

AvePoint Perimeter 1.9.1

Administrator Guide

Issued February 2018

Table of Contents

What's New in this Guide	10
About AvePoint Perimeter	11
AvePoint Perimeter Pro Features	11
Licensing AvePoint Perimeter	11
Installing AvePoint Perimeter	12
AvePoint Perimeter System Components Overview	13
AvePoint Perimeter Manager	16
AvePoint Perimeter Agent	17
AvePoint Perimeter Gateway.....	17
AvePoint Perimeter External Portal	17
Integrating Perimeter External Portal with SAP Jam Group	18
Installation and Publishing Scenarios for the External Portal and Gateway.....	19
AvePoint Perimeter WOPI Host Server	19
AvePoint Perimeter Secured Share Solution	20
AvePoint Perimeter Geolocation Database	20
Installation Scenarios for the Geolocation Database	20
Permission Requirements	21
Permission Requirements for AvePoint Perimeter Manager	21
Permission Requirements for Installing AvePoint Perimeter Manager.....	21
Permission Requirements for Logging into AvePoint Perimeter Manager.....	21
Permission Requirements for AvePoint Perimeter Agent	21
Permission Requirements for AvePoint Perimeter External Portal and Gateway.....	22
Permission Requirements for Logging into AvePoint Perimeter External Portal	23
Permission Requirements for Geolocation Database.....	24
Permission Requirements for AvePoint WOPI Host Server	24
System Requirements	25
Supported Environments	25
AvePoint Perimeter Manager Server Requirements	25
Configuring Your Firewall to Allow Push Notifications	26
AvePoint Perimeter External Portal and Gateway Server Requirements.....	28

AvePoint Perimeter Geolocation Database Server and Installation Wizard System Requirements	29
SQL Server Requirements for AvePoint Perimeter Databases	29
AvePoint Perimeter WOPI Host Server System Requirements	31
AvePoint Perimeter Agent Server Installation Requirements	32
Where to Install AvePoint Perimeter Agents	32
AvePoint Perimeter Agent Server Requirements	33
End-User Devices Supported by AvePoint Perimeter	33
Supported Browsers.....	34
Supported Browsers for AvePoint Perimeter Manager	34
Supported Browsers for AvePoint Perimeter Internal Portal and AvePoint Perimeter External Portal.	34
Supported File Types for Online Viewing on the AvePoint Perimeter Internal Portal and External Portal	35
AvePoint Perimeter Installation Overview	36
Purchased Versions of Perimeter	36
Trial Versions of Perimeter	36
Installing AvePoint Perimeter Manager.....	37
Installing AvePoint Perimeter Agents	39
Modifying Perimeter Agent Configurations.....	41
Installing AvePoint Perimeter External Portal and Gateway	41
Applying and Publishing the External Portal and Gateway.....	44
Publishing the External Portal and Gateway Directly	44
Publishing the External Portal and Gateway via Reverse Proxy	44
Installing Geolocation Database (optional)	44
Installing AvePoint Perimeter WOPI Host Server	46
Setting Up Your Firewall to Unblock Specific Ports	49
Configuring the Integration of the External Portal and SAP Jam Group.....	52
Updating Database Credentials	52
Isolating SharePoint Web Front-End Server from Perimeter External Portal and Gateway Server	53
Updating AvePoint Perimeter	54
Before Getting Started with the Update.....	54
Updating AvePoint Perimeter Manager and Agent Components Using the Perimeter Upgrade Solution	54
Launching the Perimeter Upgrade Solution.....	55

Running the Requirement Pre-Scan.....	55
Configuring Service Connection	55
Configuring Update Settings	56
Updating Services.....	56
Viewing Update History	58
Updating AvePoint Perimeter Pro Secured Share Solution	59
Logging into AvePoint Perimeter Management Console for the First Time	60
Changing Your Password.....	60
Remembering the Login Credentials for Automatic Sign-In	61
Overview of the Configurations in the AvePoint Perimeter Management Console.....	62
Configuring Perimeter General Settings	62
Configuring Perimeter Secure Share Pro Features	62
Configuring Content Access Control to SharePoint Sites.....	64
Deploying and Activating the AvePoint Perimeter Secured Share Feature.....	65
Deploying the AvePoint Perimeter Secured Share Solution on a SharePoint 2016 Farm	65
Deploying the AvePoint Perimeter Secure Share Solution on a SharePoint 2013 Farm	66
Deploying the AvePoint Perimeter Secured Share Solution on a SharePoint 2010 Farm	69
Activating the AvePoint Perimeter Secured Share Feature	70
Activating the AvePoint Perimeter Secured Share Feature in Site Settings	71
Activating the AvePoint Perimeter Secured Share Feature Using SharePoint Management Shell Command Lines.....	71
Dashboard Interface	73
Viewing All Access Logs.....	73
Viewing Internal Users' Last Locations	73
Viewing Access Logs Per Platform (Last 7 Days)	73
Viewing All Internal Devices.....	73
Viewing External Users' Last Locations.....	73
Viewing All External Devices	74
Configure Menu	75
Configuring System Settings	75
Using Agent Monitor.....	75
Configuring Geolocation Database Connection.....	76

Configuring IP Location Database	77
Using License Manager	77
Configuring External User Password Policy	79
Configuring Admin Accounts.....	80
Managing Permission Levels.....	80
Managing Admin Groups	82
Managing Admin Users	84
Configuring Secured Share.....	86
Configuring System Credentials.....	87
Configuring Shared File Location	88
Configuring Office Web Apps Server Settings.....	89
Configuring Secure Share Control Policy	90
Enabling SharePoint Permissions to Grant the Available Permission Levels.....	93
Configuring Watermark Settings.....	94
Configuring Content Access Control for Secure Share.....	95
Configuring Secure Share Options and Customizations	97
Sending Secured Share Notification E-mail as the Shared by User	98
Enabling Update Notification.....	98
Customizing the Threshold for Sending Reminder E-mail Notifications for Locked Shared Files on the External Portal.....	99
Allowing Users that are not Shared With to Sign Up to the External Portal	99
Defining the Default Expiration Duration for Secure Share via CONFIG File	100
Disabling Internal Users to Share Anonymous Access or Passcode-Verified Access	100
Defining the Minimum Interval for Sending a One-Time Access Passcode	101
Deleting Shared Items Permanently	101
Configuring Application Settings.....	102
Configuring General Settings	102
Configuring Notification Settings.....	104
Configuring ADFS Authentication	106
Configuring Account Lockout Policy	107
Log Manager	107
Configuring Monitoring Settings.....	109

Monitoring Timer Job Definition.....	109
Monitoring Timer Job Status.....	110
Configuring Windows Phone Log Location	110
Job Monitor Interface	112
Monitoring User Activity and Locations via Burglar Alarm Rules	113
Types of Burglar Alarm Rules	113
Configuring SharePoint Audit Settings for Document Activity Rules at the Web Application or Site Collection Level	114
Disabling All SharePoint Audit Events.....	116
Inheriting and Stop Inheriting of SharePoint Audit Settings.....	117
Retrieving Audit Data for Document Activity Rules.....	117
Configuring Audit Retrieval Settings for a Farm	118
Manually Retrieving Data from a Farm.....	119
Configuring Filter Rules for Excluding Specific Audit Data.....	119
Configuring Document Activity Collections	120
Editing a Document Activity Collection.....	121
Deleting Document Activity Collections	121
Configuring and Applying Burglar Alarm Rules	121
Creating or Editing Burglar Alarm Rules	123
Manage Menu.....	125
Enrolling a Device.....	125
Sending an Individual Device Enrollment Request	125
Sending Device Enrollment Requests in Bulk.....	127
Managing Enrollment Requests.....	127
End-User Device Enrollment	127
Managing Enrolled Devices.....	128
Managing the Status of Enrolled Devices	129
Viewing Enrolled Devices Details	131
Deleting Enrolled Devices	133
Publishing SharePoint Sites for Accessing via Enrolled Devices	134
Managing Device Groups	134
Configuring Site Access Permission for Enrolled Devices	136

Configuring Content Access Control for SharePoint Content via Any Devices	140
Configuring Location Groups	140
Configuring Locations	142
Configuring Content Access Policies	145
Managing Internal Users	152
Viewing User Details	152
Synchronizing Active Directory Users	153
Managing External Users	153
Adding External Users	154
Viewing User Details	155
Editing an External User Profile	155
Managing the Status of External Users	156
Managing Login Accounts	157
Viewing Login Account Details	158
Assigning a User for Login Accounts	158
Sharing Files with Groups of Users via Virtual Views	158
Managing User Access Groups	159
Configuring Virtual Views for Sharing Files in Bulk	161
Sharing Virtual Views with User Access Groups	164
Managing Shared Files	166
Viewing Sharing History	167
Viewing Document Usage	168
Changing Shared Permission Settings	168
Removing Users' Shared Permissions	169
Customizing the Size of the Online Read DWG File	170
Report Menu	171
Access Points	171
Viewing Access Points Report	171
Access Logs	171
Viewing Access Logs	172
Event Logs	172
Viewing Event Logs	172

Exporting Event Logs	173
Access Violation Logs	173
Viewing Access Violation Logs	173
Exporting Access Violation Logs.....	174
Access Warning Logs	174
Viewing Access Warning Logs	174
Exporting Access Warning Logs	174
2-Factor Authentication Logs.....	174
Viewing 2-Factor Authentication Logs	175
Exporting 2-Factor Authentication Logs	175
Burglar Alarm Report	175
Viewing Burglar Alarm Report	176
Exporting Burglar Alarm Report.....	176
Daily Audit Tracking	176
Viewing Daily Audit Tracking Report.....	176
Exporting Daily Audit Tracking Report	178
Advanced Search.....	178
Uninstalling AvePoint Perimeter.....	180
Uninstalling AvePoint Perimeter Manager	180
Uninstalling External Portal and Gateway	180
Uninstalling AvePoint Perimeter WOPI Host Server	181
Uninstalling AvePoint Perimeter Agents.....	181
Uninstalling the AvePoint Perimeter App from Your Device	181
Appendix A: Publishing the External Portal and Gateway	182
Publishing the External Portal and Gateway Directly	182
Publishing the External Portal and Gateway via Reverse Proxy	182
Configuring the Reverse Proxy for the External Portal and Gateway Overview.....	182
Installing Application Request Routing Feature and URL Rewrite Feature	182
Creating the Reverse Proxy's Website and Modifying the Web.config File	183
Disabling IIS Compression	185
Exporting and Importing the AvePoint Perimeter Certificate	186
Verifying the External and Gateway Server Certificate	190

Appendix B: AvePoint Perimeter and Location Data	193
How is the Location Services feature used?	193
What location data is obtained and when is it obtained?	193
What does Perimeter do with the location data?	193
How long does Perimeter keep the location data?	193
How do I secure this data on the backend?	193
Appendix C: Customizing AvePoint Perimeter E-mail Templates, E-mail Display Language, Web Pages, and Portals	194
Customizing E-mail Templates	194
Customizing the Logo Image of E-mail Templates	196
Customizing Text and Link URL of the Text in E-mail Templates	196
Customizing the Look and Feel of E-mail Templates	197
Customizing the E-mail Display Language.....	199
Customizing the Look and Feel of Web Pages	199
Customizing the Look and Feel of Web Pages for SharePoint On-Premises Sites	201
Customizing the Look and Feel of Web Pages for ADFS Authenticated Sites.....	202
Customizing Pictures in Web Pages	202
Customizing the Look and Feel of the Perimeter Management Console and Internal Portal Login Page	203
Customizing the Look and Feel of the Perimeter External Portal Login Page	205
Notices and Copyright Information	206

What's New in this Guide

- Added the following configurations in the **AppSettings.config** file.
 - o The option to allow internal users to share anonymous access or passcode-verified access to SharePoint content via Secure Share. For detailed instructions, refer to the [Disabling Internal Users to Share Anonymous Access or Passcode-Verified Access](#) section.
 - o The deletion operation can now be defined for users who are granted the **Delete** permission to shared items. To permanently delete shared items when deleting, refer to [Deleting Shared Items Permanently](#).

About AvePoint Perimeter

AvePoint Perimeter provides enterprise users with secure content access to SharePoint and file system assets from iOS devices (iPad, iPhone, or iPod Touch) or Android devices. This application works with the on-site AvePoint Perimeter Manager to allow secure offline viewing of SharePoint content from every endpoint. In addition, AvePoint Perimeter provides location/IP-based controls over content access to ensure that documents are only accessed from known or trusted locations and IP addresses, and uses iOS/Android/Windows Phone built-in Location Services features to provide pinpoint accuracy to the user's location. The application provides both 2-factor authentication by using a QR Code or access password and anonymous access to trusted users without the need for Active Directory (AD) or SharePoint accounts.

AvePoint Perimeter Pro Features

AvePoint Perimeter Pro offers two additional features over AvePoint Perimeter: **AvePoint Perimeter Secured Share** and **Virtual Views**.

Internal users can use the **AvePoint Perimeter Secured Share** feature to share files, folders, and libraries within SharePoint sites and configure permission controls for the shared documents. The people with whom the files are shared can view the shared files, folders, and libraries via AvePoint Perimeter External Portal or enrolled iOS/Android devices, edit shared files, synchronize the modified shared files back to the original files in SharePoint, and upload new files to shared folders or libraries in the AvePoint Perimeter External Portal. Additionally, Perimeter administrators can set up Content Access Control for Secure Share in the Perimeter Management Console to allow or deny internal/external user access to the shared content through Perimeter Portals or mobile devices by configuring the location or IP address rules.

Internal users can manage the files they share via the AvePoint Perimeter Internal Portal. Also, in AvePoint Perimeter Manager, administrators can manage all of the files shared through the **AvePoint Perimeter Secured Share** feature and can share files based on predefined criteria with groups of users via the **Virtual Views** feature. Refer to the [Configuring Perimeter Secure Share Pro Features](#) section for a brief overview of deploying and using Perimeter Pro features.

Licensing AvePoint Perimeter

AvePoint Perimeter (purchased or trial versions) automatically comes with a 30-day license for all features, including Perimeter Pro features, upon completion of the installation. When this 30-day license expires, a pop-up window appears to inform you that the license has expired and includes a link to the **License Manager**. At this point, you can only navigate to **License Manager** by clicking the URL in the pop-up window; you are not able to access any other interface in the Perimeter Manager until you apply a new valid license. For detailed information on applying a license, refer to [Importing and Exporting](#)

[License Files](#). To purchase a new license, contact your AvePoint account representative or visit the [AvePoint](#) website for more information.

***Note:** If applying a Perimeter Pro license to take advantage of Perimeter Pro features (**AvePoint Perimeter Secured Share** and **Virtual Views**), ensure that the **Secured Share** field is **Yes** in the **License Manager** interface after you apply your license.

***Note:** Even with an expired Perimeter Manager license, all of the AvePoint Perimeter mobile apps within this Perimeter management system will still work properly, as will all previously configured content access policies. However, system administrators cannot view or manage enrolled devices, or share files via the Virtual Views feature, nor can they view end-user access to SharePoint sites via the Perimeter Manager. Lastly, new end-users cannot enroll their mobile devices or share SharePoint files using the AvePoint Perimeter Secured Share feature.

Installing AvePoint Perimeter

The steps for installing AvePoint Perimeter depend upon the type of version you choose to install, a purchased version of Perimeter or a trial version of Perimeter. Users installing a trial version of AvePoint Perimeter will take slightly different steps to install than those who have purchased the product. Users who install a trial version will have Perimeter up and running quickly in their environment, however this is not the most secure or AvePoint recommended method of installation. For detailed information on the different ways you can install AvePoint Perimeter, refer to [AvePoint Perimeter Installation Overview](#) and [Installing AvePoint Perimeter](#).

AvePoint Perimeter System Components Overview

The AvePoint Perimeter management system consists of the following components: Manager, Gateway, External Portal, Geolocation Database, WOPI Host Server, Agent, and Secured Share solution.

Below are detailed architectural diagrams that outline the workflow processes for the following Perimeter System components: Internal/External user access to Perimeter through secured share, ports used by Perimeter for installation alongside Active Directory and Exchange, ports used for Perimeter to and from the Internet and Perimeter's mobile device interaction framework.

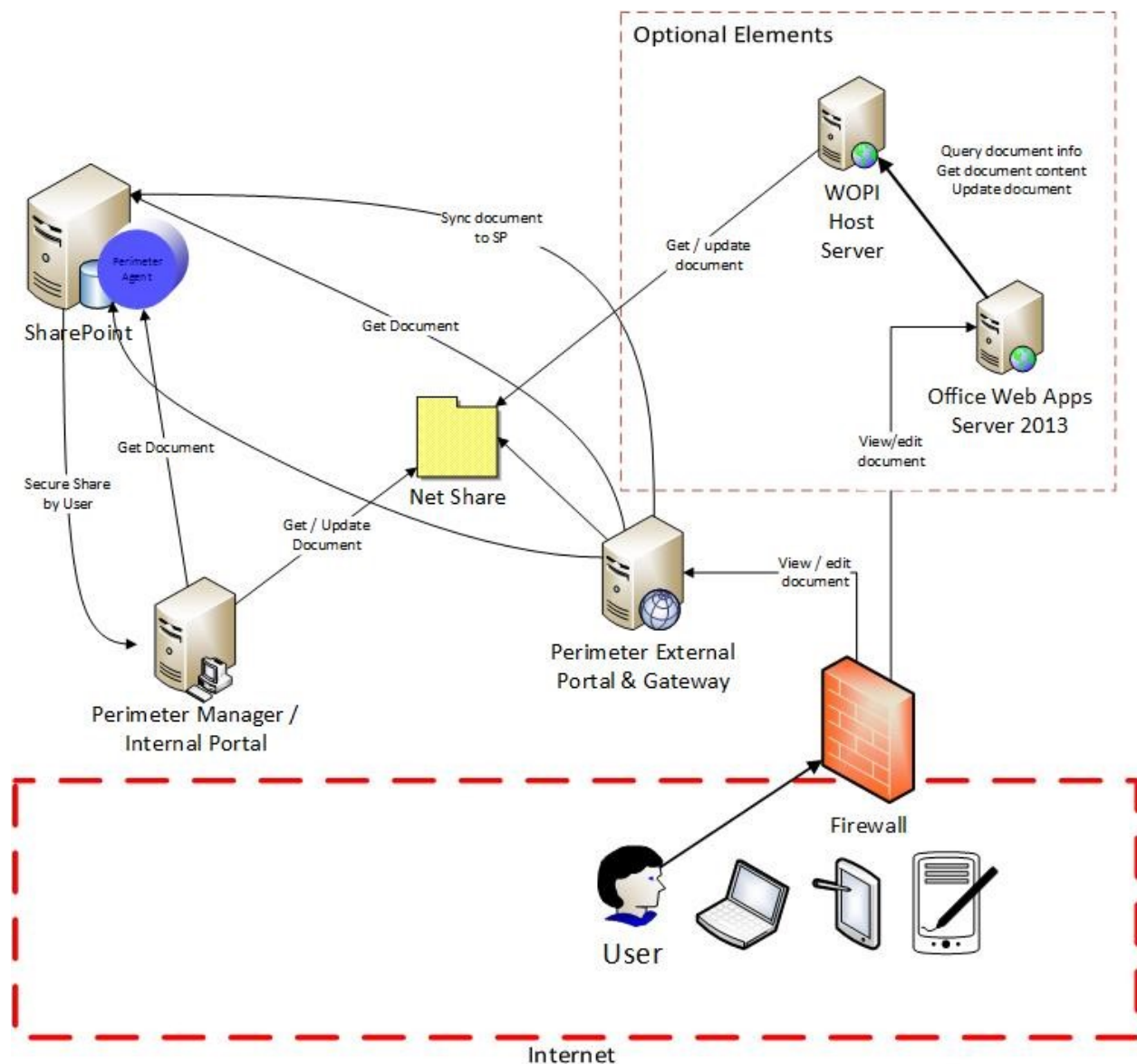


Figure 1: Architectural diagram for Perimeter Secured Share feature.

