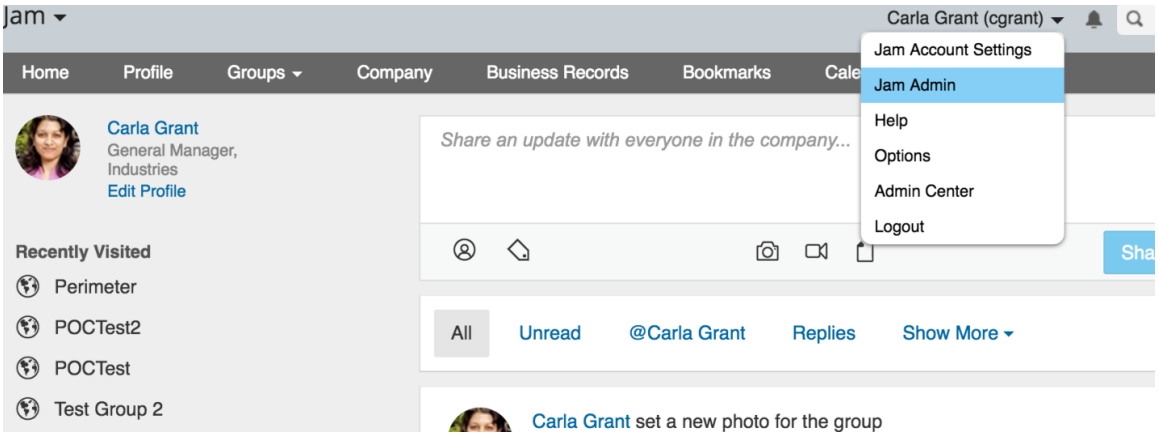

Figure 7: Selecting Jam Admin.

4. In the **Admin** interface, click **Integrations** on the left pane, and then click **OpenSocial Gadgets**.

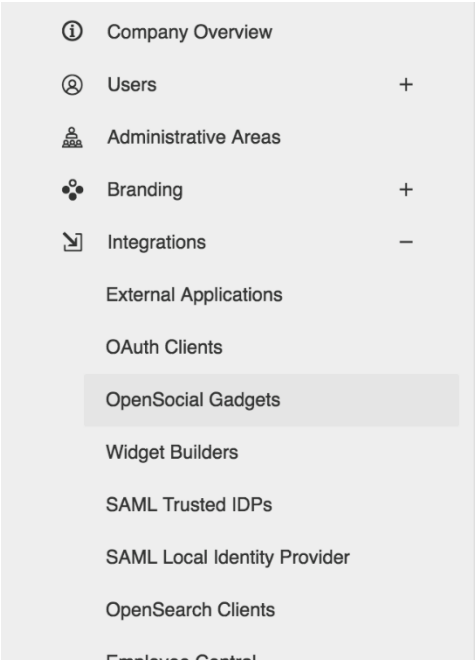

Figure 8: Clicking OpenSocial Gadgets.