Ports Used by Perimeter for Installation

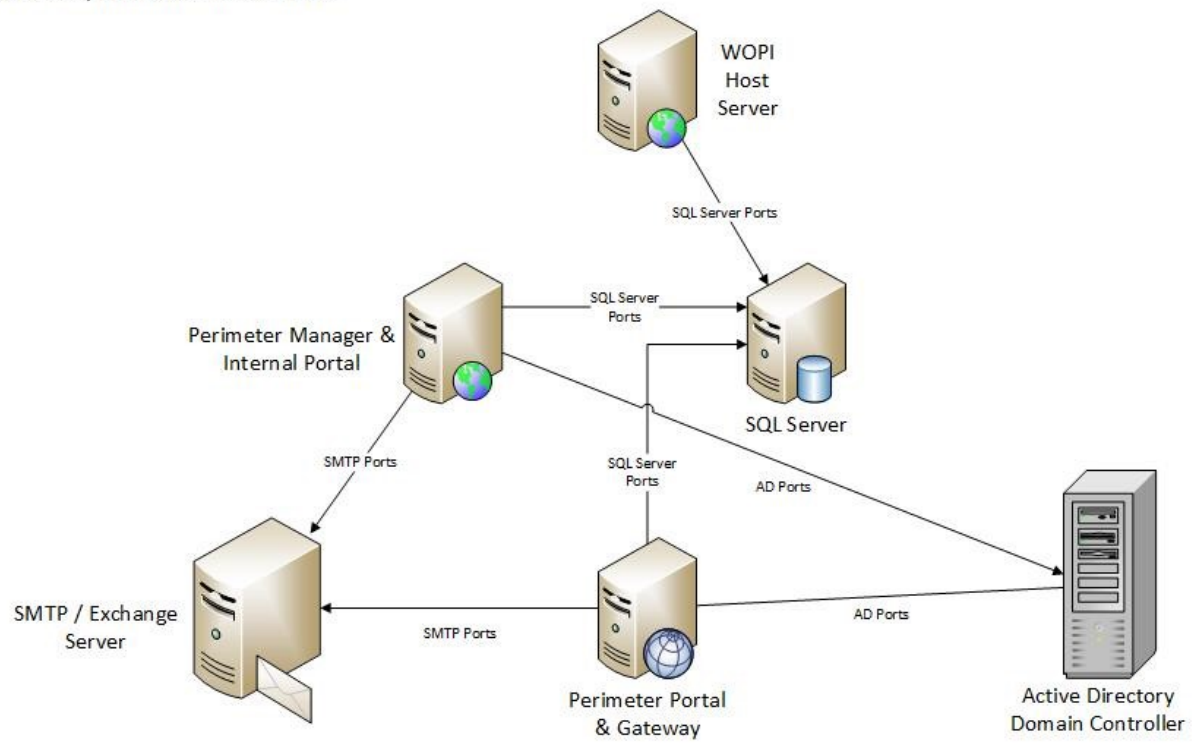
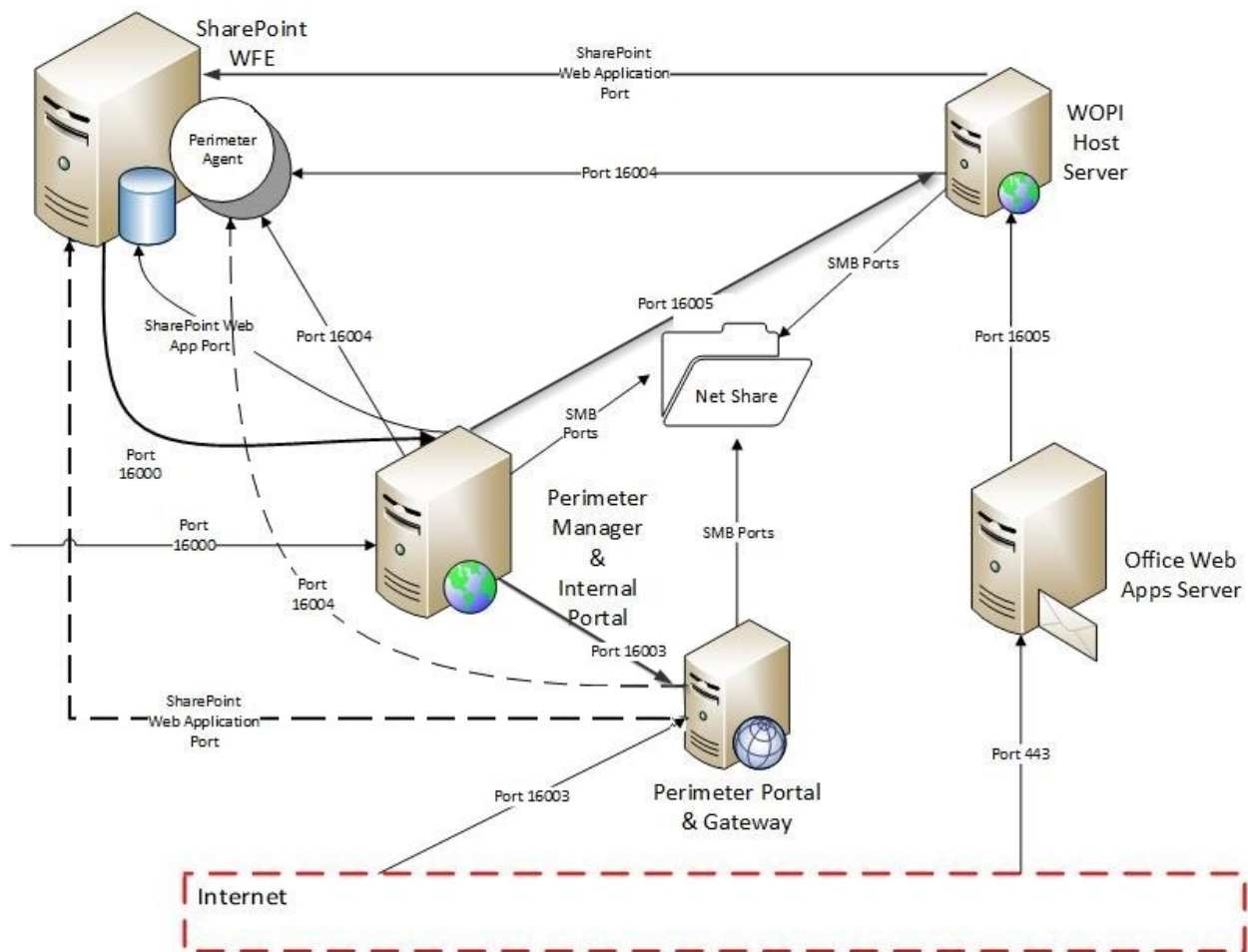


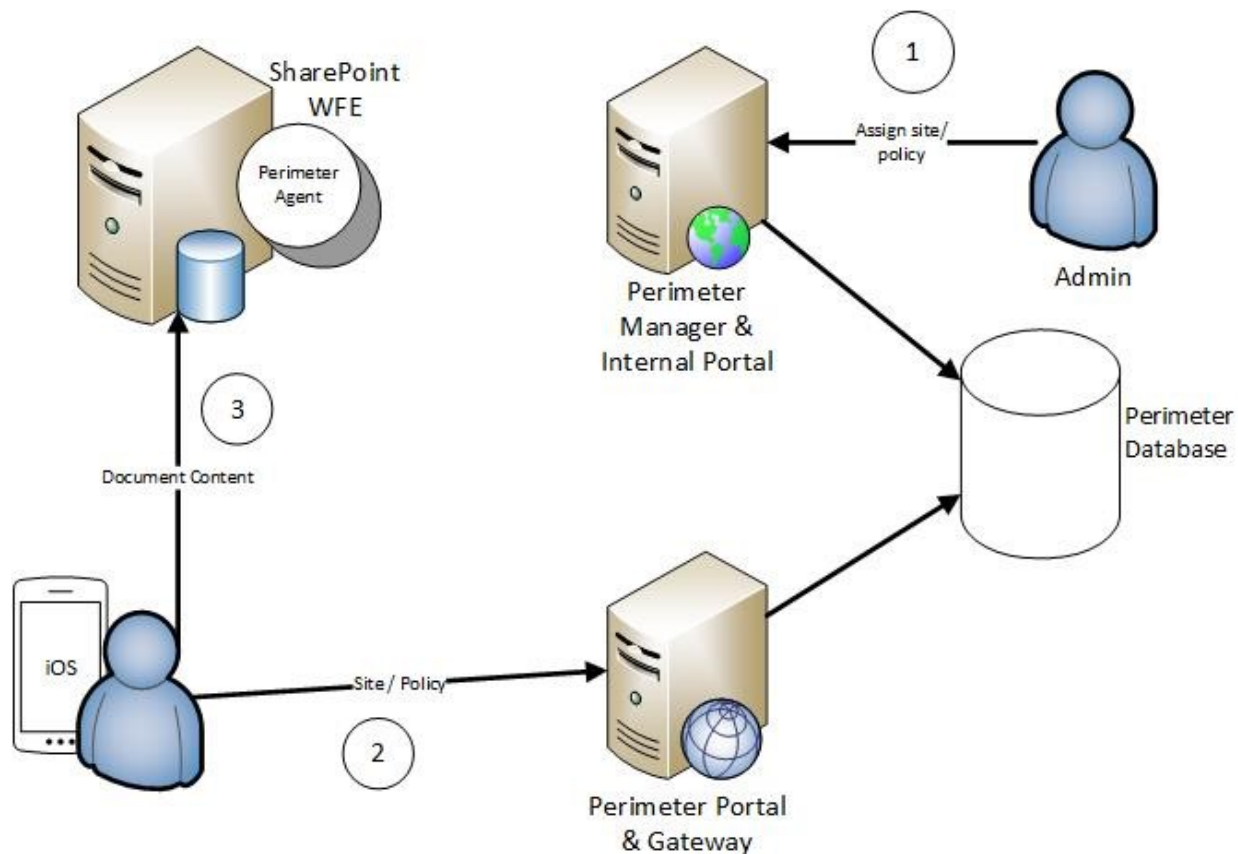
Figure 2: Ports used by Perimeter for installation alongside Active Directory and Exchange.



Ports Used For Perimeter Installation

Figure 3: Ports used for Perimeter to and from the Internet.

***Note:** The ports used by Perimeter must be unblocked by your firewall after all of the Perimeter components have been installed. For details, refer to [Setting Up Your Firewall to Unblock Specific Ports](#). If you do not want to allow the SharePoint Web front-end server to receive requests from the Perimeter External Portal & Gateway, you can block their communication and use the Perimeter Manager & Internal Portal to communicate with the SharePoint server. To isolate the SharePoint Web front-end server from Perimeter External Portal & Gateway, refer to [Isolating SharePoint Web Front-End Server from Perimeter External Portal and Gateway Server](#).



- 1) Admin assigns site & policy to users in the Perimeter Manager
- 2) End-user enrolls his/her iOS device.
Site & policy is applied to device through communication with Perimeter Portal & Gateway.
- 3) End-user is able to access SharePoint directly through his/her iOS device.

Figure 4: Mobile device interaction framework.

AvePoint Perimeter Manager

The AvePoint Perimeter Manager consists of the AvePoint Perimeter Manager Service and two components: the Management Console and the Internal Portal.

- Using the Management Console, Perimeter Administrators manage all of the settings and operations across the Perimeter management system. Perimeter Administrators also manage all of the files shared through the AvePoint Perimeter Secured Share feature and share files with groups of users based on predefined criteria.

- Using the Internal Portal, the internal users of your organization manage the SharePoint files, folders, and libraries they share via the AvePoint Perimeter Secured Share feature. Site collection administrators can view and manage all of the shared files, folders, and libraries within their site collections.

All of the Perimeter Agents can communicate with the Manager through the Manager Service, therefore the server where you install the Manager must be accessible by the all of the Agent servers. Refer to [AvePoint Perimeter Manager Server Requirements](#) for system requirements of the Manager.

AvePoint Perimeter Agent

The AvePoint Perimeter Agent runs the AvePoint Perimeter Agent Service. An AvePoint Perimeter Agent communicates with SharePoint/Active Directory Federation Services (ADFS) servers based on the commands it receives from the Perimeter Manager Service. Refer to [AvePoint Perimeter Agent Server Installation Requirements](#) for the system requirements for the Agent.

AvePoint Perimeter Gateway

The AvePoint Perimeter mobile app communicates with the AvePoint Perimeter Manager via the Gateway. To enable communication between the mobile app and the Perimeter Manager, the IIS website containing the Gateway needs to be published to the Internet to allow for mobile device access. Refer to [AvePoint Perimeter External Portal and Gateway Server Requirements](#) for system requirements for the Gateway. For details on the configuration methods for installing and publishing the Gateway, refer to [Installation and Publishing Scenarios for the External Portal and Gateway](#).

AvePoint Perimeter External Portal

Using the **AvePoint Perimeter Secured Share** feature, internal users of your organization can share SharePoint files, folders, and libraries with internal users within the organization or external users outside of the organization. Also, administrators can share files with both internal users and external users through the Perimeter Manager. After the files are shared by internal users/administrators, the persons with whom the files are shared can perform the following operations on the shared files, folders, and libraries at the AvePoint Perimeter External Portal:

- Open shared files/folders/libraries.
- Download shared files.
- Edit shared files and synchronize the modified shared files back to the original files in SharePoint via the following methods:
 - o Edit shared files in browser via Office Web Apps, and save the changes to the files via the Apps. The changes will be saved to the shared files at the External Portal and then synchronized to the corresponding original files in SharePoint immediately.

- o Download the shared files, edit the downloaded files, and then upload the modified files to the External Portal. The uploaded files will overwrite the corresponding original files in SharePoint.
- Upload new files to the shared folders or libraries at the External Portal to synchronize these files to the original folders/libraries in SharePoint.

Note the following:

- The AvePoint Perimeter External Portal supports opening files with the file types listed in the [Supported File Types for Online Viewing on the AvePoint Perimeter Internal Portal and External Portal](#) section in the browser via the default online pdf viewer. In the online pdf viewer, the users can view the .pdf files converted from the shared files.
- With an Office Web Apps (OWA) server configured for the External Portal, AvePoint Perimeter External Portal supports opening and editing shared files of the .docx, .xlsx, and .pptx formats in the browser via Office Web Apps.

To ensure all of the users can access the AvePoint Perimeter External Portal via the Internet, the External Portal needs to be published to the Internet. Refer to [AvePoint Perimeter External Portal and Gateway Server Requirements](#) for the system requirements for the External Portal, and [Installing AvePoint Perimeter External Portal and Gateway](#) for how to install and publish the External Portal.

Integrating Perimeter External Portal with SAP Jam Group

If you are using both SAP Jam groups and AvePoint Perimeter, you can configure an OpenSocial Gadget for your SAP Jam group to integrate the AvePoint Perimeter External Portal with that SAP Jam group.

The following additional features will be available on the AvePoint Perimeter External Portal that is integrated in SAP Jam group via OpenSocial Gadget:

- The group owner with whom the SharePoint folders are shared can assign the shared folders through the AvePoint Perimeter External Portal to all of the members in the SAP Jam group.
- Group members can access the files or folders within the assigned folders on the AvePoint Perimeter External Portal and perform additional actions since they will be granted the same permission level as the group owner.

***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.

For detailed instructions on configuring the integration, refer to [Configuring the Integration of External Portal and SAP Jam Group](#).

Installation and Publishing Scenarios for the External Portal and Gateway

During the Manager installation, the External Portal and Gateway are automatically installed on the Manager server under the same IIS website. The following two installation and publishing scenarios for the External Portal and Gateway are available:

- AvePoint recommends installing the External Portal and Gateway on another server and publishing the External Portal and Gateway's IIS website to the Internet. With this configuration, the Manager's IIS website is protected from the Internet, further ensuring system security. For more information on installing the External Portal and Gateway on a separate server from the Manager, refer to [Installing AvePoint Perimeter External Portal and Gateway](#).
- To have Perimeter up and running quickly in your environment, you can use the External Portal and Gateway that were automatically installed on the Manager server under the same IIS website with the Manager after publishing the shared website to the Internet. However, AvePoint does not recommend this configuration because the Manager will also be published to the Internet, which may pose a security risk to your Perimeter management system.

For more information on publishing the External Portal and Gateway, refer to [Appendix A: Publishing the External Portal and Gateway](#).

AvePoint Perimeter WOPI Host Server

A WOPI host server is a document storage location that can connect to WOPI clients to open and edit documents in a Web browser. To enable users to open and edit shared files in a browser from the AvePoint Perimeter Internal Portal and External Portal within the AvePoint Perimeter management system, the AvePoint Perimeter WOPI Host Server is required to handle the communication between the AvePoint Perimeter Internal Portal/External Portal and Office Web Apps (WOPI clients), and store the files that are opened or edited in the browser using Office Web Apps.

The WOPI Host Server must be installed on a server that can communicate with all of the following servers:

- AvePoint Perimeter Manager server (where the AvePoint Perimeter Internal Portal resides)
- AvePoint Perimeter External and Gateway server (where the AvePoint Perimeter External Portal resides)
- Office Web Apps Server that you want to use for opening and editing shared documents in web browsers at the AvePoint Perimeter Internal and External Portal

Refer to [AvePoint Perimeter WOPI Host Server System Requirements](#) for system requirements for the WOPI Host Server. For details on installing WOPI Host Server, refer to [Installing AvePoint Perimeter WOPI Host Server](#).

AvePoint Perimeter Secured Share Solution

The **AvePointPerimeterSecureShare.wsp** solution for SharePoint farms adds the **AvePoint Perimeter Secured Share** feature into SharePoint sites. This feature allows internal users within your organization to share files within internal SharePoint sites with users within and outside your organization. The feature also allows internal users to configure permission settings on the files and set an expiration time for how long the files will be shared with other users.

AvePoint Perimeter Geolocation Database

The Geolocation Database is an optional database that stores geographic and political boundary data (location names with the corresponding coordinates) that can be used to define locations. During Perimeter installation, you can choose whether or not to install this database.

The Geolocation database enables you to define location groups based on geographic and political boundary data from the database without relying on data retrieved from external resources such as Bing Maps. For more information on configuring location groups based on geographic and political boundaries, refer to [Adding a New Geographic Location Group](#).

***Note:** The entire Geolocation database will use about 4 GB of space in the target SQL Server, and the initial loading process for this database may use up to 25 GB of space. To successfully populate the Geolocation database, ensure there is enough available disk space on the target SQL Server, and the **ExecutionPolicy** that determines which Windows PowerShell scripts can run on your computer is set to **Unrestricted** (all Windows PowerShell scripts can be run).

Installation Scenarios for the Geolocation Database

To install the Geolocation database, choose either of the following two methods:

- If you have the **db_owner** database role in a blank database that can be populated with the required data and used as a Geolocation database, use the **AvePoint Perimeter Geolocation Database Installation Wizard** to populate the desired blank database with the geography location information to define locations based on geographic and political boundaries information.
- If you have the **dbcreator** server role in a particular SQL Server to create a new database that will be used as the Geolocation database, use the **AvePoint Perimeter Geolocation Database Installation Wizard** to create the database in the specified SQL Server, and then populate it with the required geography location information that can be used to define locations based on geographic and political boundaries information.

Refer to [AvePoint Perimeter Geolocation Database Server and Installation Wizard System Requirements](#) for additional system requirements.

Permission Requirements

In order to install and use AvePoint Perimeter system components properly, certain permissions are required. The following sections provide details on the permission requirements for each component.

Permission Requirements for AvePoint Perimeter Manager

The sections below offer detailed information on the AvePoint Perimeter Manager's permission requirements.

Permission Requirements for Installing AvePoint Perimeter Manager

To install and use the AvePoint Perimeter Manager, ensure the application pool account used to create the application pool for the Manager Service's IIS website has the following permissions:

- Local System Permissions – User is a member of the local **Administrators** group of the Manager server.
- SQL Permissions – If you select **Windows Authentication** as the Database Credentials for the Manager Configuration database, you must have either the **dbcreator** server role in the SQL Server that will contain the new Manager Configuration database, or the **db_owner** database role in the existing Manager Configuration database.

***Note:** Windows Authentication for the Manager Configuration database automatically uses the application pool account configured in **Application Pool Settings** instead of the currently logged-in account.

Permission Requirements for Logging into AvePoint Perimeter Manager

To log into the AvePoint Perimeter Manager (the Management Console and the Internal Portal), ensure the account used meets the following requirements:

- If you are an administrator, log into the AvePoint Perimeter Management Console using an administrator account. For detailed information on administrator accounts, refer to [Updating AvePoint Perimeter](#) and [Configuring Admin Accounts](#).
- If you are an internal user, log into the AvePoint Perimeter Internal Portal using your Active Directory credentials.

Permission Requirements for AvePoint Perimeter Agent

To install AvePoint Perimeter Agent, ensure the Agent account has the following permissions:

- Local System Permission – User is a member of the local **Administrators** group, or user must have the following permissions or roles in the local system:
 - o Log on as batch job in group policy.

- o Group member of WSS_WPG, IIS_IUSRS.
- o Full control permission for Perimeter Certificate on Agent server
- o Full control permission for Agent installation folder.
- SharePoint Permission – User must be a member of the **Farm Administrators** group and have **Full Read** permission to the User Policy of the Web applications.
- SQL Permissions –
 - o For SharePoint 2010 farm, user must have:
 - **db_owner** database role in Configuration Database, Central Admin Database, and all of the content databases under the Web applications to use the Secure Share feature.
 - o For SharePoint 2013 or SharePoint 2016 farm, user must have:

***Note:** The following are the minimum permissions of using Perimeter 1.7 or later in the SharePoint 2013 or SharePoint 2016 environment. For the earlier versions of Perimeter, the permission requirements are the same as required for SharePoint 2010 farm.

 - **SharePoint_Shell_Access** database role in Configuration Database, Central Admin Database, and all of the content databases under the Web applications that are required to use the Secure Share feature.
 - **SharePoint_Shell_Access** database role of FBA provider database, if SharePoint Web application enabled Form-Based Authentication.

***Note:** The **SharePoint_Shell_Access** role can only be assigned via SharePoint Management Shell. For instructions on how to assign this role to a user, refer to the following Microsoft technical article:
<https://technet.microsoft.com/en-us/library/ff607596.aspx>.

Permission Requirements for AvePoint Perimeter External Portal and Gateway

To install AvePoint Perimeter External Portal and Gateway on a server, ensure the application pool account used to create the application pool for the External Portal and Gateway's IIS website has the following permissions:

- Local System Permissions – User is a member of the local **Administrators** group of the External Portal and Gateway server.
- SQL Permissions – If you select **Windows Authentication** as the Database Credentials for the Manager Configuration database that the External Portal and Gateway will connect to, you must have the **db_owner** database role in the designated Manager Configuration database.

***Note:** Windows Authentication for the Manager Configuration database automatically uses the application pool account configured in **Application Pool Settings** instead of the currently logged-in account.

Permission Requirements for Logging into AvePoint Perimeter External Portal

After internal users/administrators share files, folders, or libraries, those with whom the files, folders, or libraries are shared can view the shared files, folders, or libraries in the AvePoint Perimeter External Portal. To log into the AvePoint Perimeter External Portal, ensure the account used meets the following requirements:

- If the files, folders, or libraries are shared with an internal user, the internal user logs into the AvePoint Perimeter External Portal directly using the Active Directory credentials or e-mail address logins.
- If the files, folders, or libraries are shared with an external user, the external user must register to the AvePoint Perimeter External Portal and then log into the portal with the registered user account.

Permission Requirements for Geolocation Database

To install the Geolocation database, ensure the user running the Geolocation Database Installation Wizard must have the following permissions:

- Local System Permissions – User is a member of the local **Administrators** group of the machine that runs the installation wizard.
- SQL Permissions – If you select **Windows Authentication** as the Database Credentials for the Geolocation database, you must have either the **dbcreator** server role in the SQL Server that will contain the new Geolocation database, or the **db_owner** database role in the existing blank Geolocation database.

Permission Requirements for AvePoint WOPI Host Server

To install AvePoint Perimeter WOPI Host Server on a server, ensure the application pool account used to create the application pool for the WOPI Host Server's IIS website has the following permissions:

- Local System Permissions – User is a member of the local **Administrators** group of the WOPI Host Server host.
- SQL Permissions – If you select **Windows Authentication** as the Database Credentials for the Manager Configuration database that the WOPI Host Server will connect to, you must have the **db_owner** database role in the designated Manager Configuration database.

***Note:** Windows Authentication for the Manager Configuration database automatically uses the application pool account configured in **Application Pool Settings** instead of the currently logged-in account.

System Requirements

Refer to the sections below for system requirements that must be in place prior to installing AvePoint Perimeter.

Supported Environments

AvePoint Perimeter is compatible with the following platforms:

- Microsoft SharePoint Server/Foundation 2010 (up to and including Service Pack 2)
- Microsoft SharePoint Server/Foundation 2013 (up to and including Service Pack 1)
- Microsoft SharePoint Server 2016
- Active Directory Federation Services (ADFS) 2.0

AvePoint Perimeter Manager Server Requirements

Before installing AvePoint Perimeter Manager, make sure the Manager server meets the following requirements:

***Note:** To ensure the AvePoint Perimeter Manager server can properly send real-time push notifications to iOS devices via the Apple Push Notification Service (APNS), and to Android devices via Google Cloud Messaging (GCM), you must configure the firewall of your Manager server to allow APNS/GCM traffic to get past your firewall after the Manager installation completes. For details, refer to [Configuring Your Firewall to Allow Push Notifications](#).

Component	Requirements
Operating System Edition	Recommended: Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 Minimum: Windows Server 2008*
Available Physical Memory	Recommended: 1 GB or greater Minimum: 512 MB
Available Disk Space	Recommended: 1 GB or greater Minimum: 1 GB
.NET Framework Version	.NET Framework 3.5 SP1 For Windows Server 2012 and Windows 8, or later operating system editions, .NET Framework 4.5 must be installed in addition to .NET Framework 3.5 SP1.
.NET Framework Features	HTTP Activation and Non-HTTP Activation should be installed. For Window Server 2012 and Windows 8, or later operating system editions, the features including HTTP Activation, Message Queuing (MSMQ)

Component	Requirements
	Activation, Named Pipe Activation, TCP Activation, and TCP Port Sharing for .NET Framework 4.5 should be installed.
Windows Process Activation Service	Windows Process Activation Service should be started, and Process Model, .NET Environment, and Configuration APIs should be installed.
Net.TCP Port Sharing Service	Net.TCP Port Sharing Service should be started.
Web Server (IIS) Role	<p>For Windows Server 2008, the following Windows features should be installed:</p> <ul style="list-style-type: none"> • Web Server • Common HTTP Features (Static Content, Default Document) • Application Development (ASP.NET, .NET Extensibility, ISAPI Extensions and ISAPI Filters) • Management Tools (IIS Management Console, IIS 6 Management Compatibility and IIS 6 Metabase Compatibility) <p>For Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2, the following Windows features should be installed:</p> <ul style="list-style-type: none"> • Web Server • Common HTTP Features (Static Content, Default Document) • Application Development (ASP.NET 3.5, .NET Extensibility 3.5, ISAPI Extensions, ISAPI Filters) • Management Tools (IIS Management Console, IIS 6 Management Compatibility, IIS 6 Metabase Compatibility)
PowerShell Version	PowerShell 2.0 or above

*AvePoint Perimeter supports Windows Server 2008, but Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 are recommended. Running the latest versions of Windows servers ensures the most current patches and security updates from Microsoft.

Configuring Your Firewall to Allow Push Notifications

AvePoint Perimeter Manager sends real-time push notifications to iOS devices via the Apple Push Notification Service (APNS), and to Android devices via Google Cloud Messaging (GCM). After the Manager installation completes, you need to configure the firewall of your Manager server to allow APNS/GCM traffic to get past your firewall.

To ensure that APNS traffic can get past your firewall, open the following ports on your firewall:

- TCP port 5223 (used by iOS devices to communicate with APNS servers)
- TCP port 2195 (used by AvePoint Perimeter Manager to send notifications to APNS)

To ensure Android devices inside your network can receive push notifications, configure your firewall to allow Android devices' connectivity with GCM.

- The ports to open are: TCP ports 5228, 5229, and 5230. GCM typically only uses 5228, but it sometimes uses 5229 and 5230.
- GCM doesn't provide specific IP addresses, so you should allow your firewall to accept outgoing connections to all of the IP addresses contained in the IP blocks listed in Google's ASN of 15169.

AvePoint Perimeter External Portal and Gateway Server Requirements

Before installing AvePoint Perimeter External Portal and Gateway, make sure the External Portal and Gateway server meets the following requirements:

Component	Requirements
Operating System Edition	Recommended: Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 Minimum: Windows Server 2008*
Available Physical Memory	Recommended: 1 GB or greater Minimum: 512 MB
Available Disk Space	Recommended: 1 GB or greater Minimum: 1 GB
.NET Framework Version	.NET Framework 3.5 SP1 For Windows Server 2012 and Windows 8, or later operating system editions, .NET Framework 4.5 must be installed in addition to .NET Framework 3.5 SP1.
.NET Framework Features	HTTP Activation and Non-HTTP Activation should be installed. For Window Server 2012 and Windows 8, or later operating system editions, the features including HTTP Activation, Message Queuing (MSMQ) Activation, Named Pipe Activation, TCP Activation, and TCP Port Sharing for .NET Framework 4.5 should be installed.
Windows Process Activation Service	Windows Process Activation Service should be started, and Process Model, .NET Environment, and Configuration APIs should be installed.
Net.TCP Port Sharing Service	Net.TCP Port Sharing Service should be started.
Web Server (IIS) Role	For Windows Server 2008, the following Windows features should be installed: Web Server Common HTTP Features (Static Content, Default Document) Application Development (ASP.NET, .NET Extensibility, ISAPI Extensions and ISAPI Filters) Management Tools (IIS Management Console, IIS 6 Management Compatibility and IIS 6 Metabase Compatibility) For Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2, the following Windows features should be installed: Web Server Common HTTP Features (Static Content, Default Document) Application Development (ASP.NET 3.5, .NET Extensibility3.5, ISAPI Extensions, ISAPI Filters) Management Tools (IIS Management Console, IIS 6 Management Compatibility, IIS 6 Metabase Compatibility)
PowerShell Version	PowerShell 2.0 or above

*AvePoint Perimeter supports Windows Server 2008, but Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 are recommended. Running the latest versions of Windows servers ensures you have the most current patches and security updates from Microsoft.

AvePoint Perimeter Geolocation Database Server and Installation Wizard System Requirements

To install a Geolocation database in SQL Server, you must ensure that the SQL Server meets the [SQL Server Requirements for AvePoint Perimeter Databases](#) and that it has at least 25 GB of available disk space. The entire Geolocation database is about 4 GB, but the Geolocation database's initial loading process may use up to 25 GB of space. In addition, you must ensure that the **ExecutionPolicy** that determines which Windows PowerShell scripts can run on your computer is set to **Unrestricted**, which indicates that all Windows PowerShell scripts can be run.

Before installing the Geolocation database, ensure that the server where you run the **AvePoint Perimeter Geolocation Database Installation Wizard** meets the following requirements:

Component	Requirements
Operating System Edition	Recommended: Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 Minimum: Windows Server 2008*
Available Physical Memory	Recommended: 1 GB or greater Minimum: 512 MB
Available Disk Space	Recommended: 1 GB or greater Minimum: 1 GB
.NET Framework Version	.NET Framework 3.5 SP1 For Windows Server 2012 and Windows 8, or later operating system editions, .NET Framework 4.5 must be installed in addition to .NET Framework 3.5 SP1.
PowerShell Version	PowerShell 2.0 or above

*AvePoint Perimeter supports Windows Server 2008, but Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 are recommended. Running the latest versions of Windows servers ensures the most current patches and security updates from Microsoft.

SQL Server Requirements for AvePoint Perimeter Databases

Refer to the table below for the SQL Server requirements for AvePoint Perimeter databases.

Databases	SQL Server Editions
Manager Configuration Database and Geolocation Database	<ul style="list-style-type: none">• Microsoft SQL Server 2016• Microsoft SQL Server 2014 SP1• Microsoft SQL Server 2014• Microsoft SQL Server 2012 Service Pack 1

Databases	SQL Server Editions
	<ul style="list-style-type: none">• Microsoft SQL Server 2012• Microsoft SQL Server 2008 R2 Service Pack 1

AvePoint Perimeter WOPI Host Server System Requirements

Refer to the table below for the Perimeter WOPI Host Server system requirements:

Component	Requirements
Operating System Edition	Recommended: Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 Minimum: Windows Server 2008*
Available Physical Memory	Recommended: 1 GB or greater Minimum: 512 MB
Available Disk Space	Recommended: 1 GB or greater Minimum: 1 GB
.NET Framework Version	.NET Framework 3.5 SP1 For Windows Server 2012 and Windows 8, or later operating system editions, .NET Framework 4.5 must be installed in addition to .NET Framework 3.5 SP1.
.NET Framework Features	HTTP Activation and Non-HTTP Activation should be installed. For Window Server 2012 and Windows 8, or later operating system editions, the features including HTTP Activation, Message Queuing (MSMQ) Activation, Named Pipe Activation, TCP Activation, and TCP Port Sharing for .NET Framework 4.5 should be installed.
Windows Process Activation Service	Windows Process Activation Service should be started, and Process Model, .NET Environment, and Configuration APIs should be installed.
Net.TCP Port Sharing Service	Net.TCP Port Sharing Service should be started.
Web Server (IIS) Role	For Windows Server 2008, the following Windows features should be installed: Web Server Common HTTP Features (Static Content, Default Document) Application Development (ASP.NET, .NET Extensibility, ISAPI Extensions and ISAPI Filters) Management Tools (IIS Management Console, IIS 6 Management Compatibility and IIS 6 Metabase Compatibility) For Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2, the following Windows features should be installed: Web Server Common HTTP Features (Static Content, Default Document) Application Development (ASP.NET 3.5, .NET Extensibility3.5, ISAPI Extensions, ISAPI Filters) Management Tools (IIS Management Console, IIS 6 Management Compatibility, IIS 6 Metabase Compatibility)
PowerShell Version	PowerShell 2.0 or above

*AvePoint Perimeter supports Windows Server 2008, but Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 are recommended. Running the latest versions of Windows servers ensures you have the most current patches and security updates from Microsoft.

AvePoint Perimeter Agent Server Installation Requirements

Before installing AvePoint Perimeter Agent, make sure the Agent is installed on the correct server and that the server meets the requirements detailed in the table below.

Where to Install AvePoint Perimeter Agents

AvePoint Perimeter Agents can be installed on different machines according to the features you wish to use:

- To use the **SharePoint Policy** feature, an AvePoint Perimeter Agent must be installed on each SharePoint Web front-end server in the SharePoint environment.
- To use the **Federation Policy** feature, an AvePoint Perimeter Agent must be installed on the ADFS server or the ADFS proxy server.
- To use the **Secured Share** features (including the **AvePoint Perimeter Secured Share** site feature in SharePoint sites and the **Virtual Views** feature in AvePoint Perimeter Manager), an AvePoint Perimeter Agent must be installed on each SharePoint Web front-end server of the SharePoint environment.
- To use the **Burglar Alarm Rules** feature, an AvePoint Perimeter Agent must be installed on each Web front-end server in the SharePoint environment.

AvePoint Perimeter Agent Server Requirements

Before installing AvePoint Perimeter Agent, make sure the Agent server meets the following requirements:

Component	Requirements
Operating System Edition	Recommended: Windows Server 2012 and Windows Server 2012 R2 Minimum: Windows Server 2008 R2*
Available Physical Memory	Recommended: 512 MB or greater Minimum: 256 MB
Available Disk Space	Minimum: 1 GB
.NET Framework Version	.NET Framework 3.5 SP1 For Windows Server 2012 and Windows 8, or later operating system editions, .NET Framework 4.5 must be installed in addition to .NET Framework 3.5 SP1.
.NET Framework Features	HTTP Activation and Non-HTTP Activation should be installed. For Window Server 2012 and Windows 8, or later operating system editions, the features including HTTP Activation, Message Queuing (MSMQ) Activation, Named Pipe Activation, TCP Activation, and TCP Port Sharing for .NET Framework 4.5 should be installed.
Windows Process Activation Service	Windows Process Activation Service should be started, and Process Model, .NET Environment, and Configuration APIs should be installed.
Net.TCP Port Sharing Service	Net.TCP Port Sharing Service should be started.

*AvePoint Perimeter supports Windows Server 2008 R2, but Windows Server 2012 and Windows Server 2012 R2 are recommended. Running the latest versions of Windows servers ensures the most current patches and security updates from Microsoft.

End-User Devices Supported by AvePoint Perimeter

AvePoint Perimeter is supported for use on iOS 8 or later on the iPhone, iPod Touch, and iPad, mobile devices with Android operating system 4.0 or later, or Windows Phone 8.0.

Supported Browsers

The sections below detail the supported browser versions for AvePoint Perimeter Manager, AvePoint Perimeter Internal Portal, and AvePoint Perimeter External Portal.

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

Supported Browsers for AvePoint Perimeter Manager

See below for AvePoint Perimeter Manager browser support:

Browser	Version
Internet Explorer	IE 9 or later
Google Chrome	49.0.2623.112 m or later

Supported Browsers for AvePoint Perimeter Internal Portal and AvePoint Perimeter External Portal

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

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 the 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.

AvePoint Perimeter Installation Overview

The steps for installing AvePoint Perimeter depend upon your type of installation: users trialing AvePoint Perimeter will take slightly different steps to install than those who have purchased the product.

Purchased Versions of Perimeter

Customers who want to perform a complete installation according to AvePoint's recommended methods should follow the steps below, in order:

1. [Installing AvePoint Perimeter Manager](#)

***Note:** For additional network security, AvePoint recommends installing the External Portal and Gateway on a server different from the Perimeter Manager.

2. [Installing AvePoint Perimeter External Portal and Gateway](#)
3. [Publishing the External Portal and Gateway via Reverse Proxy](#)
4. [Verifying the External and Gateway Server Certificate](#)

***Note:** AvePoint recommends that the server certificate on the External Portal and Gateway or reverse proxy (if the External Portal and Gateway is published via reverse proxy) be a valid certificate obtained from a commercial certificate authority.

5. [Installing Geolocation Database](#)
6. [Installing AvePoint Perimeter WOPI Host Server](#)
7. [Installing AvePoint Perimeter Agents](#)

Trial Versions of Perimeter

Users who want to quickly get Perimeter up and running in their environment (such as those who are trialing AvePoint Perimeter) should follow the steps below, in order. Note that these steps will get you up and running quickly, but are not the most secure or AvePoint-recommended methods of installation.

1. [Installing AvePoint Perimeter Manager](#)

***Note:** For quick installation, install the External Portal and Gateway onto the Perimeter Manager server.

2. [Publishing the External Portal and Gateway Directly](#)
3. [Verifying the External and Gateway Server Certificate](#)

***Note:** For quick installation, use a self-signed certificate.

4. [Installing AvePoint Perimeter WOPI Host Server](#)
5. [Installing AvePoint Perimeter Agents](#)

The AvePoint Perimeter Installation Wizards guide you through the installation process. To complete the installation successfully, a local administrator must run the Installation Wizard.

Installing AvePoint Perimeter Manager

Before installing AvePoint Perimeter Manager, ensure that the [AvePoint Perimeter Manager Server Requirements](#) are met and that the user running the installation wizard is a member of the local **Administrators** group of the current server.

The AvePoint Perimeter Manager must be installed in the same Active Directory domain as your SharePoint farms where you want to deploy the AvePoint Perimeter management system.

***Note:** After the Manager Installation completes, the **AvePoint Perimeter Manager Installation Wizard** installs not only the Manager (including Management Console and Internal Portal) but also the External Portal and Gateway on the Manager server under the same IIS website. The External Portal and Gateway must be published to the Internet through either of these two methods: you can publish this shared IIS website to the Internet (not recommended), or you can install the External Portal and Gateway on a separate server and publish the External Portal and Gateway's IIS website to the Internet (recommended). For details on the configuration methods for installing and publishing the External Portal and Gateway, refer to [Installation and Publishing Scenarios for the External Portal and Gateway](#).

To install AvePoint Perimeter Manager, complete the following steps:

1. Download the Manager ZIP file by requesting a demo version or by contacting an AvePoint representative for links to this package.
2. Extract the package. Open the extracted AvePoint Perimeter Manager directory and double-click the **Setup.exe** file.
3. After the Welcome screen appears, click **Install Manager**.
4. Carefully review the **License Agreement**. After you have read the agreement, select the **I accept the terms in the license agreement** checkbox, and click **Next**.
5. Click **Browse** and select the location for the Manager installation. The default installation location is *C:\Program Files\AvePoint*. Click **Next**.
6. Perimeter performs a brief pre-scan of the environment to ensure that your system meets the AvePoint Perimeter Manager system requirements. The status for each rule is listed in the **Status** column.
7. Click the status hyperlink to view detailed information on the scan results, or click **Details** to view detailed information on all of the requirements.

***Note:** You cannot proceed with the installation if any of the rules have a **Status** of **Failed**.

- If any of the rules have a **Failed** status, your system does not meet the minimum requirement of the corresponding rule. You must update your environment to meet the

AvePoint Perimeter Manager system requirements, and then click the **Rescan** button to check your environment again.

- If any of the rules have a **Warning** status, your system meets the minimum requirement of the corresponding rule but does not meet the recommended condition. In this case, you can still click **Next** to configure the **Manager Service Configuration**.
- If all of the rules are **Passed**, your system meets all of the recommended conditions in the AvePoint Perimeter Manager system requirements. Click **Next** to configure the **Manager Service Configuration**.

8. Set up the **Manager Service Configuration**:

- a. **Manager Service Host** – Enter the current machine’s hostname, IP address, or fully qualified domain name (FQDN).

***Note:** Ensure that the Manager Service host can communicate with all of the Agent machines through the entered hostname, IP address, or FQDN.

- b. **IIS Website Settings** – Configure the IIS website settings for the Manager Service. Create a new IIS website that will be used to access Perimeter Manager.

- **Create a new IIS Website** – Enter the website name and create a new IIS website for the Manager Service. Do not change the default website port (16000) used to access Perimeter Manager Service unless a port conflict exists.
- **Website Port** – Manager Service communication port. The default port is 16000.

***Note:** If you change the port after the installation completes, go to the ... \AvePoint\Perimeter\Manager\bin\config directory on the server where Perimeter Manager is installed, find the **AppSettings.Config** file, make the same change to the value of the **ControlPort** attribute in the **AppSettings.config** file, and then restart the IIS website. Otherwise, Perimeter features cannot work well.

- c. **Application Pool Settings** – Create a new IIS application pool for the Manager Service’s website. The application pool is used to handle requests that are sent to the Manager Service’s website.

- **Create a new application pool** – Enter the application pool name and application pool account settings to create a new IIS application pool for the Manager Service’s website.

- d. Click **Next** to configure the database settings for the Manager Service.

9. AvePoint Perimeter Manager supports **MS SQL** databases only, so only **MS SQL** is available as the **Database Type**. Configure the following settings for the Manager Configuration Database:

- a. **Database Server** – The MS SQL Server name.

***Note:** Ensure that SQL Server meets the [SQL Server Requirements for AvePoint Perimeter Databases](#).

- b. **Database Name** – Enter a database name for the Manager Service. If the database does not exist, it will be created in the MS SQL Database Server entered above.
 - c. **Database Credentials** – Select the credentials for this Manager Configuration database.
 - o **Windows Authentication** (the default option) – Use this method if you want the user’s identity to be confirmed by Windows. By default, this account is the application pool account configured in the previous step instead of the currently logged-in account and cannot be changed. As such, this account must have either the **dbcreator** server role in the SQL Server that will contain the new Manager Configuration database or the **db_owner** database role in the existing Manager Configuration database.
 - o **SQL Authentication** – SQL Server will confirm the user’s identity according to the user’s account and password. The account must have the following permissions: **db_owner** database role in the existing Manager Configuration database or **dbcreator** server role in the SQL Server that will contain the Manager Configuration database.
- *Note:** If you want to change the database credentials after the installation, refer to [Updating Database Credentials](#).
- 10. Click **Next** to proceed with the installation, or click **Back** to change any of the previous settings. Click **Cancel** to abandon all configurations and exit the installation wizard.
 - 11. The installation process displays via the progress bar in the **Installation Process** page.
 - 12. Once the Manager installation completes, a pop-up window appears to ask whether to continue to install the Geolocation database immediately.
 - To install the Geolocation database immediately, click **Yes** to access the **Geolocation Database Settings** page to start to install the Geolocation database. For details on installing the Geolocation database, refer to [Installing Geolocation Database](#).
 - To finish the Manager Installation without installing the Geolocation database, click **No** to access the **Complete** page.
 - 13. In the **Complete** page, click **Finish** to exit the installation wizard.

Installing AvePoint Perimeter Agents

Before installing AvePoint Perimeter Agents:

- See [Where to Install AvePoint Perimeter Agents](#).
- Ensure that the [AvePoint Perimeter Agent Server Requirements](#) are met.
- Ensure that the user running the installation wizard is a member of the local **Administrators** group on the current server.
- Verify that the AvePoint Perimeter Manager Service is running.

To install AvePoint Perimeter Agents, complete the following steps:

1. Download the Agent ZIP file by requesting a demo version or by contacting an AvePoint representative for links to this package.
2. Extracted this package.
3. Navigate to the AvePoint Perimeter Agent directory, and double-click the **Setup.exe** file. The Welcome screen appears.
4. Click **Install Agent**.
5. Carefully review the **License Agreement**.
6. After you have read the agreement, check the **I accept the terms in the license agreement** checkbox, and click **Next**.
7. Click **Browse**.
8. Select the location for the Agent installation. The default installation location is *C:\Program Files\AvePoint*. Click **Next**.
9. Perimeter will perform a brief pre-scan of the environment to ensure that all rules meet the AvePoint Perimeter Agent system requirements. The status for each rule will be listed in the **Status** column. Click the status hyperlink to view detailed information on the scan results, or click **Details** to view detailed information on all of the requirements.

***Note:** You cannot proceed with the installation if the **Status** of any of the rules is **Failed**.

- If the status of any rule is **Failed**, your system does not meet the minimum requirement of the corresponding rule. You must update your environment to meet the AvePoint Perimeter Agent system requirements, and then click the **Rescan** button to check your environment again.
 - If the status of any rule is **Warning**, your system meets the minimum requirement of the corresponding rule but does not meet the recommended condition. In this case, you can still click **Next** to configure the **Communication Configuration**.
 - If all of the rule statuses are **Passed**, your system meets all of the recommended conditions in the AvePoint Perimeter Agent system requirements. Click **Next** to configure the **Communication Configuration**.
10. After verifying that the requirements above are met, set up the **Communication Configuration**:
 - a. **Perimeter Agent Host** – Enter the current server’s hostname, IP address, or fully qualified domain name (FQDN).
 - b. **Perimeter Agent Port** – The port entered here is used by the Manager or other Agents for communication. The default port number is 16004.
 - c. **Manager Service Host** – The hostname or IP address of the machine that has the Manager Service installed on it.

- d. **Manager Service Port** – The port used for communication with Manager Service. This port should match the information you entered during the Manager configuration. The default port number is 16000.
 - e. **Agent Account** – Enter the Agent account under which the Agent activities are performed. Ensure that the **AvePoint Perimeter Agent** Account has the permissions explained in the [Permission Requirements for AvePoint Perimeter Agent](#) section of this guide.
11. Click **Next** to begin the installation, click **Back** to change any of the previous settings, or click **Cancel** to abandon all configurations and exit the installation wizard.
 12. After the installation completes, click **Finish** to exit the installation wizard.

Modifying Perimeter Agent Configurations

To modify the configuration of an already-installed Perimeter Agent, use the **AvePoint Perimeter Agent Configuration Tool** by completing the following steps:

1. Navigate to the server where the Agent you want to configure is installed.
1. Navigate to **Start > All Programs > AvePoint Perimeter**.
2. Open the **Agent** folder and click **AvePoint Perimeter Agent Configuration Tool** to access this tool.
3. Modify the desired **Agent Communication** settings in this tool. For more information on configuring the settings, refer to [Installing AvePoint Perimeter Agents](#).
4. When you finish the configurations, click **OK** to save the modifications and exit this tool.

Installing AvePoint Perimeter External Portal and Gateway

To install the AvePoint Perimeter External Portal and Gateway on a server, ensure that [AvePoint Perimeter External Portal and Gateway Server Requirements](#) are met and the user running the installation wizard is a member of the local **Administrators** group of the current server.

To install the AvePoint Perimeter External Portal and Gateway, complete the following steps:

1. Download the Manager ZIP file by requesting a demo version or by contacting an AvePoint representative for links to this package.
2. Extract the package.
3. In the extracted AvePoint Perimeter Manager directory, double-click the **Setup.exe** file. The Welcome screen appears.
4. Click **Install External Portal and Gateway**.
5. Carefully review the **License Agreement**.

6. After you have read the agreement, select the **I accept the terms in the license agreement** checkbox, and click **Next**.
7. Click **Browse**.
8. Select the location for the External Portal and Gateway installation. The default installation location is *C:\Program Files\AvePoint*. Click **Next**.
9. Perimeter performs a brief pre-scan of the environment to ensure that your system meets the AvePoint Perimeter External Portal and Gateway system requirements. The status for each rule is listed in the **Status** column. Click the status hyperlink to view detailed information on the scan results, or click **Details** to view detailed information on all of the requirements.