5. Click **Add Gadget**. The **Register OpenSocial Gadget** interface appears.

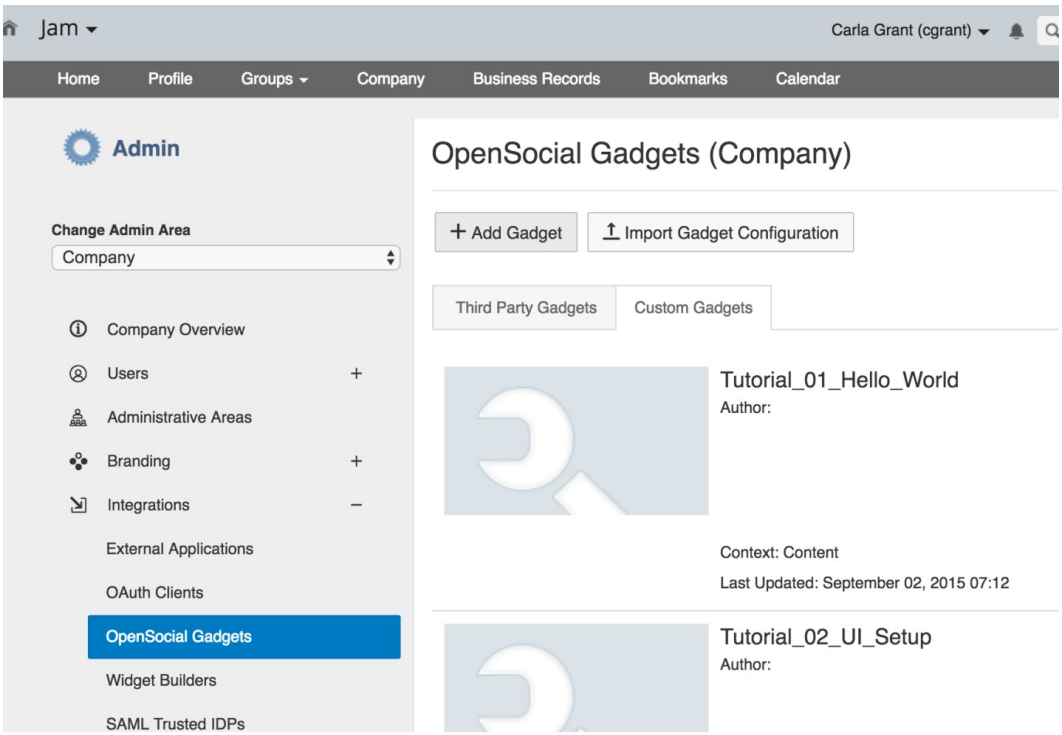

Figure 9: Clicking Add Gadget.

6. Enter the URL of the XML file into the **URL** field, and select **Group** from the **Context** drop-down list to create the OpenSocial gadget.

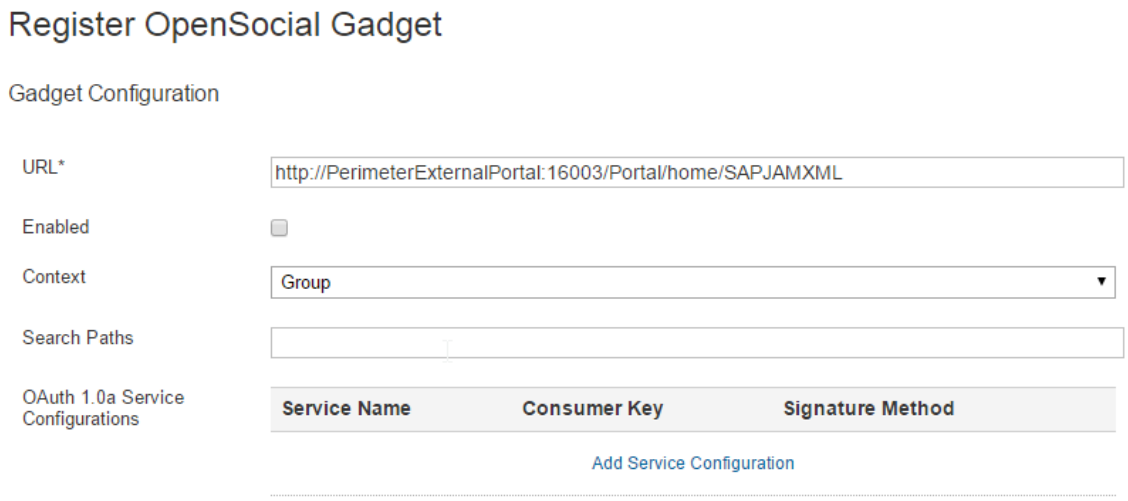

Figure 10: Configuring OpenSocial gadget.

7. Click **Save** to save this gadget.
8. Click **Groups** on the ribbon and select the group that you want to integrate with AvePoint Perimeter.

9. Click **Group Admin** on the bottom of the left pane and select **Edit Group** from the drop-down list. The **Edit Group** interface appears.

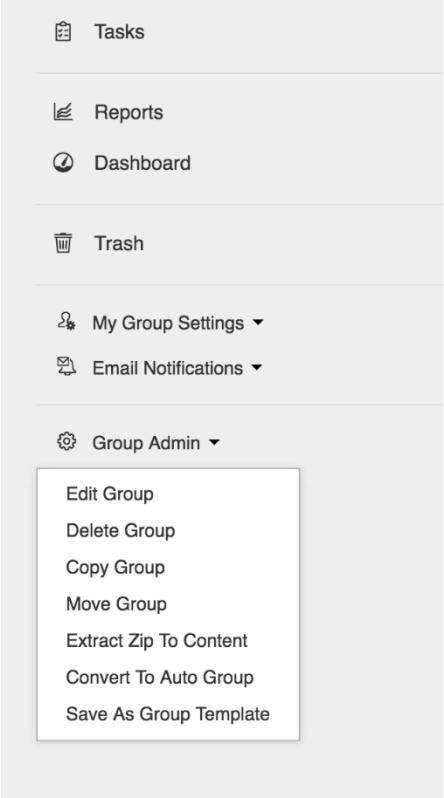

Figure 11: Clicking Group Admin.