***Note:** You cannot proceed with the installation if the **Status** of any of the rules is **Failed**.

- If the status of any rule is **Failed**, your system does not meet the minimum requirement of the corresponding rule. You must update your environment to meet the AvePoint Perimeter External Portal and Gateway system requirements, and then click the **Rescan** button to check your environment again.
- If the status of any rule is **Warning**, your system meets the minimum requirement of the corresponding rule but does not meet the recommended condition. In this case, you can still click **Next** to configure the **Portal and Gateway Configuration**.
- If all of the rule statuses are **Passed**, your system meets all of the recommended conditions in the AvePoint Perimeter External Portal and Gateway system requirements. Click **Next** to configure the **Portal and Gateway Configuration**.

10. Set up the **Portal and Gateway Configuration**:

- a. **Portal and Gateway Host** – Enter the current machine’s hostname, IP address, or fully qualified domain name (FQDN).

***Note:** Ensure that the External Portal and Gateway host can communicate with all of the Agent machines through the entered hostname, IP address, or FQDN.

- b. **IIS Website Settings** – Configure the IIS website settings for the AvePoint Perimeter External Portal and Gateway. Create a new IIS website that will be used to access the AvePoint Perimeter External Portal and Gateway.
 - o **Create a new IIS Website** – Enter the website name and create a new IIS website for the External Portal and Gateway. Do not change the default website port (16003) used to access the External Portal and Gateway unless a port conflict exists.
 - o **Website Port** – Enter the External Portal and Gateway communication port. The default port is 16003.

***Note:** If you change the port after the installation completes, go to the ...*\AvePoint\Perimeter\GatewayPortal\bin\config* directory on the server where Perimeter External Portal and Gateway is installed, find the **AppSettings.Config** file, make the same change to the value of the **ControlPort** attribute in the

AppSettings.config file, and then restart the IIS website. Otherwise, Perimeter features cannot work well.

- c. **Application Pool Settings** – Create a new IIS application pool for the External Portal and Gateway’s website. The application pool is used to handle requests that are sent to the External Portal and Gateway’s website.
 - o **Create a new application pool** – Enter the name for a new IIS application pool you **want** to create for the External Portal and Gateway’s website.
 - o **Application Pool Account** – Enter the username and password of the account used to create the new application pool.
 - d. Click **Next** to configure the database settings for the External Portal and Gateway.
11. To ensure that the AvePoint Perimeter External Portal and Gateway can run properly, you must ensure the Portal is connected to the same Manager Configuration database configured for your Perimeter Manager. AvePoint Perimeter Manager Configuration database supports **MS SQL** databases only, so only **MS SQL** is available as the **Database Type**. Configure the following settings for connecting the External Portal and Gateway to the Manager Configuration database:
- a. **Database Server** – The MS SQL Server which contains the Manager Configuration database used by the Perimeter Manager.
 - a. **Database Name** – Enter the database name for the Manager Configuration database used by the Perimeter Manager.
 - b. **Database Credentials** – Select the credentials for this Manager Configuration database.
 - o **Windows Authentication** (the default option) – Use this method if you want the user’s identity to be confirmed by Windows. By default, this account is the application pool account chosen in the previous step and cannot be changed. As such, this account must have the **db_owner** database role in the Manager Configuration database specified above.
 - o **SQL Authentication** – SQL Server will confirm the user’s identity according to the user’s account and password. The account must have the **db_owner** database role in the Manager Configuration database specified above.
- *Note:** If you want to change the database credentials after the installation, refer to [Updating Database Credentials](#).
12. Click **Next** to proceed with the installation, click **Back** to change any of the previous settings, or click **Cancel** to abandon all configurations and exit the installation wizard. The installation process displays via the progress bar in the **Installation Process** page.

Once the installation completes, click **Finish** to exit the installation wizard.

***Note:** After installation completes, make sure the Perimeter External Portal and Gateway Server can use the SMTP server to relay e-mails to the external users.

Applying and Publishing the External Portal and Gateway

To ensure all of the users can access the AvePoint Perimeter External Portal via the Internet and the AvePoint Perimeter mobile apps can communicate with the AvePoint Perimeter Manager via the Gateway, the External Portal and Gateway's Website need to be published to the Internet.

There are two methods for publishing the External Portal and Gateway: publishing the External Portal and Gateway directly, or publishing the External Portal and Gateway via reverse proxy. For additional security, AvePoint recommends publishing the External Portal and Gateway via reverse proxy.

Publishing the External Portal and Gateway Directly

To publish the External Portal and Gateway directly to the Internet, configure port mapping between the public URL and the internal URL on the router. The router will forward all of the requests to the public URL, and users can then access the External Portal and Gateway using the public URL.

Publishing the External Portal and Gateway via Reverse Proxy

To publish the External Portal and Gateway via reverse proxy, you need a reverse proxy server that is mapped to the public URL and that can forward requests from the public URL to the back-end External Portal and Gateway server. For detailed information on this step, see [Publishing the External Portal and Gateway via Reverse Proxy](#).

Installing Geolocation Database (optional)

By using the **AvePoint Perimeter Geolocation Database Installation Wizard**, you can install the Geolocation database by creating a new Geolocation database or populating an existing blank database with the required geography location information.

Before installing the Geolocation database, ensure that the [AvePoint Perimeter Geolocation Database Server and Installation Wizard System Requirements](#) are met and that the user running the installation wizard has the permissions required [Permission Requirements for Geolocation Database](#).

To install the AvePoint Perimeter Geolocation Database, complete the following steps:

1. Download the Manager ZIP file by requesting a demo version or by contacting an AvePoint representative for links to this package.
2. Extract the package.
3. In the extracted AvePoint Perimeter Manager directory, double-click the **Setup.exe** file. The Welcome screen appears.
4. Click **Install Geolocation Database**.
5. Carefully review the **License Agreement**.

6. After you have read the agreement, select the **I accept the terms in the license agreement** checkbox, and click **Next**.
7. Click **Browse**.
8. Select the location to store the files that will be used to install the Geolocation database to the target SQL Server. The default location is *C:\Program Files\AvePoint*. Click **Next**.
9. Perimeter performs a brief pre-scan of the environment to ensure that your system meets the AvePoint Perimeter Geolocation Database Installation Wizard system requirements. The status for each rule is listed in the **Status** column. Click the status hyperlink to view detailed information on the scan results, or click **Details** to view detailed information on all of the requirements.

***Note:** You cannot proceed with the installation if the **Status** of any of the rules is **Failed**.

- If the status of any rule is **Failed**, your system does not meet the minimum requirement of the corresponding rule. You must update your environment to meet the AvePoint Perimeter Geolocation database server system requirements, and then click the **Rescan** button to check your environment again.
 - If the status of any rule is **Warning**, your system meets the minimum requirement of the corresponding rule but does not meet the recommended condition. In this case, you can still click **Next** to configure the **Gateway Configuration**.
 - If all of the rule statuses are **Passed**, your system meets all of the recommended conditions in the AvePoint Perimeter Geolocation Database Installation Wizard system requirements. Click **Next** to configure the database settings for the Geolocation database.
10. AvePoint Perimeter Manager supports **MS SQL** databases only, so only **MS SQL** is available as the **Database Type**. Configure the following settings for the Geolocation database:
 - a. **Database Server** – The MS SQL Server name.

***Note:** Ensure that SQL Server meets the [SQL Server Requirements for AvePoint Perimeter Databases](#).
 - b. **Database Name** – Enter a database name for the new Geolocation database you want to create in the MS SQL Database Server entered above or the blank Geolocation database you want to populate the geography location information.
 - c. **Database Credentials** – Select the credentials for this Geolocation database.
 - **Windows Authentication** (the default option) – Use this method if you want the user's identity to be confirmed by Windows. By default, this account is the account used to run this installation wizard and cannot be changed. As such, this account must have the **dbcreator** server role to the SQL Server that will contain the new Geolocation database and the **db_owner** database role in the existing blank Geolocation database.
 - **SQL Authentication** – SQL Server will confirm the user's identity according to the user's account and password. The account must have the following

permissions: **db_owner** database role in the existing blank Geolocation database or **dbcreator** server role in the SQL Server that will contain the new Geolocation database.

11. Click **Next** to proceed with the installation, click **Back** to change any of the previous settings, or click **Cancel** to abandon all configurations and exit the installation wizard. The installation process displays via the progress bar in the **Installation Process** page.
12. Once the installation completes, click **Finish** to exit the installation wizard.
13. After installing the Geolocation database, perform a maintenance job to reduce the database size. Contact your SQL Server database administrator for your organization's guidelines on performing this step. For more information on shrinking a database, refer to Microsoft's TechNet article, [Shrink a Database](#).

Installing AvePoint Perimeter WOPI Host Server

To install the AvePoint Perimeter WOPI Host Server on a server, ensure that [AvePoint Perimeter WOPI Host Server System Requirements](#) are met and the user running the installation wizard is a member of the local **Administrators** group of the current server.

***Note:** If you want to configure the load balance for WOPI Host Servers, your WOPI Hosts must be configured to use Office Online

To install the AvePoint Perimeter WOPI Host Server, complete the following steps:

1. Download the Manager ZIP file by requesting a demo version or by contacting an AvePoint representative for links to this package.
2. Extract the package.
3. In the extracted AvePoint Perimeter Manager directory, double-click the **Setup.exe** file. The Welcome screen appears.
4. Click **Install WOPI Host Server**.
5. Carefully review the **License Agreement**.
6. After you have read the agreement, select the **I accept the terms in the license agreement** checkbox, and click **Next**.
7. Click **Browse**.
8. Select the location for the WOPI Host Server installation. The default installation location is *C:\Program Files\AvePoint*. Click **Next**.
9. Perimeter performs a brief pre-scan of the environment to ensure that your system meets the AvePoint Perimeter WOPI Host Server system requirements. The status for each rule is listed in the **Status** column. Click the status hyperlink to view detailed information on the scan results, or click **Details** to view detailed information on all of the requirements.

***Note:** You cannot proceed with the installation if the **Status** of any of the rules is **Failed**.

- If the status of any rule is **Failed**, your system does not meet the minimum requirement of the corresponding rule. You must update your environment to meet the AvePoint Perimeter WOPI Host Server system requirements, and then click the **Rescan** button to check your environment again.
- If the status of any rule is **Warning**, your system meets the minimum requirement of the corresponding rule but does not meet the recommended condition. In this case, you can still click **Next** to configure the **WOPI Host Server Configuration**.
- If all of the rule statuses are **Passed**, your system meets all of the recommended conditions in the AvePoint Perimeter WOPI Host Server system requirements. Click **Next** to configure the **WOPI Host Server Configuration**.

10. Set up the **WOPI Host Server Configuration**:

- WOPI Host Server Host** – Enter the current machine’s hostname, IP address, or fully qualified domain name (FQDN).

***Note:** Ensure that the WOPI Host Server host can communicate with all of the Agent machines through the entered hostname, IP address, or FQDN.
- IIS Website Settings** – Configure the IIS website settings for the AvePoint Perimeter WOPI Host Server. Create a new IIS website that will be used to access the AvePoint Perimeter WOPI Host Server.
 - Create a new IIS Website** – Enter the website name and create a new IIS website for the WOPI Host Server. Do not change the default website port (16005) used to access the WOPI Host Server unless a port conflict exists.
 - Website Port** – Enter the WOPI Host Server communication port. The default port is 16005.

***Note:** If you change the port after the installation completes, go to the ...\\AvePoint\\Perimeter\\WopiServer\\bin\\config directory on the server where Perimeter WOPI Host Server is installed, find the **AppSettings.Config** file, make the same change to the value of the **ControlPort** attribute in the **AppSettings.config** file, and then restart the IIS website. Otherwise, Perimeter features cannot work well.
- Application Pool Settings** – Create a new IIS application pool for the WOPI Host Server’s website. The application pool is used to handle requests that are sent to the WOPI Host Server’s website.
 - Create a new application pool** – Enter the name for a new IIS application pool you want to create for the WOPI Host Server’s website.
 - Application Pool Account** – Enter the username and password of the account used to create the new application pool.
- Click **Next** to configure the database settings for the WOPI Host Server.

11. To ensure that the WOPI Host Server can work properly, you must ensure the WOPI Host Server is connected to the same Manager Configuration database configured for your Perimeter Manager. AvePoint Perimeter Manager Configuration database supports **MS SQL** databases only, so only **MS SQL** is available as the **Database Type**. Configure the following settings for connecting the WOPI Host Server to the Manager Configuration database:
 - a. **Database Server** – The MS SQL Server which contains the Manager Configuration database used by the Perimeter Manager.
 - b. **Database Name** – Enter the database name for the Manager Configuration database used by the Perimeter Manager.
 - c. **Database Credentials** – Select the credentials for this Manager Configuration database.
 - o **Windows Authentication** (the default option) – Use this method if you want the user's identity to be confirmed by Windows. By default, this account is the application pool account chosen in the previous step and cannot be changed. As such, this account must have the **db_owner** database role in the Manager Configuration database specified above.
 - o **SQL Authentication** – SQL Server will confirm the user's identity according to the user's account and password. The account must have the **db_owner** database role in the Manager Configuration database specified above.
12. Click **Next** to proceed with the installation, click **Back** to change any of the previous settings, or click **Cancel** to abandon all configurations and exit the installation wizard. The installation process displays via the progress bar in the **Installation Process** page.
13. Once the installation completes, click **Finish** to exit the installation wizard.

Setting Up Your Firewall to Unblock Specific Ports

The firewall monitors and restricts the network traffic. Add the exceptions for the following ports to allow the connections.

Source	Destination	Ports	Comments	Protocol	Direction
Admin console	Perimeter Manager/Internal Portal Server	16000	Connect Management Console with web browser	TCP	Two Ways
External Users	Office Web App Server	443	HTTPS connection to OWA Server	TCP	One Way
External Users	Perimeter External Portal Server	16003	HTTPS connection to Perimeter Gateway (or through Reverse Proxy)	TCP	One Way
Office Web App Server	Perimeter WOPI Host Server	16005	Customizable in WOPI Host Server installation	TCP	One Way
Perimeter External Portal Server	Active Directory Domain Controller	Depend on configuration	Active Directory Ports	TCP/UDP	One Way
Perimeter External Portal Server	SMTP/Exchange Server	587	SMTP Port (Default Port: 587)	TCP	One Way
Perimeter External Portal Server	Shared File Location	445	SMB Ports (Default Port: 445)	TCP	One Way
Perimeter External Portal Server	SharePoint Web front-end server with Perimeter Agent installed	16004	Customizable in Perimeter Agent installation *Note: If you have isolated the SharePoint Web front-end server from the External Portal server, this port will not be used. For details, refer to Isolating SharePoint Web Front-End Server from Perimeter External Portal and Gateway Server .	TCP	One Way
Perimeter External Portal Server	SharePoint Web front-end server	80/443	SharePoint Web Application Ports (Default Port: 80/443) *Note: If you have isolated the SharePoint Web front-end server from the External Portal server, this port will not be used. For details, refer to Isolating SharePoint Web Front-End Server from Perimeter External Portal and Gateway Server .	Http/https	One Way
Perimeter External Portal Server	Perimeter Manager/Internal Portal Server	16000	External Portal server uses this port to connect Manager/Internal Portal server for data checking and download file from SharePoint	TCP	Two Ways

Source	Destination	Ports	Comments	Protocol	Direction
Perimeter External Portal Server	SQL Server	1433	SQL Ports (Default Port: 1433)	TCP	One Way
Perimeter Manager/Internal Portal Server	Apple Push Notification service (APNs) External (Apple)	2195	AvePoint Perimeter Manager sends real-time push notifications to iOS devices via the Apple Push Notification service (APNs). After the Manager installation completes, you need to configure the firewall of your Manager server to allow APNs traffic to get past your firewall.	TCP	One Way
Perimeter Manager/Internal Portal Server	Google Cloud Messaging (GCM)	5228, 5229, 5230, or 443	GCM does not provide specific IP addresses, so you must allow your firewall to accept outgoing connections to all of the IP addresses contained in the IP blocks listed in Google's ASN of 15169. TCP ports: 5228, 5229, and 5230. GCM typically only uses 5228, but it sometimes uses 5229 and 5230. The newer versions of Android also fall back to port 443 if ports 5228-5230 are blocked by a firewall.	TCP	One Way
Perimeter Manager/Internal Portal Server	Active Directory Domain Controller	Depend on configuration	Active Directory Ports	TCP/UDP	One Way
Perimeter Manager/Internal Portal Server	SQL Server	1433	SQL Ports (Default Port: 1433)	TCP	One Way
Perimeter Manager/Internal Portal Server	SMTP/Exchange server	587	SMTP Port (Default Port: 587)	TCP	One Way
Perimeter Manager/Internal Portal Server	Perimeter WOPI Host Server	16005	Customizable in the WOPI Host Server installation, and required for testing the connection to WOPI Host Server and collecting diagnostic log file	TCP	One Way
Perimeter Manager/Internal Portal Server	Perimeter External Portal Server	16003	Customizable in the External Portal installation and required for testing the connection to External Portal server and collecting diagnostic log file	TCP	One Way
Perimeter Manager/Internal Portal Server	Shared File Location	445	SMB ports used by Perimeter manager to check shared file location	TCP	One Way
Perimeter Manager/Internal Portal Server	SharePoint Web front-end server	80/443	SharePoint Web Application Ports	TCP	One Way

Source	Destination	Ports	Comments	Protocol	Direction
Perimeter Manager/Internal Portal Server	SharePoint Web front-end server with Perimeter Agent installed	16004	Perimeter Manager communicates with Perimeter Agent	TCP	One Way
Perimeter WOPI Host Server	SQL Server	1433	SQL Ports (Default Port: 1433)	TCP	One Way
Perimeter WOPI Host Server	SMTP/Exchange server	587	SMTP port (Default Port: 587)	TCP	One Way
Perimeter WOPI Host Server	SharePoint Web front-end server	80/443	SharePoint Web Application Ports (Default Port: 80/443)	TCP	One Way
Perimeter WOPI Host Server	Shared File Location	445	SMB ports used by WOPI Host server to access shared file location	TCP	One Way
Perimeter WOPI Host Server	SharePoint Web front-end server with Perimeter Agent installed	16004	Customizable in Perimeter Agent installation	TCP	One Way
SharePoint Web front-end server with Perimeter Agent installed	Perimeter Manager/Internal Portal Server	16000	Perimeter Agent replies to Perimeter Manager	TCP	One Way

Configuring the Integration of the External Portal and SAP Jam Group

AvePoint provides an XML file so that SAP Jam group owner can use this file in the OpenSocial Gadget to enable the integration. The URL of that XML file is in the format of `http://[ExternalPortal:port]/portal/home/SAPJAMXML`. After you have finished the installation of all Perimeter components, you must go to a configuration file to update that URL with your external portal hostname and port number. Complete the steps below:

1. Navigate to the `... \AvePoint\Perimeter\Manager\files` directory on the server where Perimeter External Portal is installed.
2. Open the **PerimeterList.xml** file using Notepad.
3. Find the **action = 'https://externalPortalHost:Port/Portal/Home/AssignIndex'** attribute in this file, and change the External Portal hostname and port number to the value of this attribute.
4. Save the modification and close the file.

Updating Database Credentials

Complete the steps below to update the access credentials for the Perimeter Manager database or External Portal and Gateway database.

1. Find the Command Prompt on the server where the Perimeter Manager or the External Portal and Gateway has been installed.
2. Right-click **Command Prompt**, and then select **Run as administrator** in the drop-down list.
3. Enter the full path of the **PerimeterManagerPostInstall.exe** file in the **bin** folder under the installation path of Perimeter Manager server or the External Portal and Gateway server.
4. Enter **s** and then press Enter to display the access information.
5. Enter **PerimeterManagerPostInstall.exe c false "username"**. Replace the **username** with the user you want to use in the future. Follow the message to enter the password of the user.
***Note:** If you want to use Windows Authentication to access databases, enter **PerimeterManagerPostInstall.exe c true**.
6. Exit the **Command Prompt** window after the execution completes.

Isolating SharePoint Web Front-End Server from Perimeter External Portal and Gateway Server

To isolate the SharePoint Web front-end servers that have Perimeter Agent installed from the Perimeter External Portal & Gateway server and use the Perimeter Manager & Internal Portal server to communicate with the SharePoint Web front-end servers, complete the steps below:

1. Go to the ...*\AvePoint\Perimeter\GatewayPortal\bin\Config* directory on the server where Perimeter External Portal and Gateway is installed.
2. Find the **AppSettings.config** file and open it with Notepad.
3. Add the `<add key="IsolateExPortalSP" value="true"/>` node into the `<appsettings></appsettings>` node.
4. Save the configurations and close this file.
5. Restart the IIS service on the External Portal and Gateway server.

Updating AvePoint Perimeter

To update your Perimeter system to Perimeter 1.9.1, you must update the Perimeter Manager, Gateway, Portal, and Agents via the Upgrade solution tool. The upgrade solution tool is an automated tool that enables you to directly update Perimeter to the latest version. This tool is provided in the update patch **AvePoint_Perimeter_1.0_SP9_CU1.zip**.

***Note:** If you have changed the AvePoint Perimeter's IIS website names or application pool names after the installation of the Manager, External Portal and Gateway, and WOPI Host Server completed, you must modify the information in specific configuration files as well before you start the update progress. For details, refer to [Before Getting Started with the Update](#).

If you purchased AvePoint Perimeter Pro and are using the Secured Share solution, refer to [Updating AvePoint Perimeter Pro Secured Share Solution](#) after updating the Perimeter components listed below.

Before Getting Started with the Update

If you have changed the IIS website names or application pool names for Perimeter Manager, External Portal and Gateway, or WOPI Host Server after the installation completed, you must make the same changes in the **PerimeterManagerPostInstall.Config** file. Otherwise, the update may fail.

To check and edit the post installation information, complete the steps below:

1. Go to the **bin** folder under the installation path of Perimeter Manager server, External Portal and Gateway server, and the WOPI Host Server. The default Manager installation path is ... \AvePoint\Perimeter\Manager; the default External Portal and Gateway installation path is ... \AvePoint\Perimeter\GatewayPortal; the default WOPI Host Server installation path is ... \AvePoint\Perimeter\WopiServer.
2. Find the **PerimeterManagerPostInstall.Config** file and open it with Notepad.
3. Confirm or edit the values of the **WebSiteName** attribute and the **AppPoolName** attribute to ensure that these values are same as the website names and application pool names listed in IIS Manager.
4. Save the changes and close the file.

Updating AvePoint Perimeter Manager and Agent Components Using the Perimeter Upgrade Solution

This section explains how to update Perimeter Manager and Agent components using the upgrade solution tool. To use this tool, run the tool on the AvePoint Perimeter Manager server. The user running this tool must be a member of the local Administrators group on the Perimeter Manager server.

Launching the Perimeter Upgrade Solution

The Perimeter Upgrade Solution is included in your Perimeter update package. Follow the steps below to launch the Perimeter Upgrade Solution:

1. Download the **AvePoint_Perimeter_1.0_SP9_CU1.zip** folder by contacting an AvePoint representative.
2. Copy the downloaded **AvePoint_Perimeter_1.0_SP9_CU1.zip** file to the AvePoint Perimeter Manager server or AvePoint Perimeter External Portal and Gateway server of the Perimeter system to be updated.
3. Extract the **AvePoint_Perimeter_1.0_SP9_CU1.zip** folder.
4. Open the extracted **AvePoint_Perimeter_1.0_SP9_CU1** folder and double-click the **RunUpgrade.bat** file to start the Perimeter Upgrade Solution. The **Requirement Pre-Scan** interface for updating **AvePoint Perimeter** appears, and the **Requirement Pre-Scan** starts automatically. For details on the **Requirement Pre-Scan**, see the next section [Running the Requirement Pre-Scan](#).

Running the Requirement Pre-Scan

In the **Requirement Pre-Scan** interface, the Perimeter Upgrade Solution automatically scans your environment to ensure the following requirements are met:

- **Net.TCP Port Sharing Service is running** – This requirement ensures that the AvePoint Perimeter services can share the ports for communication during the upgrade.
- **Checking if the AvePoint Perimeter Manager Service is running** – This requirement ensures that the AvePoint Perimeter Manager Service is running on the AvePoint Perimeter Manager server.
- **Checking if the adapter for AvePoint Perimeter Manager Service is installed** – This requirement ensures that the AvePoint Perimeter Manager Service adapter is installed on the current server. The Perimeter Upgrade Solution uses this adapter to retrieve information from the AvePoint Perimeter Manager Service.

You cannot advance to the next step if any of the requirements have a **Status** of **Failed**. If any of the requirements have a **Failed** status, update your environment and then click the **Retry Scan** button to scan your environment again.

Once all of the requirements have a **Passed** status, click **Continue**. Proceed to the next section in this guide.

Configuring Service Connection

Configure the service host to connect the local host to the service you want to update. Complete the following settings:

- **Local Host** – Confirm the local hostname or IP address of the server that is running this update.
- **Service Host** – Confirm the hostname or IP address of the server where the service you want to update resides.
- **Service Port** – Confirm the port number for connecting to this service.

Click **Continue**. Refer to the next section for instructions.

Configuring Update Settings

The **Update Settings** interface allows you to view and customize the general settings in the Perimeter Upgrade Solution.

To access **Update Settings**, click the settings () button in the upper-right corner of the **Perimeter Upgrade Solution** interface. In the **Update Settings** interface, you can view the following settings:

- **Patch Storage Location** – The location to store the update patches imported from the local system. The default path is the ...*PatchManager*\PatchFolder directory under the extracted folder on the local system.
- **Update Port** – The port used to communicate with the Perimeter Service host servers during the update processes. The default update port is **14007**.

You can use the default **Update Settings**, or customize these **Update Settings** by completing the following steps:

1. **Patch Storage Location** – Select the desired location to store the update patches imported from the local system by completing the following steps:
 - a. Click the **Browse** button. The **Browse For Folder** window appears.
 - b. Select the desired folder and click **OK**.

***Note:** You must ensure the current logon user has **Write** permissions in the selected folder.
2. **Update Port** – Enter the desired port into the **Update Port** text box for communicating with the Perimeter Service host servers during the update processes and click **Test** to verify whether the entered port is available.
3. Click **Save** to save the configurations.

Updating Services

The **Upgrade** interface provides a wizard for installing an update patch on the Perimeter Service host servers. To use the **Upgrade** wizard for updating services, complete the following steps:

1. Access the **Upgrade** wizard by clicking **Upgrade** in the **AvePoint Perimeter** homepage, or clicking **Upgrade** on the ribbon.

2. In the **Step 1. Patch Selection** interface, you will import update patches from your server and select the update patch for updating AvePoint Perimeter:
 - a. Click **Import Patch**. The **Open** window appears.
 - b. Select the desired update patch and click **Open**. The Perimeter Upgrade Solution will import the selected update patch to the **Patch Storage Location** configured in the **Update Settings** interface. After the selected patch is successfully imported, you can view the detailed information of the imported patch in the viewing pane, including the patch name, type, version, size and last installation time.
 - To view the product versions that can be updated via installing an update patch, select the patch in the viewing pane and click **Supported Versions** on the ribbon. A pop-up window appears, listing the supported product versions of the selected update patch.
 - To delete a previously imported update patch from the local system, select the patch in the viewing pane and click **Delete Patch** on the ribbon. The original file and the corresponding file stored in the **Patch Storage Location** will be deleted at the same time.
 - c. Select the update patch that will be used to update AvePoint Perimeter in the viewing pane.
 - d. Click **Next**.
3. In the **Step 2. Service Selection** interface, all of AvePoint Perimeter's installed services are displayed in the viewing pane, including the service host address, service port, current version, service type, service status, and the installation status of the update patch selected in the previous step.

***Note:** You must ensure the selected service is started and the current version of the selected service is included in the **Supported Versions** of the update patch selected in the previous step.

Select the services you want to update in the viewing pane and click **Next**. You can select Manager components (**Manager**, **External Portal and Gateway**, and **WOPH Host Server**) and Agents at the same time to update the services together.
4. In the **Step 3. Overview** interface, the update patch selected in **Step 1. Patch Selection** and services selected in **Step 2. Service Selection** are displayed in the viewing pane. Review your update selections and click **Install** to start the installation.

***Note:** If a restart of the IIS service on the service host is needed after the update patch installs, a pop-up message will ask you if you want to restart the IIS service immediately after installation completes, or do it manually later.
5. In the **Step 4. Installation Progress** interface, the installation progress is displayed via the progress bar. In the viewing pane, you can view the installation progress for each service host.

To view the details of the installation progress on a specific service host, click **View Details** in the **Action** column of the corresponding service host and view the details in the pop-up window.
6. Click **Next**.

7. In the **Installation Complete** page, perform one of the following operation:
 - To exit this Perimeter Upgrade Solution, click **Finish**.
 - To use the **Upgrade** wizard to update other services, click **Continue Upgrade** to go to the **Step 1. Patch Selection** interface of the **Upgrade** wizard.
 - To go to the AvePoint Perimeter homepage, click **Go to AvePoint Perimeter**.

Viewing Update History

After you have installed or attempted to install patches to update AvePoint Perimeter, you can view the update history of AvePoint Perimeter and the installation history of imported update patches in the **View History** interface.

To access **View History**, click **View History** in the **AvePoint Perimeter** homepage or click **View History** on the ribbon. There are two tabs in the **View History** interface:

- **Patch** – On this tab, all of the patches you have installed or attempted to install are displayed, including the patch name, type, version, size and last installation time of each patch. For details information on viewing the installation history of a specific patch, refer to [Viewing Installation History of Update Patches](#).
- **Service** – On this tab, all of the services you have updated or attempted to update are displayed, including the service host, service type, service status, and update time of each service. For details information on viewing the update history of a specific service, refer to [Viewing Update History of Services](#).

Viewing Installation History of Update Patches

To view the installation history of a specific update patch, complete the following steps:

1. Click the **Patch** tab.
2. On the **Patch** tab, select the update patch whose installation history you want to view and click **View History** in the **Action** column. The **Installation History** interface for the selected patch appears.
3. In the **Installation History** interface, all of the services where this patch has been installed or attempted to install are displayed, including the service host, service type, installation status, installation time of each service. To view the details of the installation progress of the selected patch on a specific service, select the desired service and click **View Details** in the **Action** column. The **View History** interface appears, displaying the details of the installing the selected patch on the selected service.

Viewing Update History of Services

To view the update history of a specific service, complete the following steps:

1. Click the **Service** tab.

2. On the **Service** tab, select the service whose update history you want to view and click **View History** in the **Action** column. The **Update Service History** interface for the selected patch appears.
3. In the **Update Service History** interface, all of the patches you have installed or attempted to install on this service are displayed, including the patch name, patch version, installation status, installation time of each patch. To view the details of the update history of a specific service by installing a specific update patch, select the desired patch and click **View Details** in the **Action** column. The **View History** interface appears, displaying the details of the installing the selected patch on the selected service.

Updating AvePoint Perimeter Pro Secured Share Solution

If you have deployed the AvePoint Perimeter Pro Secured Share solution in your SharePoint farm, you must remove the previously deployed solution from the farm and then deploy the new AvePoint Perimeter solution.

To update the AvePoint Perimeter Pro Secured Share solution in your SharePoint farm, follow the steps below to remove the previously deployed solution and then deploy the new version's solution:

1. Go to the **Central Administration** interface of your SharePoint farm and navigate to **System Settings > Manage farm solutions** to access the **Solution Management** interface.
2. Click the link of the solution. The **Solution Properties** page appears.
3. Click **Retract Solution** to retract the solution from the farm. The **Retract Solution** page appears.
4. Click **OK** and return to the **Solution Management** page.
5. After the status of the solution becomes **Not Deployed**, click the link of the solution. The **Solution Properties** page appears.
6. Click **Remove Solution** and click **OK** in the window to remove the solution from the SharePoint farm. After the solution is removed, the solution is no longer displayed in the **Solution Management** page.
7. Deploy the new AvePoint Perimeter Pro Secured Share solution of Perimeter to your SharePoint farm. For details, refer to [Deploying and Activating the AvePoint Perimeter Secured Share Feature](#).
8. After the AvePoint Perimeter Pro Secured Share solution is successfully updated to Perimeter 1.9.1, you also need to update the data of the files that were shared via the previously deployed **Secured Share** feature within your SharePoint farm to ensure these files can be properly accessed and managed in Perimeter 1.9.1. To update the data of the secured shared files, manually run a **Secure share maintenance** timer job in Perimeter Manager > **Configure > Timer Job Definition**. For detailed information on manually running a timer job, refer to [Monitoring Timer Job Definition](#).

Logging into AvePoint Perimeter Management Console for the First Time

To access AvePoint Perimeter Manager, ensure your browser is included in the [Supported Browsers for AvePoint Perimeter Manager](#).

In AvePoint Perimeter Manager, multiple administrator accounts may be configured in the **Account Manager**. However, when logging into AvePoint Perimeter Manager for the first time, you must log in using the built-in administrator account credentials shown below:

- Login ID: **admin**
- Password: **admin**

By default, the built-in administrator account has the **Secure Share Control** permission level in Perimeter Management Console.

In the **Login** page of the Perimeter Management Console, you can select the **Remember my login** option to let the Management Console remember your login credentials, which will allow you to automatically log into the Management Console without providing your login credentials in a specific time range. To enable this feature, configure the settings in the **AppSettings.config** file. For details on enabling this feature and customize the time range, refer to [Remembering the Login Credentials for Automatic Sign-In](#).

***Note:** If your Perimeter environment is updated from Perimeter 1.7 or earlier, the permissions of the existing Perimeter administrators will be the same as before.

Changing Your Password

Since AvePoint Perimeter is a security product, AvePoint highly recommends that you change this password upon initial login regardless of whether you are trialing the product or installing it onto a production environment.

Complete the steps below to edit your account settings and change your password.

1. When you log into the Perimeter Manager GUI, the currently logged-on user will be displayed at the top right corner of the Perimeter interface. Click the current username. A drop-down list appears. Click **My Settings** and enter the **My Settings** page.
2. In the **My Settings** interface, you can view the detailed information of the current logged-on user and the Administration groups it belongs to. Click **Edit** on the ribbon.
3. In the **Password Settings** field, select the **Change my password** option. If one user does not have the permission to change the password, the password field is dimmed out. Provide your **Old password** and enter and confirm your new password.

4. After you finish the configuration, click **Save** to save your changes and exit the **My Settings** page.

Remembering the Login Credentials for Automatic Sign-In

By default, if you select the **Remember my Login** option on the Perimeter Management Console **Login** page, only your account name will be remembered. If you want to allow the Perimeter Management Console to remember your login credentials (username and password) so that the users can automatically log into the Management Console within a specific time range, complete the steps below:

1. Go to the ... \AvePoint\Perimeter\Manager\bin\Config directory on the server where the Perimeter Manager is installed.
2. Find the **AppSettings.config** file and open it with Notepad.
3. Add the `<add key="keepMeSignIn" value="true"/>` node into the `<appsettings></appsettings>` node. With the value set to **true**, selecting the **Remember my Login** option will allow the Management Console to remember your login credentials and keep you signed in within 8 hours by default.
4. To change the time range, find the `<add key="keepMeSignInHours" value="8"/>` node. Enter another integer for the **value** attribute. The unit of time is **Hour**.
5. Save the configurations and close this file.

Overview of the Configurations in the AvePoint Perimeter Management Console

After you logged into the Perimeter Management Console as the Perimeter administrator, you can get started with [Configuring Perimeter General Settings](#) or add other administrator accounts into the Management Console and control their activities in the Management Console by granting them specific permission levels.

AvePoint Perimeter provides only two default permission levels: **Full Control** and **Secure Share Control**. The built-in administrator account is granted the **Secure Share Control** permission level by default. The **Secure Share Control** permission level only provides users with access to the basic settings of using Perimeter and the Secure Share related configurations; The **Full Control** permission level allows users to access any settings in the Perimeter Management Console. For details on managing administrator accounts and the permission levels, refer to [Configuring Admin Accounts](#).

The **Home** page of the Perimeter Management Console lists all of the basic settings required for using Secure Share and the configurations that enhance the use of the Secure Share feature. Refer to [Configuring Perimeter Secure Share Pro Features](#) for the overview of deploying and using the Secure Share feature, and refer to [Configuring Content Access Control to SharePoint Sites](#) for the instructions on controlling and monitoring access to the SharePoint sites.

Configuring Perimeter General Settings

To work with Perimeter, you must complete the following general settings:

1. [Configuring General Settings](#)
2. [Configuring Notification Settings](#)
3. [Configuring Windows Phone Log Location](#) (Optional)
4. Request and configure a Bing Maps key, if you want to use Bing Maps in Perimeter for location services. For details, refer to [Applying the Bing® Maps Key](#).

Configuring Perimeter Secure Share Pro Features

After [Configuring Perimeter General Settings](#), follow the steps below to configure the AvePoint Perimeter Pro **Secured Share** and **Virtual Views** features. Click the links to jump to the corresponding sections for detailed instructions.

1. To enable internal users of your organization to share files with others via the **AvePoint Perimeter Secured Share** feature within SharePoint sites, complete the following settings:

- a. [Deploying the AvePoint Perimeter Secured Share Solution on a SharePoint 2016 Farm, Deploying the AvePoint Perimeter Secured Share Solution on a SharePoint 2013 Farm, or Deploying the AvePoint Perimeter Secured Share Solution on a SharePoint 2010 Farm](#)
 - b. [Activating the AvePoint Perimeter Secured Share Feature](#)
2. To configure settings for managing Secure Share feature, you can perform the following actions:
 - [Configuring System Credentials](#)
 - [Configuring Shared File Location](#)
 - [Configuring Office Web Apps Server Settings](#)
 - [Configuring Secure Share Control Policy](#)
 - [Allowing SharePoint Permissions to Decide the Available Permission Levels](#)
 - [Configuring Watermark Settings](#)
 - [Configuring Content Access Control for Secure Share](#)
 - Configuring Secure Share Options and Customizations
 - [Sending Secured Share Notification E-mail as the Shared by User](#)
 - [Enabling Update Notification](#)
 - [Customizing the Threshold for Sending Reminder E-mail Notifications for Locked Shared Files on the External Portal](#)
 - [Allowing Users that are not Shared With to Sign Up to the External Portal](#)
 - [Defining the Default Expiration Duration for Secure Share via CONFIG File](#)
 - [Defining the Minimum Interval for Sending a One-Time Access Passcode](#)
 - [Configuring External User Password Policy](#)
3. To view and manage all of the files shared via the **AvePoint Perimeter Secured Share** feature, use the **Manage Shared Files** feature in Perimeter Manager. For details, see [Managing Shared Files](#).
4. To share SharePoint files with groups of users based on predefined criteria via the **Virtual Views** feature in AvePoint Perimeter Manager, complete the following settings:
 - a. [Managing User Access Groups](#)
 - b. [Configuring Virtual Views for Sharing Files in Bulk](#)
 - c. [Sharing Virtual Views with User Access Groups](#)

Configuring Content Access Control to SharePoint Sites

After [Configuring Perimeter General Settings](#), follow the steps below to deploy content access control on your SharePoint environment. Click the links to jump to the corresponding sections for detailed instructions.

1. First, enroll mobile devices into this AvePoint Perimeter management system. This allows you to manage mobile device access and configure content access control features for your SharePoint environment. For detailed instructions, refer to [Sending an Individual Device Enrollment Request](#).

2. To control content access to your environment via any device, complete the following settings:

***Note:** To use the **Location Type** and **Location** conditions while configuring rules for **Content Access Policy** features, configure the settings in steps **a**, **b**, and **c** before performing step **d**.

- a. [Configuring Geolocation Database Connection](#) (optional)
- b. [Configuring Location Groups](#) (optional)
- c. [Configuring Locations](#) (optional)

***Note:** In order to set content access policies for a particular user/device, that device must be enrolled in this step. For information on enrolling devices, see [Enrolling a Device](#).

- d. [Configuring Content Access Policies](#)

3. To publish SharePoint sites for secured accessing via enrolled devices based on pre-defined criteria, complete the following settings:

- a. [Managing Device Groups](#)
- b. [Configuring Site Access Permission for Enrolled Devices](#)

4. To monitor end-user activity and locations within your environment via Burglar Alarm Rules, complete the following settings:

***Note:** To use **Document Activity** Burglar Alarm rules which monitor user activities using the same definitions as SharePoint audit events (For details on these activities, refer to [Types of Burglar Alarm Rules](#)), configure the settings in steps **a**, **b**, and **c** before performing step **d**.

- a. [Configuring SharePoint Audit Settings for Document Activity Rules at the Web Application or Site Collection Level](#) (optional)
- b. [Retrieving Audit Data for Document Activity Rules](#) (optional)
- c. [Configuring Document Activity Collections](#) (optional)
- d. [Configuring and Applying Burglar Alarm Rules](#)

Deploying and Activating the AvePoint Perimeter Secured Share Feature

Prior to using the AvePoint Perimeter Secured Share feature in your SharePoint farm, you must deploy the **AvePointPerimeterSecureShare.wsp** solution on your SharePoint farm. The sections below offer detailed instructions on deploying and activating the AvePoint Perimeter Secured Share feature to SharePoint farms.

Deploying the AvePoint Perimeter Secured Share Solution on a SharePoint 2016 Farm

To deploy the **AvePointPeirmeterSecureShare2016.wsp** solution on your SharePoint 2016 farm, complete the steps below:

1. Log into the Agent server which is the Web front-end server of the SharePoint farm where you want to deploy the **AvePointPerimeterSecureShare2016.wsp** solution as a member of the **Local Administrators** group of the local computer and a member of the **Farm Administrators** of your SharePoint farm.
2. Navigate to **Start > All Programs > Microsoft SharePoint 2016 Products**.
3. Right-click on **SharePoint 2016 Management Shell** and select **Run as administrator**.
4. In the **Administrator: SharePoint 2016 Management Shell** command line interface, enter and run the following command:
add-spsolution
5. Enter the path of the **AvePointPerimeterSecureShare2016.wsp** file for the **LiteralPath** parameter and press **Enter** to start installing the **AvePointPerimeterSecureShare2016.wsp** solution on your SharePoint farm. The **AvePointPerimeterSecureShare2016.wsp** solution file is stored in the `\bin\SecureShare\2016` folder under the installation path of the Perimeter Agent. The default path is `... \Program Files\AvePoint\Perimeter\Agent\bin\SecureShare\2016\AvePointPerimeterSecureShare2016.wsp`. When the command is successfully executed, the **AvePointPerimeterSecureShare2016.wsp** solution is installed on your SharePoint farm.
6. To verify that the **AvePointPerimeterSecureShare2016.wsp** is installed on your SharePoint farm, navigate to **Central Administration > System Settings > Manage farm solutions** in SharePoint to access the **Solution Management** page. You can view the **avepointperimeterseureshare2016.wsp** in the **Solution Management** page.
7. To deploy the **avepointperimeterseureshare2016.wsp** solution on your SharePoint farm, click the **avepointperimeterseureshare2016.wsp** solution to access the **Solution Properties** page.
8. Click **Deploy Solution**. The **Deploy Solution** page appears.
9. In the **Deploy When?** field, select **Now**.

10. In the **Deploy To?** field, select **All Content Web applications** from the drop-down list.
11. Click **OK** to start deploying the solution.

When the solution is successfully deployed, the **Status** of the **avepointperimetersecureshare2016.wsp** solution in the **Solution Management** page becomes **Deployed**, and the **Deploy To** column displays all of the content Web applications within this farm.

Deploying the AvePoint Perimeter Secure Share Solution on a SharePoint 2013 Farm

In your SharePoint 2013 farm, there may be site collections in either SharePoint 2013 experience version or SharePoint 2010 experience version. If you only want to use the secure share feature in SharePoint 2013 experience version site collections, complete the steps below to deploy the **AvePointPerimeterSecureShare.wsp** solution:

1. Log into the Agent server which is the Web front-end server of the SharePoint farm where you want to deploy the **AvePointPerimeterSecureShare.wsp** solution as a member of the **Local Administrators** group of the local computer and a member of the **Farm Administrators** of your SharePoint farm.
2. Navigate to Start > All Programs > Microsoft SharePoint 2013 Products.
3. Right-click on **SharePoint 2013 Management Shell** and select **Run as administrator**.
4. In the **Administrator: SharePoint 2013 Management Shell** command line interface, enter and run the following command:

```
add-spsolution
```
5. Enter the path of the **AvePointPerimeterSecureShare.wsp** file for the **LiteralPath** parameter and press **Enter** to start installing the **AvePointPerimeterSecureShare.wsp** solution on your SharePoint farm. The **AvePointPerimeterSecureShare.wsp** solution file is stored in the `\bin\SecureShare\2013` folder under the installation path of the Perimeter Agent. The default

path is ... \Program

Files\AvePoint\Perimeter\Agent\bin\SecureShare\2013\AvePointPerimeterSecureShare.wsp.

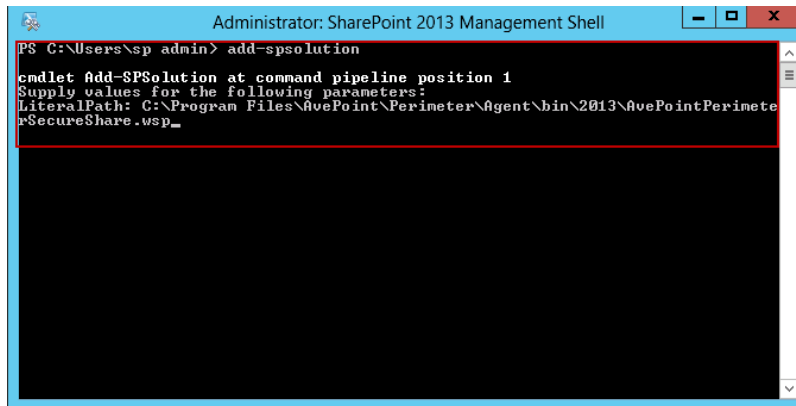


Figure 2: Administrator: SharePoint 2013 Management Shell command line interface.

When the command is successfully executed, the **AvePointPerimeterSecureShare.wsp** solution is installed on your SharePoint.

6. To verify that the **AvePointPerimeterSecureShare.wsp** is installed on your SharePoint farm, navigate to **Central Administration > System Settings > Manage farm solutions** in SharePoint to access the **Solution Management** page. You can view the **avepointperimetersecurshare.wsp** in the **Solution Management** page.
7. To deploy the **avepointperimetersecurshare.wsp** solution on your SharePoint farm, click the **avepointperimetersecurshare.wsp** solution to access the **Solution Properties** page.
8. Click **Deploy Solution**. The **Deploy Solution** page appears.
9. In the **Deploy When?** field, select **Now**.
10. In the **Deploy To?** field, select **All Content Web applications** from the drop-down list.
11. Click **OK** to start deploying the solution.
12. When the solution is successfully deployed, the **Status** of the **avepointperimetersecurshare.wsp** solution in the **Solution Management** page becomes **Deployed**, and the **Deploy To** column displays all of the content Web applications within this farm.