10. Click the **Setup** tab on the **Edit Group** interface.

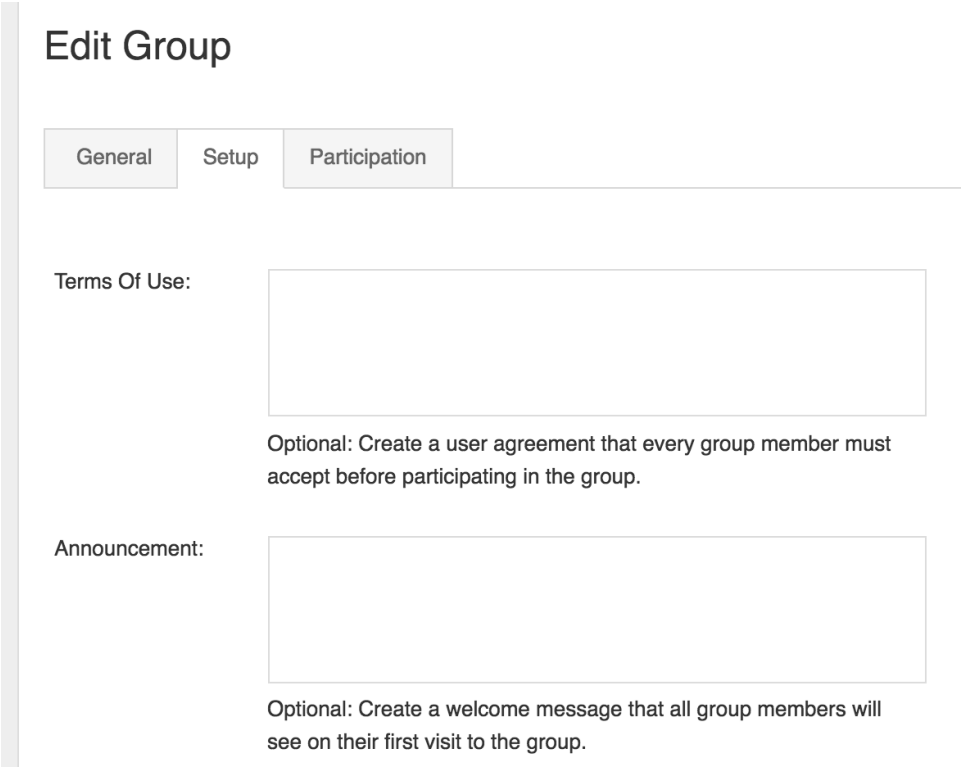

Figure 12: Clicking the Setup tab.

11. In the **Select Primary Group Extension** field, select the **Perimeter** gadget.
12. Click **Save changes** to save your configurations to this group. The group owner can now assign a shared SharePoint folder to all of the members in this group via the AvePoint Perimeter External Portal, and the members in this group will have the same permissions as the owner has to the shared folder.

Assigning Folders

The **Assign Folder** feature is an action that you can perform on the shared folder. The folder will be assigned to the SAP Jam group members, therefore, the group members will have the same permission as you have to the shared folder.

***Note**: This action does not support the nested folders in the shared folder.

Complete the steps below to assign a folder to group members:

1. Search or locate the folder, and then click the actions ( ) button in the **ACTION** column next to this folder.

2. Select the **Assign Folder** option from the drop-down list. A message will appear informing you whether or not the folder has been successfully assigned. You can go to the **My Assigned Files** interface to view the files in the assigned folder, and you can also perform actions to the files according to your permission. For more details on using the AvePoint Perimeter External Portal, refer to Using the AvePoint Perimeter External Portal.

   ***Note**: If you want to stop the Jam group members from accessing the files within the assigned folders, you can select the **Unassign Folder** option from the drop-down list.

Jam Group Members

In the **My Files** interface of the AvePoint Perimeter External Portal, you can view the files within the assigned folder if your SAP Jam group owners have assigned SharePoint folders that are shared with them; you can also perform actions to those files that you have the same permission for as your group owner. For details on using the AvePoint Perimeter External Portal, refer to Using the AvePoint Perimeter External Portal.

***Note**: In the integrated AvePoint Perimeter External Portal, group members can only view or operate the files in the folders assigned by the group owner. If there are other items that are shared with a group member through the AvePoint Perimeter Secure Share feature, the group member must log into the organizations' Perimeter External Portal as an external user to view and operate the shared items.

Notices and Copyright Information

AvePoint, Inc.
525 Washington Blvd
Suite 1400
Jersey City, New Jersey 07310
USA