***Note:** If you want to use the Secure Share feature in either SharePoint 2010 experience version site collections or SharePoint 2013 experience version site collections in a SharePoint 2013 farm, you must install and deploy the solution as follows:

1. Log into the Agent server which is the Web front-end server of the SharePoint farm where you want to deploy the **AvePointPerimeterSecureShare.wsp** solution as a member of the **Local Administrators** group of the local computer and a member of the **Farm Administrators** of your SharePoint farm.
2. Navigate to **Start > All Programs > Microsoft SharePoint 2013 Products**.
3. Right-click on **SharePoint 2013 Management Shell** and select **Run as administrator**.

4. In the **Administrator: SharePoint 2013 Management Shell** command line interface, enter `get-spsolution` and press Enter. Copy the solution ID from the **SolutionId** column of **AvePointPerimeterSecureShare.wsp**

5. Enter the following commands:

```
Install-SPSolution -Identity "SolutionId" -AllWebApplications -GACDeployment -CompatibilityLevel {14,15}
```

***Note:** Enter the **SolutionId** that was copied in Step 4 of **AvePointPerimeterSecureShare.wsp** solution as the value of the **Identity** parameter.

6. When the command is successfully executed, the **AvePointPerimeterSecureShare.wsp** solution is installed on your SharePoint 2013 farm and deployed to all of the Web applications containing the site collections in either the SharePoint 2010 or SharePoint 2013 experience version.

Deploying the AvePoint Perimeter Secured Share Solution on a SharePoint 2010 Farm

To deploy the **AvePointPerimeterSecureShare2010.wsp** solution on your SharePoint 2010 farm, complete the following steps:

1. Log into the Agent server which is the Web front-end server of the SharePoint farm where you want to deploy the **AvePointPerimeterSecureShare2010.wsp** solution as a member of the **Local Administrators** group of the local computer and a member of the **Farm Administrators** of your SharePoint farm.
2. Navigate to **Start > All Programs > Microsoft SharePoint 2010 Products**.
3. Right-click on **SharePoint 2010 Management Shell** and select **Run as administrator**.
4. In the **Administrator: SharePoint 2010 Management Shell** command line interface, enter and run the following command:

```
add-spsolution
```

5. Enter the path of the **AvePointPerimeterSecureShare2010.wsp** file for the **LiteralPath** parameter and press **Enter** to start installing the **AvePointPerimeterSecureShare2010.wsp** solution on your SharePoint farm. The **AvePointPerimeterSecureShare2010.wsp** solution file is stored in the `\bin\SecureShare\2010` folder under the installation path of the Perimeter Agent. The default path is `...Program Files\AvePoint\Perimeter\Agent\bin\SecureShare\2010\AvePointPerimeterSecureShare2010.wsp`.

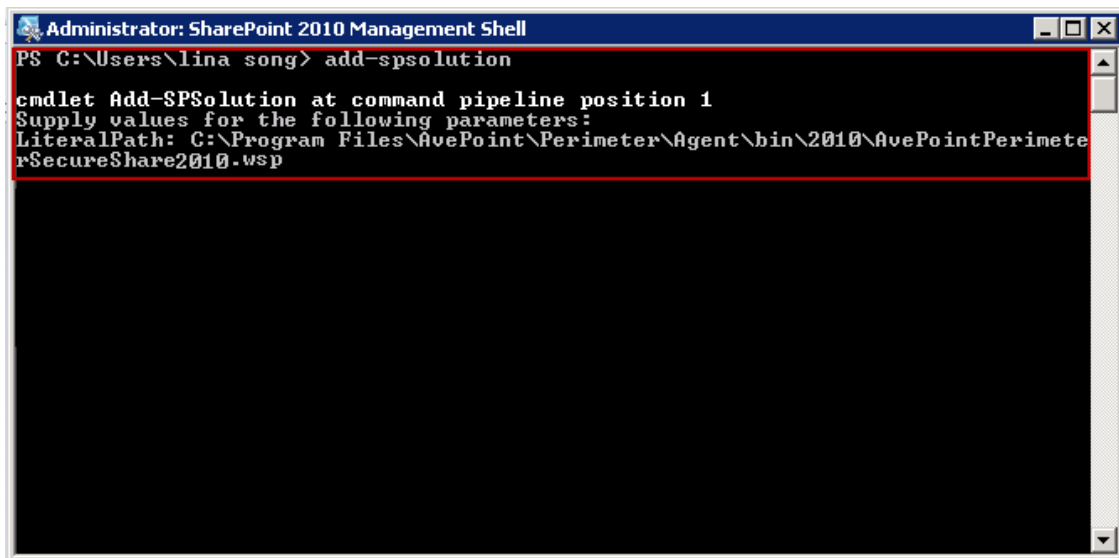


Figure 3: Installing the solution in the Administrator: SharePoint 2010 Management Shell command line interface.

When the command is successfully executed, the **AvePointPerimeterSecureShare2010.wsp** solution is installed on your SharePoint.

6. To verify that the **AvePointPerimeterSecureShare2010.wsp** is installed on your SharePoint farm, navigate to **Central Administration > System Settings > Manage farm solutions** in SharePoint to access the **Solution Management** page. You can view the **avepointperimeterseureshare2010.wsp** in the **Solution Management** page.
7. To deploy the **avepointperimeterseureshare2010.wsp** solution on your SharePoint farm, click **avepointperimeterseureshare2010.wsp** to access the **Solution Properties** page.
8. Click **Deploy Solution**. The **Deploy Solution** page appears.
9. In the **Deploy When?** field, select **Now**.
10. In the **Deploy To?** field, select **All Content Web applications** from the drop-down list.
11. Click **OK** to start deploying the solution.
12. When the solution is successfully deployed, the **Status** of the **avepointperimeterseureshare2010.wsp** solution in the **Solution Management** page becomes **Deployed**, and the **Deploy To** column displays all of the content Web applications within this farm.

Activating the AvePoint Perimeter Secured Share Feature

After the **AvePointPerimeterSecureShare2016.wsp** (for SharePoint 2016), **AvePointPerimeterSecureShare.wsp** (for SharePoint 2013), or **avepointperimeterseureshare2010.wsp** (for SharePoint 2010) solution is deployed to a Web application, the **AvePoint Perimeter Secured Share** feature is added to each site within the Web application. To activate the **AvePoint Perimeter Secured Share** feature in SharePoint sites, select either of the following methods:

- To activate the **AvePoint Perimeter Secured Share** feature in one site at a time, follow the instructions in [Activating the AvePoint Perimeter Secured Share Feature in Site Settings](#).
- To activate the **AvePoint Perimeter Secured Share** feature in all of the sites within site collections in bulk, follow the instructions in [Activating the AvePoint Perimeter Secured Share Feature Using SharePoint Management Shell Command Lines](#).

***Note:** If users who do not belong to the Active Directory domain within your SharePoint farm can log into sites using ADFS authentication, they can also use the **AvePoint Perimeter Secured Share** feature to share files from sites where this feature is active. To ensure that these users can properly use the **AvePoint Perimeter Secured Share** feature, you must first synchronize these users to the Perimeter system from the domain controller of the Active Directory domain they reside in before activating the **AvePoint Perimeter Secured Share** feature in the site. To do this, use the **Synchronize Active Directory Users** feature. For details, refer to [Synchronizing Active Directory Users](#).

Activating the AvePoint Perimeter Secured Share Feature in Site Settings

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

1. Access the site for which you want to activate **AvePoint Perimeter Secured Share** feature. In SharePoint 2010, navigate to: **Site Actions > Site Settings > Manage site features**. In SharePoint 2013 and SharePoint 2016, navigate to: Settings Icon (⚙) > **Site Settings > Manage site features**.
2. Click **Activate** next to the **AvePoint Perimeter Secured Share** feature to enable the feature for this site.
3. After activating the **AvePoint Perimeter Secured Share** feature, the status of the feature reads **Active** in the **Status** column.
4. Click **OK** to save the change.

Activating the AvePoint Perimeter Secured Share Feature Using SharePoint Management Shell Command Lines

To activate the **AvePoint Perimeter Secured Share** feature in all of the sites within site collections in bulk, use the SharePoint Management Shell by completing the following steps:

1. Log into the Web front-end server that contains the sites where you want to activate the **AvePoint Perimeter Secured Share** feature as a member of the local **Administrators** group.
2. Navigate to **Start > All Programs > Microsoft SharePoint 2016 Products/Microsoft SharePoint 2013 Products/Microsoft SharePoint 2010 Products**.
3. Right-click on **SharePoint 2016 Management Shell/SharePoint 2013 Management Shell/SharePoint 2010 Management Shell** and select **Run as administrator**. The **Administrator: SharePoint 2016 Management Shell/Administrator: SharePoint 2013 Management Shell/Administrator: SharePoint 2010 Management Shell** command line interface appears.
4. Enter the following command to get the URLs of the site collections where you want to activate the **AvePoint Perimeter Secured Share** feature in each child site and press **Enter**.

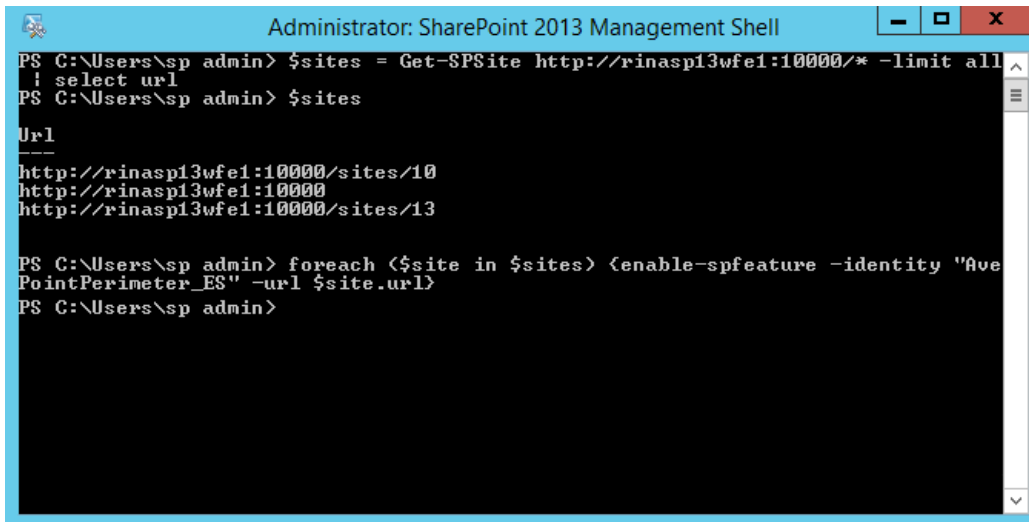
```
$sites = Get-SPSite [https://WebApplicationURL/*] -limit all | select url
```

[https://WebApplicationURL/*] is used to filter the URLs of the desired site collections. In this case, this command is used to get the URLs of all of the site collections within the Web application.

5. Enter `$sites` and press **Enter** to display the URLs that the command in step 4 generates.
6. Enter either of following commands and press **Enter** to activate the **AvePoint Perimeter Secured Share** feature in each site within the site collections whose URLs are displayed in step 5.
 - To activate the **AvePoint Perimeter Secured Share** feature in a SharePoint 2013 or SharePoint 2016 environment, enter `foreach ($site in $sites) {enable-spfeature -identity "AvePointPerimeter_ES" -url $site.url}` and press **Enter**.

- To activate the **AvePoint Perimeter Secured Share** feature in a SharePoint 2010 environment, enter `foreach ($site in $sites) {enable-spfeature -identity "AvePointPerimeter2010_ES2010" -url $site.url}` and press **Enter**.

After the command is executed successfully, the **AvePoint Perimeter Secured Share** feature are activated in each site within the site collections gotten by the command in step 4.



```
Administrator: SharePoint 2013 Management Shell
PS C:\Users\sp admin> $sites = Get-SPSite http://rinasp13wfe1:10000/* -limit all
; select url
PS C:\Users\sp admin> $sites

Url
---
http://rinasp13wfe1:10000/sites/10
http://rinasp13wfe1:10000
http://rinasp13wfe1:10000/sites/13

PS C:\Users\sp admin> foreach ($site in $sites) {enable-spfeature -identity "Ave
PointPerimeter_ES" -url $site.url}
PS C:\Users\sp admin>
```

Figure 4: Activating the AvePoint Perimeter Secured Share Feature using SharePoint Management Shell command lines.

Dashboard Interface

For an overview of the management system in a more intuitive way, navigate to the **Dashboard** to view the charts of the **All Access Logs**, **Internal Users' Last Locations**, **Access Logs Per Platform (Last 7 Days)**, **All Internal Devices**, **External Users' Last Locations**, and **All External Devices**. The **Dashboard** interface is not available for the users who only have the **Secure Share Control** permission level.

Viewing All Access Logs

The **All Access Logs** Graph displays all of the login sessions by day, week or month. The X-axis is the date, week or month. The Y-axis is the number of login sessions by day/week/month. You can click the previous (⏪) button and the next (⏩) button to turn the page to more data of the previous period or the next period.

Viewing Internal Users' Last Locations

The **Users' Last Locations** bar chart displays the distribution of all of the internal users' last locations. The Y-axis is the location name and the X-axis is the user count of the corresponding location.

Viewing Access Logs Per Platform (Last 7 Days)

The **Access Logs Per Platform (Last 7 Days)** bar chart displays the platform distribution of the devices used in the login session in the last 7 days. The X-axis is the platform name and the Y-axis is the session count of the corresponding platform.

Viewing All Internal Devices

The **All Internal Devices** ring chart displays the platform distribution of all of the enrolled internal devices (including internal users' personal devices and work-issued devices). The ring chart consists of parts with different colors. Each color refers to a type of platform. You can also hover your cursor over each part to view the count and percentage of the corresponding platform's enrolled devices, or click on the part to view the detailed information of the corresponding platform's enrolled devices.

Viewing External Users' Last Locations

The **External Users' Last Locations** bar chart displays the distribution of all of the external users' last locations. The Y-axis is the location name and the X-axis is the user count of the corresponding location.

Viewing All External Devices

The **All External Devices** ring chart displays the platform distribution of all of the enrolled external users' devices. The ring chart consists of parts with different colors. Each color refers to a kind of platform. You can also hover your cursor over each part to view the count and percentage of the corresponding platform's enrolled devices, or click on the part to view the detailed information of the corresponding platform's enrolled devices.

Configure Menu

The **Configure** menu in AvePoint Perimeter allows you to customize configurations that affect the entire AvePoint Perimeter platform. Here you can configure the **System Settings**, **Admin Accounts**, **Application Settings**, **Monitor**, **Secured Share**, and **Windows Phone Logs**.

Configuring System Settings

System Settings includes the Agent Monitor, Geolocation Database and License Manager. Refer to sections below to view and manage your Perimeter Agents and licenses.

Using Agent Monitor

To access **Agent Monitor**, navigate to the **Configure** menu, and click **Agent Monitor** under the **System Settings** heading. In **Agent Monitor**, you will see a list of the AvePoint Perimeter Agents that have been registered to the current AvePoint Perimeter Manager Service. You can customize how your Agents are displayed in the following ways:

- **Manage Columns** – Manages which columns are displayed in the list by using the **Manage Columns** drop-down list, so that only the information you want to see will be shown. Click the **Manage Columns**, select the checkboxes next to the column names in the drop-down list, and then click **OK** to have the selected columns shown in the list. The columns available for selecting are:
 - **Agent Name** – The host name of each registered Agent.
 - **Status** – The status of each registered Agent.
 - **Agent Host** – The host name/IP address configured during the Perimeter Agent Installation.
 - **Version** – The AvePoint Perimeter version of each registered Agent.
 - **Farm Name** – The name of the farm where the Agent resides.
 - **Last Registration Time** – The last registration time of the Agent.
- **Filter the column** – Filters which Agents are displayed in the list by Agent **STATUS**. Click the column name **STATUS**, select the checkboxes next to the status values, and click **OK** to have the corresponding Agents shown in the list.
- **Sort the column** (▼) – To sort the Agents, click the column name of the **AGENT NAME**, **FARM NAME**, or **LAST REGISTRATION TIME** column and then select to sort the Agents in ascending or descending order.

Select an Agent by selecting the checkbox next to the Agent Name, and then click the open menu button (▼) to the right of the **AGENT NAME** to select the actions you want to perform or click the corresponding buttons on the ribbon:

- **Configure** – After you select an Agent, this button becomes available. Click **Configure** on the ribbon to access the Configure interface. Here, you can configure the SharePoint Account for the Agent.
 - **SharePoint Account** – The **SharePoint Account** is used by the Perimeter Agent to provide Perimeter with access and control to your SharePoint environment.
 - The default SharePoint account is the Agent account configured during the Agent Installation.
 - To configure a new SharePoint account for the Perimeter Agent, enter the **Username** and **Password** for the desired account into the corresponding text box. The account configured here must have the required permissions for Agent account in the [Permission Requirements for AvePoint Perimeter Agent](#) section of this guide.
- Click **Validation Test** to see whether the values you entered are valid, and then click **Save** to save the configuration.
- **Restart** – Click **Restart** on the ribbon to restart the selected Perimeter Agent. This may be useful in situations where the data transfer rate is sluggish, or if a running job hangs.
 - **Remove** – If an Agent is down, click **Remove** to remove it from this Perimeter management system. The removed Agent will no longer be used by the Perimeter Manager. Note that this does not uninstall the Agent. If you want to re-connect a removed Agent to the Manager, use the **AvePoint Perimeter Agent Configuration** tool.

Configuring Geolocation Database Connection

To access the **Geolocation Database**, navigate to the **Configure** menu, and click **Geolocation Database** under the **System Settings** heading. In **Geolocation Database**, you can configure the Geolocation database connection for your Perimeter Manager.

If you connect your Perimeter Manager to a Geolocation database, you can define location groups based on geographic and political boundary data from the database without relying on data retrieved from external resources like Bing Maps. For more information on configuring location groups based on geographic and political boundaries, refer to [Adding a New Geographic Location Group](#).

To connect your Perimeter Manager to an available Geolocation database, complete the following steps:

1. Configure the settings in the **Database Settings** section:
 - a. **Database Type** – AvePoint Perimeter Manager supports **MS SQL** databases only, so **MS SQL** is the only available **Database Type**.
 - b. **Database Server** – The MS SQL Server name that contains the Geolocation database to which you want to connect.
 - c. **Database Name** – Enter the database name for the Geolocation database to which you want to connect.

2. **Database Credentials** – Select the credentials to access this Geolocation database.
 - **Windows Authentication** (the default option) – Use this method if you want the user's identity to be confirmed by Windows. By default, this account is the current logon account of your Perimeter Manager server cannot be changed. As such, this account must have the **db_owner** database role in the Geolocation database entered above.
 - **SQL Authentication** – SQL Server will confirm the user's identity according to the user's account and password. The account must have the **db_owner** database role in the Geolocation database entered above.
3. Click **Validation Test** to see whether the information you entered are valid and click **Save** to save the configurations, or click **Cancel** to exit this page without saving the configurations.

Configuring IP Location Database

You can configure an IP location database to allow Perimeter to locate the users via IP address for Secure Share content access control. The IP location database includes the IP2Location LITE data. More information is available at <http://www.ip2location.com>.

To access the **IP Location Database**, navigate to the **Configure** menu, and click **IP Location Database** under the **System Settings** heading.

Complete the steps below to configure the IP Location Database settings:

1. Select the **Enable IP location database** option to enable the IP location database settings.
2. In the **Database Settings** section, choose the corresponding mode for creating a new database or using an existing IP location database.

***Note:** The existing IP location database must be a database of SQL Server.
3. Enter the hostname or IP address of the database server into the **Database Server** text box, and enter the database name that you want to create or use into the **Database Name** text box.
4. In the **Database Credentials** section, select the authentication type of your credentials used to access the database, and then click **Validation Test** to test the connection.
5. Click **Create** to create a new IP location database or click **Save** to save the settings for using an existing database.

Using License Manager

To access **License Manager**, navigate to the **Configure** menu, and click **License Manager** under the **System Settings** heading. In **License Manager**, you can view and manage the license information and the licensed users.

***Note:** By default, there is a 30-day built-in trial license in the downloaded package. This license ensures that you can have AvePoint Perimeter up and running right after the Manager and Agent installation completes. The license expires 30 days after the initial Perimeter Manager installation. To obtain an

official license, contact your local AvePoint representative for details. The following users will consume the Perimeter license: the users who use Secure Share feature to share items and the users who enroll their devices.

Viewing License Information

In the **License Manager** interface, you can view the following information:

- **License Type** – Shows whether you have an Enterprise license.
- **License Version** – Shows the version of the license.
- **Total User Quantity** – The number of internal end-users that can be registered into the Perimeter management system using this license. To view the detail information on each registered internal user, go to the **Manage Internal Users** interface. For more information on using the **Manage Internal Users** interface, refer to [Managing Internal Users](#).
- **Expiration Time** – The expiration time of your license.
- **Registered User Quantity** – The number of registered internal end-users within the current Perimeter management system with this license.
- **Remaining User Quantity** – The remaining number of internal end-users that can be registered into the Perimeter management system with this license.
- **Status** – Shows whether your Perimeter license is working.
- **Secured Share** – Shows whether you have purchased the license for the Pro features: the **AvePoint Perimeter Secured Share** feature and the **Virtual Views** feature.

Importing and Exporting License Files

In **License Manager**, you can import a license file to apply a new license as well as export a license file to a local computer.

To import a license file, complete the following steps:

1. Click **Import** on the ribbon. The Import License interface appears.
2. In the Import License interface, click **Browse**.
3. Find and choose the desired LIC file, then click **Open**. Click **Preview** to preview the details of the imported license file.
4. Click **Apply** to apply this license, or click **Cancel** to return to the previous page without applying this license.

To export a license file, click **Export** on the ribbon. Your browser will prompt you to open or save the LIC file. Click **Save** or **Save as** to save it to a designated location.

Configure License Expiration Alert Settings

If you want to send license expiration alerts by e-mail, enable the **Send e-mail reminder** feature in the **Settings** page and configure the alert settings. Follow the instructions below:

1. In the **License Manager** page, click the **Settings** button on the ribbon.
2. In the **Expiration Settings** section, select the **Send e-mail reminder** option to enable the alert.
3. Enter the e-mail addresses into the **Reminder Recipients** box to receive the alert e-mail. Use semicolons (;) to separate the e-mail addresses.
4. In the **Reminder Schedule** field, you can configure when to start sending the e-mail alert. Enter a number into the box to start sending alerts before the specified number of days the license expires.

Managing Licensed Users

If you want to view and manage licensed users, click **Manage Licensed Users** on the ribbon. In the **Manage Licensed Users** page, you can view all of the licensed users and their basic information, search license users, remove inactive licensed users, or assign the license and sharing of inactive licensed users to other users.

- **Remove** – If you want to remove the license from an inactive user, select that user and click **Remove** on the ribbon. You can select multiple inactive users to remove their licenses in bulk. The devices they enrolled will be wiped and all of the secure shares shared by them will be deleted and they will no longer be able to manage the shared items via Perimeter mobile app or Portals.
- **Assign** – If you want to remove licensed users and assign their license and sharing to another user, select those users in the table and click **Assign**. In the **Assign** window, enter a user in the box and check the username. You can only enter one user to inherit the license and sharing. Click **Assign**. The devices of the selected licensed users will be wiped and all of secure shares shared by them will be assigned to the user you entered. The selected licensed users will no longer have access to the shared items through Perimeter mobile app or Portals.

Configuring External User Password Policy

In the **External User Password Policy** page, you can enable the password policy for external users and choose the password policy you want to enforce on the external users' passwords when passwords are being changed or created.

Complete the steps below to configure the external user password policy:

1. To access **External User Password Policy**, navigate to the **Configure** menu, and then click **External User Password Policy** under the **System Settings** heading.
2. In the **External User Password Policy** page, select the **Enable password policy for external users** option to enforce the password policy on external users' passwords.
3. In the **Password Strength** field, select the type of password policy you want to enforce.
 - **Enforce only minimum length and password lifespan** – With this option selected, external users' passwords only need to meet the minimum password length and the expiration settings.
 - **Enforce defined policy AND the minimum length and password lifespan** – With this option selected, the external users' passwords must meet the complexity requirement in addition to the minimum password length and the expiration settings.
4. **Minimum Password Length** – Enter a number between 6 and 14 into the text box to define the minimum character length of external users' passwords
5. **Password Lifespan** – Select the **No end date** option if the external users' passwords are allowed to never expire, or select the **Expire after** option to define when the password will expire after being created or changed.
 - **Expire after** – Enter an integer greater than zero into the text box, and then select **Days**, **Weeks**, **Months**, or **Years** from the drop-down list as the time unit.
6. Click **Save** to save your configuration, or click **Cancel** to exit the **External User Password Policy** page without saving any changes.

Configuring Admin Accounts

The **Admin Accounts** interface allows you to view and manage administrator accounts for AvePoint Perimeter, as well as configure administration groups with custom permission levels. Here, you can give specific users, or groups of users, your desired permission levels of access to AvePoint Perimeter.

It is important to understand how users, groups, and permissions work together in AvePoint Perimeter: users are placed into groups, and groups are then assigned permissions. Only groups are assigned permissions, so you must create at least one group and assign that group permissions. To assign only one user a specific permission level, create a group, place that user in the group, and then assign the group the desired permission level.

Managing Permission Levels

Use Permission Levels to create pre-configured permissions that can be applied to user groups. This way you can quickly and easily apply the same permission configuration to multiple users.

To configure permission levels for AvePoint Perimeter, navigate to the **Configure** menu, and then click **Permission Level** under the **Admin Accounts** heading. In the **Permission Level** interface, the two default permission levels and all previously configured permission levels are displayed.

You can customize how these permission levels are displayed:

- **Manage Columns** – Click **Manage Columns** in the upper-right corner, select the checkboxes next to the column names in the drop-down list, and click **OK** to have the selected columns shown in the list. The columns available for selecting are:
 - **Name** – The name of the permission level.
 - **Description** – The description of the permission level.
- **Sort the column** – To sort permission levels, click the column name of the **NAME** column, and then select to sort the permission levels in ascending or descending order.

To manage your permission levels, you can perform the following actions:

- **Advanced Search** – Click **Advanced Search** to configure the search column name rules and conditions for filtering the permission levels. Click **Add a Rule**, select **Equals** or **Contains** from the **Condition** list, and enter the value. You can add multiple rules and configure the condition between the rules. Use **And** or **Or** to define the rule conditions and click **Validation Test** to test your settings. Click **Search** to filter the permission levels according to your settings. Click **Reset** to clear your settings.
- **Add** – Click **Add** to create a new permission level:
 - i. **Basic Information** – Enter a name for the new permission level and an optional **Description** for future references.
 - ii. **Grant Permission for Different Modules** – Select the modules or functions you want to grant permission to. For modules, such as Dashboard, Manage, Report, Configure, and Job Monitor, select the corresponding checkbox to grant that permission to each function in the corresponding module.

Click **Save** to save the configuration. Click **Cancel** to return to the Permission Level Interface without saving changes.

- **Edit** – To edit a previously configured permission level, select the permission level you wish to edit by selecting the corresponding checkbox, then click **Edit** to navigate to the page to edit this permission level.
 - i. In the **Basic Information** section, you can modify the permission level name and a Description of this permission level.
 - ii. In the **Grant Permission for Different Modules** section, you can select which modules or functions you wish to allow this permission level to access by selecting the corresponding checkboxes.

Click **Save** to save the configuration. Click **Cancel** to return to the Permission Level Interface without saving changes.

- **Delete** – To delete a previously configured permission level, select the permission level you wish to delete by selecting the corresponding checkbox, then click **Delete** on the ribbon. A pop-up window appears to confirm this action. Click **OK** to delete the selected permission level and return to the **Permission Level** interface, or click **Cancel** to return to the **Permission Level** interface without deleting the selected permission level.

Managing Admin Groups

Admin Groups allow you to apply the same permission levels to all users within the same user group. This way, you can change the permission levels of multiple users by editing your user group rather than individually configuring permission levels for each user. You can also change the permission levels for a user by changing which group they belong to.

To access administration group configurations, navigate to the **Configure** menu, and then click **Admin Groups** under the **Admin Accounts** heading. In the Admin Groups configuration interface, you will see a list of previously configured administration user groups. The Administrators group comes pre-configured and users in this group have full control over all modules.

You can customize how these administration groups are displayed in the following ways:

- **Manage Columns** – Manages which columns are displayed in the list so that only the information you want to see will be shown. Click **Manage Columns** in the upper-right corner, select the checkboxes next to the column names in the drop-down list, and click **OK** to have that the selected columns shown in the list. The columns available for selecting are:
 - **Name** – The name of the group.
 - **Description** – The description of the group.
 - **Username** – The names of the users belonging to this group.
- **Sort the column**–To sort the administrator groups, click the column name of the **NAME** column and then select to sort the administrator groups in ascending or descending order.

Adding Admin Groups

To add a new administration group for AvePoint Perimeter, click **Add** on the ribbon and configure the following settings:

1. In the **Group Information** section, enter the group name, permission and an optional description for the group to be created.
 - **Group Name** – Enter a **Group Name** in the provided textbox.

- **Permission** – Assign the permission levels to the group by selecting the previously created permission levels from the **Permission** drop-down list.
 - **Description** – Enter an optional **Description** for the group for future reference.
2. In the **Add Users** section, select users from the drop-down list to add to this group. This assigns the users the permission levels configured above.
 3. Click **Save** on the ribbon to save the configurations, or click **Cancel** to return to the group interface without saving the configurations.

Editing Admin Groups

To edit a group, select the group by selecting the corresponding checkbox, then click **Edit** on the ribbon, or click the open menu button (***) next to the name of the desired group and then click **Edit** in the pop-up menu. You will be brought to the page for editing the group. Here you can change the name, description for this group, as well as the permission levels.

When you have finished making changes to the configurations for this group, click **Save** to save and return to the **Admin Groups** interface, or click **Cancel** to return to the **Admin Groups** interface without saving any changes.

Deleting Admin Groups

To delete administration groups from AvePoint Perimeter, complete the following steps:

1. Select the groups by selecting the corresponding checkboxes, and then click **Delete** on the ribbon. Alternatively, you can select a group, click the open menu button (***) next to the group name, and then click **Delete** in the pop-up menu.
2. A confirmation window will pop up for this deletion. Click **OK** to delete the selected groups, or click **Cancel** to return to the Admin Groups interface without deleting any groups.

Managing Users in Admin Groups

In the **Admin Groups** interface, all of the users belonging to each group are listed in the **Username** column. To manage the users in an administration group, select the group in the **Admin Groups** interface and then you can perform the following actions:

- **Adding Users into Group** – To add users into this group, click **Edit** on the ribbon to enter the page for editing the selected group. Within the group, select the users you want to add into this group from the **Add Users to Group** drop-down list. Click **Save** on the ribbon to save the configurations, or click **Cancel** to return to the group interface without adding any users.
- **Removing Users from Group** – To remove users from this group, click **Edit** on the ribbon to enter the page for editing the selected group. Within the group, find the user you want to remove from this group in the **Add Users to Group** field, and then click the remove button (✖) next to the username. The username will disappear from the **Add**

Users to Group field. Click **Save** to remove the selected user, or click **Cancel** to return to group interface without removing the selected user.

Managing Admin Users

To view and manage administration users for AvePoint Perimeter, navigate to the **Configure** menu, and then click **Admin Users** under the **Admin Accounts** heading. In the **Admin Users** interface, you will see a list of previously added users. You can customize how these users are displayed in the following ways:

- **Manage Columns** – Manages which columns are displayed in the list so that only the information you want to see will be shown. Click **Manage Columns** in the upper-right corner, select the checkboxes next to the column names in the drop-down list, and click **OK** to have the selected columns shown in the list. The columns available for selecting are:
 - **Username** – The name of the user.
 - **Description** – The description of the user.
 - **Status** – The status of the user account.
 - **E-Mail Address** – The e-mail address of the user.
 - **Type** – The type of the user. **Local User** is the only available user type for AvePoint Perimeter's administration users.
 - **Group Name** – The names of the administration groups where the user has been added.
- **Sort the column** – To sort the administrator users, click the column name of **USERNAME** or **E-MAIL ADDRESS** and then select to sort the user in ascending or descending order.
- **Filter the column** – Filter which users are displayed based on the values of the **USERNAME/STATUS/TYPE** column. Click the Open Menu (☰) button next to the column name, select the checkboxes in the drop-down menu, and click **OK** to have the corresponding users shown in the list.

Adding Admin Users

To add an admin user for AvePoint Perimeter, click **Add** in the **Admin Users** interface and then configure the following settings:

- **User Information** – In the **User Information** section, configure the settings below:
 - **User Type** – Choose the type of the user you are adding. You can select to create a **Local System Account** or a **Windows Authentication Account**.
 - **Username** – Enter a name for the user you are adding. If you are adding a Windows Authentication Account as the Perimeter administrator, you can search for and check the username.
 - **E-mail Address** – This field is only for a **Local System Account**. Enter the e-mail address of the user you are adding.

- **Add User to Groups** – Select the groups from the drop-down list to add the user.
- **Description** – Enter an optional **Description** for the user for future reference.
- **Security Information** – Enter the desired password into the **Password** and **Confirm password** text boxes.

Figure 5: The Add page.

When you are finished, click **Save** to add the user and return to the **Admin Users** interface, or click **Cancel** to return to the **Admin Users** interface without saving the configurations for this new user.

Editing Admin Users

To edit an admin user for AvePoint Perimeter, select the user by selecting the corresponding checkbox, then click **Edit** on the ribbon, or click the open menu button (*******) next to the username and then click **Edit** in the pop-up menu. You will be brought to the page for editing the user. Here you can configure the following settings for a user:

- **User Information** – In the User Information section, you can configure the settings below:

- **Username** – Enter the name of the user you are editing.
- **E-mail Address** – Change the e-mail address of the user you are editing.
- **Add User to Groups** – Change the groups that the user belongs to. Select the desired groups from the drop-down list to add the user. The user will have all of the permissions of the selected group, or you can also remove the user from a group by clicking the remove button next to the group name.
- **Description** – Enter an optional **Description** for the user for future reference.
- **Security Information** – Select the **Reset the password** checkbox to change the user's password. Enter the new password in the **Password** field and re-enter the new password in the **Confirm Password** field.

When you are finished, click **Save** to save the changes made and return to the **Admin Users** interface, or click **Cancel** to return to the **Admin Users** interface without saving any changes made.

Deleting Admin Users

To delete previously configured admin users, select the users by selecting the corresponding checkbox, then click **Delete** on the ribbon or click the open menu button (***) next to the username and then click **Delete** in the pop-up menu. A confirmation window will pop up for this deletion. Click **OK** to delete the selected users, or click **Cancel** to return to the **Admin Users** interface without deleting the selected users.

***Note:** The built-in administrator account – **Admin** cannot be deleted.

Deactivating and Activating Admin Users

Refer to the section below to activate or deactivate an admin user.

- **Activate** – To activate the *Inactive* user, select the user by selecting the corresponding checkbox, then click **Active** on the ribbon or click the open menu button (***) next to the username and then click **Active** in the pop-up menu.
- **Deactivate** – To deactivate the *Active* user, select the user by selecting the corresponding checkbox, then click **Deactivate** on the ribbon or click the open menu button (***) next to the username and then click **Deactivate** in the pop-up menu. This makes the status of the user become **Inactive**. The **Inactive** users are not allowed to login Perimeter.

Configuring Secured Share

Secured Share in the **Configure** menu allows you to configure the required settings for sharing files, folders, and libraries in SharePoint via the **AvePoint Perimeter Secured Share** feature in SharePoint or using the **Virtual View** feature in Perimeter. Prior to sharing files, folders, and libraries, you must configure the **System Credentials** for downloading the original files (including the files that are shared

directly and the files within the shared virtual views, folders and libraries) from SharePoint and the **Shared File Location** to store the downloaded copies of the shared files. Optionally, if you want to enable users to open shared files of the **.docx**, **.pptx**, and **.xlsx** formats in browser via Office Web Apps or Office Online at the AvePoint Perimeter Internal and External Portal, edit shared files of these three file formats via Office Web Apps or Office Online and synchronize the modifications to the original SharePoint files at the External Portal, configure the **Office Web Apps Server**.

Configuring System Credentials

In **System Credentials**, you can configure the Web application level system credentials used to download copies of the shared files from specific Web applications. To access **System Credentials**, navigate to the **Configure** menu, and then click **System Credentials** under the **Secured Share** heading.

To configure the system credentials used to download the shared files from a specific scope, complete the following steps:

1. In the **Scope** pane, expand the tree of your desired SharePoint farm to view all of the included Web applications in this farm.
2. To access the page for configuring the system credentials from a specific Web application, click the **Configure** button next to the scope name.
3. In the **Configure System Credentials** page, select an authentication method from the **Authentication Method** list and enter the system credentials you want to use in the **Username** and **Password** text boxes.

***Note:** You must ensure the account designated in the system credentials meets the following conditions:

- This account is not a system account.
 - This account has the **Full Control** permission for all zones in the selected Web application.
 - This account has accessed each site collection where the AvePoint Perimeter Secured Share feature will be used within the selected Web application.
4. Click **Validation Test** to see whether the credentials you entered are valid, and then click **Save** to save the configuration.
 5. After you configure the system credentials for the selected Web application, this Web application's status in the Status column becomes **Configured**.
 - To edit the previously configured system credentials of a specific Web application, click the **Configure** button following the corresponding node
 - To delete the previously configured system credentials of a specific Web application, click **Remove** button following the corresponding node.

Configuring Shared File Location

In **Shared File Location**, you can configure the Universal Naming Convention (UNC) path for the location to store all of the downloaded copies of the shared files and the credentials for accessing the UNC path. These copies of the shared files can be viewed or edited by users in the AvePoint Perimeter External Portal or via the AvePoint Perimeter apps on enrolled mobile devices.

To access **Shared File Location**, navigate to the **Configure** menu, and then click **Shared File Location** under the **Secured Share** heading. To configure the shared file location for this Perimeter management system, complete the following settings:

1. In the **UNC Path** text box, enter the UNC path for the location where you want to store the downloaded copies of shard files. Note that the UNC path should be entered in the following format: `\\admin-PC\c$\data` or `\\admin-PC\ shared` folder.
2. In the **Username** and **Password** text boxes, enter the credentials of the account used to access the UNC path configured above. Note that the entered account must have **Write** permissions to the UNC path configured above.
3. Click **Validation Test** to test the entered information is valid.
4. Choose whether or not to enable the retention settings for deleting the cache of the shared files that have not been accessed within a specific time period. For details on defining the retention settings, refer to [Defining File Cache Retention Settings](#).
5. Click **OK** to save the shared file location or click **Cancel** to exit the current page without saving any configuration.

Defining File Cache Retention Settings

By default, the cache data of the shared files that are not edited, accessed, or downloaded within 30 days will be deleted. Complete the steps below to customize the retention settings for deleting file caches:

1. Go to the `\bin\config` folder under the Perimeter Manager installation path. The default Manager installation path is `...\\AvePoint\\Perimeter\\Manager`.
2. Open the **AppSettings.config** file using **Notepad**.
3. Locate the `<add key="FileCacheCleanUpDays" value="30" />` node, and modify the value of the **FileCacheCleanUpDays** attribute as you desired.

***Note:** Without this node, the retention days will be 30 days by default.

4. Save and close the **AppSettings.config** file.

Configuring Office Web Apps Server Settings

In **Office Web Apps Server Settings**, you can configure an Office Web Apps Server (OWA) for your AvePoint Perimeter Internal Portal and External Portal and the WOPI Host Server used by the OWA to enable end-users to open shared files of the **.docx**, **.pptx**, and **.xlsx** formats in browsers via the corresponding Office Web Apps (including Word Web App, Excel Web App, and PowerPoint Web App) at the Internal and External Portal, edit shared files in Office Web Apps and synchronize the modifications to the original SharePoint files at the External Portal.

To access the **Office Web Apps Server Settings** interface, navigate to the **Configure** menu, and then click **Office Web Apps Server Settings** under the **Secured Share** heading. To configure the Office Web Apps Server (OWA) for your AvePoint Perimeter Internal Portal and External Portal and WOPI Host Server for the OWA, complete the following settings:

1. **OWA Activation** – Select the **Enable Perimeter Portal users to open/edit files with OWA** checkbox to enable the Office Web Apps Server settings for the Internal and External Portal.
2. **OWA Server URL** – To set the URL of the Office Web Apps Server that will be used to communicate with the WOPI Host Server, complete the following steps:
 - a. Select the protocol (**https** or **http**) that will be used by the Office Web Apps Server to communicate with the WOPI Host Server from the drop-drop list before **://**.
 - b. Enter the rest of the desired Office Web Apps Server URL into the text box after **://**.
 - c. Click **Load Zone** to load zones of the designated Office Web Apps Server. The **Select WOPI Zone** field for setting a WOPI zone appears below.
3. **Select WOPI Zone** – Set the WOPI zone of the designated Office Web Apps Server that will be used to communicate with the WOPI Host Server.
4. **WOPI Host Server URL** – Enter the URL of your WOPI Host Server in the format: **hostname:port**. Use the **WOPI Host Server Host** and **Website Port** that you configured during the WOPI Host Server installation as the **hostname** and **port** part in the **WOPI Host Server URL**.
5. Click **Save** to save the Office Web Apps Server settings.
6. To ensure that the configured Office Web Apps Server and WOPI Host Server can be properly used to open **.docx**, **.pptx**, and **.xlsx** in the browser at the AvePoint Perimeter External and Internal Portal, you must ensure that the following SSL certificates are trusted by related servers/computers:
 - The Office Web Apps Server's certificate is trusted by the WOPI Host Server and end-user browsers at the AvePoint Perimeter Internal Portal and External Portal.
 - o AvePoint recommends using a valid certificate issued by a commercial certification authority for the Office Web Apps Server so the certificate can be automatically trusted by end-user browsers and the WOPI Host Server.
 - o If the Office Web Apps Server does not have a valid certificate issued by a commercial certification authority, you must manually import its certificate into

the **Trusted Root Certification Authorities** certificate store of the WOPI Host Server and end-users' computers.

- The WOPI Host Server's certificate is trusted by the Office Web Apps Server. To achieve this, manually import the WOPI Host Server's certificate into the **Trusted Root Certification Authorities** certificate store of the Office Web Apps Server.

Configuring Secure Share Control Policy

In **Secure Share Control Policy**, you can control the Perimeter license consumption for who can use the Perimeter secure share feature, define the users or groups who can secure share items and the permission levels they can grant, restrict the domains where the recipients of external secure share can belong, and control the files or folders that can be secure shared by defining the document attribute based rules.

To access **Secure Share Control Policy**, navigate to the **Configure** menu, and then click **Secure Share Control Policy** under the **Secured Share** heading.

License Consumption Restriction

To control the license consumption for who can use the Perimeter secure share feature, complete the settings below:

1. Navigate to **Configure > Secure Share Control Policy > License Consumption Restrictions**.
2. In the **License Consumption Restrictions** section, choose to allow all users to use Perimeter secure share or only the users imported from Active Directory. If you choose the **Only users imported from Active Directory** option, continue with the following steps. If you choose the **All users** option, proceed to step 4.
3. In the **Domain Information** section, complete the following settings:
 - **Domain Controller Address** – Enter the domain controller address where you want to import the Active Directory users.
 - **Username** and **Password** – Enter the username and password of the Active Directory account you want to use to synchronize the AD users. Make sure that the account has at least read permission in your organization directory.
 - **Domain Scope** – Select the **Import users from all domains in the same forest and the trusted domains** option or select the **Configure the search roots list myself** option to configure which users will be synchronized by LDAP Distinguished Names (DN).
4. In the **Schedule Settings** section, choose to run the synchronization immediately, or configure a schedule to synchronize the active directory users. If you choose to configure a schedule, complete the following settings:
 - **Schedule Type** – Choose to run the synchronization job **By hour**, **By day**, **By week**, or **By month**.

- **Interval** – Enter a number into the text box of **Every _ hours/days/weeks/months** to define the frequency for running the scheduled synchronization jobs.
 - **Start Time** – Select the start time from the drop-down list to run the synchronization job. If you select **By month** as the **Schedule Type**, configure the **Specify the start time by date** settings or the **Specify the start time by day of the week** settings. For more information, see the [Configuring Advanced Start Time Settings](#) section.
5. Click **Save** to save the license consumption settings. Click **Cancel** to exit this interface without saving the configurations.

User and Group Restriction

You can add rules to **User and Group Restriction** to control the internal users and groups who can use Secure Share to share SharePoint items. If you add rules in the **User and Group Restriction** tab, only the internal users and groups who meet the rule conditions can secure share SharePoint items and grant others with the prescribed permission levels.

If there are no rules configured in the **User and Group Restriction** tab for restricting who can secure share SharePoint items, all of the internal users and groups can share items. When performing Secure Share, they can either grant any of the permission levels to the shared with users or grant limited permission levels according to their own permissions in the SharePoint site. For details on granting SharePoint permissions to define the permission levels that a user can grant, refer to [Allowing SharePoint Permissions to Decide the Available Permission Levels](#).

Complete the steps below to configure rules for User and Group Restriction:

1. Navigate to **Configure > Secure Share Control Policy > User and Group Restriction**.
2. Click **Add a Rule** under the table to add a rule record.
3. Select a rule category from the drop-down list under the **Rule** column, select the rule condition for this rule category, and then enter the value in order to locate certain users or groups. For detailed explanations on rule categories and conditions, refer to [Examples of User and Group Restriction Rules](#).
4. In the **Share Type** column, select the maximum permission level that the users or groups can grant in the secure share.
5. Repeat the steps from step 2 to step 4 to add additional rules.
6. Click **Save** to save your configurations for user and group restrictions, or click **Cancel** to exit the Secure Share Control Policy page.

Examples of User and Group Restriction Rules

Refer to the table below for examples of configuring user and group restrictions rules:

Rule Category	Rule Condition	Value	Share Type	Description
Active Directory User/Group	Equals	IT_Team_All	Delete	The active directory group “IT_Team_All” can grant the Edit, Download, Read, or Delete permission in secure share.
SharePoint Group	Equals	Site_Visitor	Read	The SharePoint group “Site_Visitor” can only grant the Read permission in secure share.
	Contains	Owner	Edit	The SharePoint group that has a group name containing owner can grant the Edit, Download, or Read permission in secure share.
	Begins With	Site	Download	The SharePoint group that has a group name which begins with site can grant the Download or Read permission in secure share.
All Users	N/A	N/A	Download	All of the users in secure share can grant Download or Read permission.

Domain Restrictions

You can configure the Secure Share domain restrictions to define the allowed domains or blocked domains for the users that the files, folders, or libraries can be shared with. The users in the blocked domain list cannot have SharePoint files, folders, or libraries shared with them, and they cannot register to the Perimeter External Portal.

To restrict the domains where the recipients of external secure shares can belong, complete the settings below:

1. In the **Type** field, select **White List** or **Black List** to define the allowed domains or the blocked domains. If you configure a white list, only the users from the domains in this list can have SharePoint items shared with them via the Perimeter Secure Share feature. If you configure a

black list, the users from the domains in this list cannot have SharePoint items secure shared with them via the Perimeter Secure Share feature.

2. Enter a domain into the **Allowed Domain** text box or **Blocked Domain** text box in the format of **example.com**, and then click **Add**.
3. That domain will be added to the **Allowed Domain** lists or **Blocked Domain** list. To remove a domain from the list, select that domain, and then click **Remove**.
4. Click **Save** to save the domain restriction settings, or click **Cancel** to exit the Secure Share Control Policy page.

Document Attribute Based Restriction

You can control SharePoint files or folders that can be shared via the Secure Share feature according to document attribute based rules. To add and configure a document attribute based rule, complete the steps below:

1. In the **Default Document Policy** section, select the default action from the drop-down list. If the default action is **Allow**, the action of the rules configured in the **Document Policy Exception** table will be **Block**. If the default action is **Block**, the action for the exception rules will be **Allow**.
2. Click **Add a Rule** under the **Document Policy Exception** table to add an exception rule record.
3. Enter a file or folder attribute name into the text box under the **Attribute** column, select **Equals** or **Does Not Equal** as the condition type, and then enter the value.
4. You can click **Add a Rule** to add multiple exception rules into the table one by one.
5. Click **Save** to save your configurations, or click **Cancel** to exit the Secure Share Control Policy page.

Enabling SharePoint Permissions to Grant the Available Permission Levels

By default, when sharing files, folders, or a library via Secure Share feature in SharePoint, internal users can grant any of the permission levels to the shared with users even though internal users do not have permissions equivalent to the granted permission level. To avoid this security risk, you can use SharePoint permissions to control the permission levels that are allowed to be granted by users using Secure Share.

Refer to the instructions below to enable this permission control:

1. Go to the `\bin\config` folder under the Perimeter Manager installation path. The default Manager installation path is `... \AvePoint\Perimeter\Manager`.
2. Open the **AppSettings.config** file using **Notepad**.
3. Locate the **<appSettings>** node, set the value of the **SharePermissionBaseOnSP** attribute to **true**.
4. Save and close the **AppSettings.config** file.

The following are the permission control conditions:

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

Configuring Watermark Settings

In **Watermark Settings**, you can configure watermark settings at Web application level to protect the shared files with watermark. The shared files in the Web application that have watermark settings configured will be viewed or downloaded with the watermark applied.

To access **Watermark Settings**, navigate to the **Configure** menu, and then click **Watermark Settings** under the **Secured Share** heading. To configure the Watermark Settings for the Perimeter management system, complete the following settings:

1. Click the farm name displayed in the **SCOPE** column to expand the farm tree. All of the Web applications in the current farm are displayed.
2. Select the checkboxes ahead of the Web applications that you want to configure watermark settings for, and then click **Configure** above the column header, or click **Configure** under the **ACTION** column to configure watermark settings for each Web application separately.
3. In the **Configure** interface, select the **Enable watermark** option under the **Watermark** section, and then complete the following settings to configure the watermark settings:
 - **Text** – Select the **Current User Account** option from the drop-down list to display the username of the account that 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** to save the watermark settings and exit the interface. Click **Cancel** to exit the interface without saving the changes.

Configuring Content Access Control for Secure Share

You can enable the Content Access Control for Secure Share and configure the location or IP address rules to allow or deny the access of shared content through Perimeter Portals or mobile devices by the internal/external users that are from the designated location or location group or whose IP addresses lie in the designated range.

To access **Content Access Control**, navigate to the **Configure** menu, and then click **Content Access Control** under the **Secured Share** heading. Complete the steps below to enable and configure the Content Access Control for Secure Share:

1. In the **Content Access Control for Secure Share** field, select the **Enable content access control for secure share** option. The **Rule Settings for Content Access Control** field will be available.
2. Click **Add a Rule** to add a rule record into the table.
3. **Control Type** – Select **Location** or **IP Address** from the drop-down list.

***Note:** To use the **Location** control type, you are recommended to use an **IP Location Database** to locate the users via IP address, in addition to the locations that Perimeter are allowed to obtain. For details, refer to [Configuring IP Location Database](#).

- **Location** – Use the user-defined location or location groups or the geographic locations to locate the users. With **User-defined** selected, you can select a user-defined location or location group to control the access of users from there, or you can select **Any**, **Undefined**, or **Unavailable** to refer to the users from any location or undefined location, or whose location is unavailable.

With the location rules configured, the internal or external users must provide location information before they access the shared files in AvePoint Perimeter External Portal. By default, they can scan the QR code using Perimeter mobile app, or use the browser to provide location.

- o If your organization asks users to provide their location through the Perimeter mobile app without the browser as an alternative, refer to [Providing Location Information via Mobile App Only](#) for detailed configurations.
- o If your organization wants to apply 2-factor authentication requiring the QR code and access password for accessing shared files, refer to [Applying 2-Factor Authentication for Accessing Shared Files](#) to enable the 2-factor authentication.
- **IP Address** – Use the IP address to locate the users. You can select **Any IP Address**, **Specified IP Address**, or **IP Address Range** to locate all of the users with IP addresses, or locate the users with specific IP address, or whose IP address lies in the designated range.

4. **User Type** – Select **Internal User** or **External User** from the drop-down list to designate which type of users you want to control content access for.
5. **Action** – Select **Allow** or **Deny** from the drop-down list to allow or deny the users' access to the shared content.
6. **Description** – Add an optional description for this rule.
7. Repeat the steps from step 2 to step 6 to add multiple rules, and you can change the priority of the rules by selecting the number from the **Priority** list. If there are conflicting rules, the rules with higher priority will take effect.
8. Click **Save** to save the Content Access Control settings, or click **Cancel** to exit the interface without saving any changes.

Providing Location Information via Mobile App Only

If your organization asks all of the users to provide their location through the mobile app, complete the steps below:

1. Go to the `\bin\config` folder under the Perimeter External Portal and Gateway installation path. The default installation path is `... \AvePoint\Perimeter\GatewayPortal`.
2. Open the **AppSettings.config** file using **Notepad**.
3. Locate the `<appSettings>` node, set the value of the **IsOnlyAppLocation** attribute to **true**.
4. Save and close the **AppSettings.config** file.

Applying 2-Factor Authentication for Accessing Shared Files

If your organization wants to apply 2-factor authentication for accessing the secure shared files in Perimeter External Portal, complete the steps below:

1. Go to the `\bin\config` folder under the Perimeter External Portal and Gateway installation path. The default installation path is `... \AvePoint\Perimeter\GatewayPortal`.
2. Open the **AppSettings.config** file using **Notepad**.
3. Locate the `<appSettings>` node, set the value of the **IsTwoFactorEnableForPortal** attribute to **true**.
4. Save and close the **AppSettings.config** file.

Configuring Secure Share Options and Customizations

In the **Secure Share Options and Customizations** page, you can configure the following settings for the Secure Share.

The screenshot shows the 'AvePoint Perimeter' configuration interface. At the top is a navigation bar with links: Home, Dashboard, Manage, Report, **Configure**, and Job Monitor. Below the navigation bar is a breadcrumb trail: 'Configure > Secure Share Options and Customizations'. The main content area has a 'Save' button (with a floppy disk icon) and a 'Cancel' button (with a red X icon). The settings are organized into three sections: 1. 'Expiration Settings' (shaded header): Contains 'Default Expiration Time: Expire after 7 days' (with a text box containing '7'), 'Set Up Expiration Time: ☒ Required', and 'Maximum Expiration Time: Expiration time cannot exceed 14 days' (with a text box containing '14'). 2. 'Metadata Setting' (shaded header): Contains 'Metadata Information: ☒ Display metadata information on the Perimeter Portals'. 3. 'Permission Level Settings' (shaded header): Contains 'Delete Permission: ☒ Allow to grant the Delete permission in Secure Share'.

Figure 6: The Secure Share Options and Customizations page.

- **Expiration Settings** – Choose whether or not to require the **Expiration Time** field to be provided when performing a Secure Share on the **Secure Share** window in SharePoint. You can configure a time duration in the **Default Expiration Time** field, so that the expiration time will be automatically populated for each sharing event with a default expiration time. Additionally, you can also set up a **Maximum Expiration Time** to ensure that the expiration times that internal users can select do not exceed the limit.
***Note:** If you do not want to set up a default expiration time, enter **0** into the text box. The **Expiration Time** field in the **Secure Share** window will display blank, which represents that the secure share will not expire.
- **Metadata Setting** – Select whether or not to display the metadata information of the shared items on the Perimeter Portals and mobile apps. When using the Secure Share feature, the internal users can select a list view to share the SharePoint properties of the shared items. If the **Display metadata information on the Perimeter Portals** option is deselected, the SharePoint properties will not be displayed.

- **Permission Level Settings** – Select whether or not to allow the internal users to grant the **Delete** permission when performing a Secure Share on the **Secure Share** window in SharePoint.

Sending Secured Share Notification E-mail as the Shared by User

By default, the **AvePoint Perimeter Secured Share Notification** e-mail sent to the internal or external users with whom the files, folders, or library is shared displays the **AvePointPerimeter.Notifications** (**perimeter.notification@avepoint.com**) in the **From** field.

You can configure the **AppSettings.config** file to display the user who shared the files, folders, or library with the others as where the e-mail is from. Complete the steps below:

1. Go to the `\bin\config` folder under the Perimeter Manager installation path. The default Manager installation path is `...\AvePoint\Perimeter\Manager`.
2. Open the **AppSettings.config** file using **Notepad**.
3. Locate the `<appSettings>` node, set the value of the **IsEmailsenderisshareby** attribute to **true**.
4. Save and close the **AppSettings.config** file.

Enabling Update Notification

By default, users that have files shared with them will not be notified when the shared files are updated. With the update notification enabled, the shared with users will receive an e-mail notification if the shared by users or site collection administrators choose to notify them when shared files are updated. Additionally, you can configure a time range within which AvePoint Perimeter will only send out one update notification, regardless of how many times the files have been updated. To enable the update notification and configure a time range, complete the steps below:

1. Go to the `...\AvePoint\Perimeter\Manager\bin\config` folder on the Perimeter Manager server.
2. Open the **AppSettings.config** file using **Notepad**.
3. Locate the `<appSettings>` node, set the value of the **dynamicUpdateEmailNotification** attribute to **true**.
4. Find or add the **FileUpdateHolderSendTime** attribute, and set the value. The time unit of this attribute value is **Minute**. If this attribute is not configured, the time range will be 60 minutes by default. According to the default time range, after an update notification is sent out for a file that is being updated, users will not be notified of any updates of the same file made by the same user within the next 60 minutes.
5. Save the changes and close the file.

Customizing the Threshold for Sending Reminder E-mail Notifications for Locked Shared Files on the External Portal

By default, if a shared file has been locked for editing for more than **5** days on the AvePoint Perimeter External Portal, the Perimeter system will automatically send a reminder e-mail notification whose subject is **Action Needed: Files Locked for Editing** to the user who locked the file to remind the user to edit this file, with the user who shared this file CC'ed. To customize the threshold for sending this reminder e-mail notification in days, complete the following steps:

***Note:** For more information on customizing the template for the **Action Needed: Files Locked for Editing** e-mail notification, refer to [Customizing E-mail Templates](#).

1. Go to the `\bin\config` folder under the Perimeter Manager installation path. The default Manager installation path is `...\AvePoint\Perimeter\Manager`.
2. Open the **AppSettings.config** file using **Notepad**.
3. Within the `<appSettings>` node, set the value of the **fileLockNotificationIntervalDaysCount** attribute to an integer between **1** and **32** as the new threshold for sending the **Action Needed: Files Locked for Editing** e-mail notifications for locked shared files.

***Note:** The default value is **5**.

4. Save the changes and close the file.
5. Restart the **AvePoint Perimeter Timer Service** on the Perimeter Manager server manually to make this change take effect.

Allowing Users that are not Shared With to Sign Up to the External Portal

By default, if an external user does not have any items shared with them, the external user cannot sign up to the External Portal. If your organization wants to allow these external users to sign up to the External Portal and let them submit access requests through the secure share links of the shared items, you must edit a configuration file to enable this function.

Complete the steps below to enable this function:

1. Go to the `bin\Config` folder under the Perimeter External Portal and Gateway installation path. The default External Portal and Gateway installation path is `...\AvePoint\Perimeter\Gateway\bin\Config`.
2. Find the **AppSettings.config** file and open it with Notepad.
3. Set the value of the **allowRegisterWithoutDocuments** attribute to **true**.
4. Save your changes and close this file.

Defining the Default Expiration Duration for Secure Share via CONFIG File

With a default expiration duration defined, the expiration time will be automatically populated in the **Secure Share** window when internal users use the **Secure Share** feature to share files, folders, or libraries in SharePoint. Internal users can still customize the expiration time in the **Secure Share** window.

***Note:** If the **Secure Share Options and Customizations** has been configured, this setting in the **AppSettings.config** file will not work.

To define a default expiration duration for Secure Share via CONFIG file, complete the steps below:

1. Go to the `\bin\config` folder under the External Portal and Gateway installation path and the Manager installation path. The default installation path of External Portal and Gateway is ... `\AvePoint\Perimeter\GatewayPortal`; the default installation path of Manager is ... `\AvePoint\Perimeter\Manager`.
2. Open the **AppSettings.config** file using Notepad.
3. Find the **DefaultExpirationDays** attribute and set a value for this attribute. The time unit is **Days** and the valid value must be an integer greater than **0**.
4. Save the changes and close the file.

Disabling Internal Users to Share Anonymous Access or Passcode-Verified Access

By default, AvePoint Perimeter Secure Share feature provides all of the following secure share types:

- Require registration and verify the shared permission
- Accessible to anyone through links
- Verify viewers via passcode

If you do not want to allow anonymous access (**Accessible to anyone through links**) or passcode-verified access (**Verify viewers via passcode**) to be shared by internal users via Secure Share in SharePoint, you can configure the settings in the **AppSettings.config** file. Refer to the instructions below:

1. Go to the ... `\AvePoint\Perimeter\Manager\bin\config` directory on the server where the AvePoint Perimeter Manager is installed.
2. Open the **AppSettings.config** file with Notepad. Complete the steps below:
 - If you want to disable internal users to share the anonymous access, find the **AllowAnonymousShare** attribute and set the value to **false**.
 - If you want to disable internal users to share the passcode-verified access, find the **AllowAccessCodeShare** attribute and set the value to **false**.
3. Save the changes and close this file.

Defining the Minimum Interval for Sending a One-Time Access Passcode

If the secure share requests a passcode verification, the external users who access the shared link must provide their e-mail address to receive a passcode and then provide the passcode to Perimeter External Portal within 30 minutes for verification. By default, the minimum interval for sending another passcode is 60 seconds, which means the external users must wait at least 60 seconds to send out another passcode.

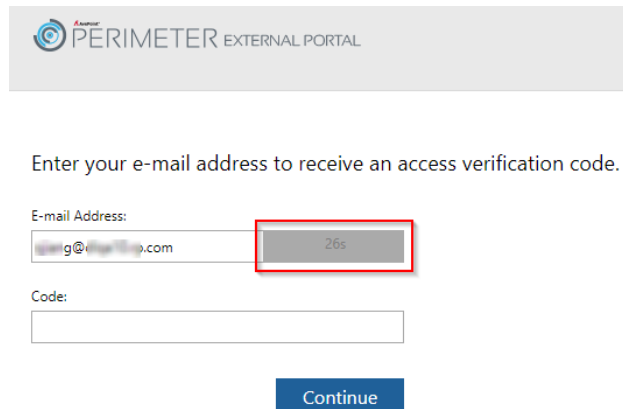


Figure 7: The minimum interval for sending another passcode.

If you want to change the minimum interval, complete the steps below:

1. Go to the `\bin\config` folder under the External Portal and Gateway installation path. The default installation path is `...\AvePoint\Perimeter\GatewayPortal`.
2. Open the **AppSettings.config** file using **Notepad**.
3. Add the `<add key="AccessCodeResentTime" value="60" />` node into the `<appsettings></appsettings>` node.
4. You can change the number for the **value** attribute. The unit of time is **Second**.
5. Save your configurations and close this file.

Deleting Shared Items Permanently

By default, the items deleted by users who are granted **Delete** permission via Secure Share of AvePoint Perimeter 1 SP9 CU1 or later will be moved to the recycle bin. If you want to permanently delete the shared items when the users delete them, you can configure the settings in **AppSettings.config** file. Complete the steps below:

1. Go to the `\bin\config` folder under the External Portal and Gateway installation path. The default installation path is `...\AvePoint\Perimeter\GatewayPortal`.

2. Open the **AppSettings.config** file using Notepad.
3. Find the **IsCompleteDeletion** attribute and set the value to **true**.
4. Save your changes and close this file.

Configuring Application Settings

Application Settings in the **Configure** menu allows you to customize configurations for default device enrollment settings and notification settings for AvePoint Perimeter.

Additionally, you can configure the **appsettings.config** file to configure the account lockout policy for the login behavior of the Perimeter Management Console and Portals. By default, the user account will be locked out for 5 minutes after five failed login attempts within 5 minutes. For details refer to [Configuring Account Lockout Policy](#).

Configuring General Settings

In **General Settings**, configure the general settings for device enrollment and portal connections, including the default device enrollment settings, URLs of the AvePoint Perimeter External Portal and AvePoint Perimeter Internal Portal, and organization contact information.

To access **General Settings**, navigate to the **Configure** menu, and then click **General Settings** under the **Application Settings** heading.

Follow the steps below to configure the general settings.

1. **Device Services URL** – Enter the URL of the Gateway of this AvePoint Perimeter management system. This URL will be included in the enrollment request e-mails to the device owners. The device owners will open this URL to download and install the AvePoint Perimeter mobile apps. You can check whether the enter URL is available by clicking the **Test** button.
2. **Default Authentication Mode** – Choose the default authentication method for this Perimeter Manager server. This is the method that will be used during the mobile device enrollment process.
 - **Directory Credentials for Organization** –Users must provide their organization usernames and passwords of their organization directory accounts during the mobile device enrollment process.
 - **One-Time Enrollment Code** – Users must provide their organization usernames and the One-Time Enrollment Codes provided in the enrollment requests during the mobile device enrollment process.
 - **Both (2- Factor Authentication with Directory Credentials & a One-Time Enrollment Code)** – Users must provide both their organization credentials (usernames and passwords) and the One-Time Enrollment Codes provided in the enrollment requests during the mobile device enrollment process.

3. **Upload Device Usage Policy** – Upload a predefined device usage policy HTML file customized by your company. This will help to ensure the security, safety and privacy of your employees' usage of the enrolled devices.
4. **Authentication Type** – Select the default authentication types for signing into the Perimeter Management Console, Internal Portal, and External Portal.
 - With **Windows Authentication** type selected, internal users can directly sign into the Internal Portal or External Portal using their Windows accounts. If you select the **Windows Authentication** as the **External Portal Default Authentication Type**, the external users must manually change the authentication type to **Form Based Authentication** and provide the username and password when signing into the External Portal.
 - If you want to allow the users from your trusted business partners to use their own organization credentials to log into Perimeter, you can select the **ADFS Authentication** type. To configure the ADFS Authentication, refer to [Configuring ADFS Authentication](#).
5. **Internal Portal URL** – Enter the base URL of the AvePoint Perimeter Internal Portal of this AvePoint Perimeter management system. You can check whether the enter URL is available by clicking the **Test** button.
6. **External Portal URL** – Enter the base URL of the AvePoint Perimeter External Portal of this AvePoint Perimeter management system. You can check whether the enter URL is available by clicking the **Test** button.
7. **Default Domain** –To enable the internal users to omit domain name while entering Active Directory usernames in the login pages of the AvePoint Perimeter Internal Portal and External Portal, enter a default domain name into this field. With the default domain name configured, internal users can enter **username** instead of **domainname/username** to log into the portals.
8. **Contact Information** – Enter the system administrator's **E-mail Address** and **Phone Number**. This information will be listed in every enrollment request e-mail. If the device owners have any questions about enrolling the devices, they can contact the system administrator for help.
9. Click **Save** to save your configurations, or click **Cancel** to cancel the configurations and exit the **General Settings** interface.

Disabling the Enroll New Device Feature on the AvePoint Perimeter External Portal

By default, users (including internal and external users) of the AvePoint Perimeter External Portal can submit an enrollment request by clicking the **Enroll New Device** link on the External Portal. (For detailed information on the **Enroll New Device** feature, refer to the [AvePoint Perimeter Pro Secured Share User Guide](#)). Then, the Perimeter Manager will send an enrollment request e-mail to this user. The user can enroll a mobile device into the Perimeter management system using the received enrollment request e-mail without requesting the enrollment request e-mail from a Perimeter administrator. The authentication mode used by the enrollment request will be either of the following:

- If sent to an internal user, the authentication mode is **Both (2- Factor Authentication with Directory Credentials & a One-Time Enrollment Code)**.

- If sent to an external user, the authentication mode is **One-Time Enrollment Code**.

If you want all of the external users and/or internal users to only be able to enroll their mobile devices via the enrollment requests sent by the Perimeter administrators, complete the following settings to disable the **Enroll New Device** feature at the AvePoint Perimeter External Portal:

5. Go to the `\bin\config` folder under the External Portal and Gateway installation path. The default installation path is `...\AvePoint\Perimeter\GatewayPortal`.
6. Open the **AppSettings.config** file using **Notepad**.
7. Configure the values of the following attributes:
 - **internalUserSelfEnrollEnabled** – To disable the **Enroll New Device** feature for internal users on the External Portal, set the value of this attribute to **false**.
 - **externalUserSelfEnrollEnabled** – To disable the **Enroll New Device** feature for external users on the External Portal, set the value of this attribute to **false**.

***Note:** The default values of the **internalUserSelfEnrollEnabled** and **externalUserSelfEnrollEnabled** attributes are both **true**, which means that the **Enroll New Device** feature is enabled for both the internal and external users on the External Portal.

8. Save the changes and close the file.

Configuring Notification Settings

Configure settings, including SMTP server information and notification parameters, for sending notifications via e-mail.

Configuring Outgoing E-mail Settings

The outgoing e-mail server must be configured before AvePoint Perimeter can send out e-mail notifications. To configure the Outgoing e-mail server, complete the following steps:

1. **Outgoing e-mail server (SMTP)** – Enter the address of the outgoing e-mail server.
2. **SSL authentication** – Configure this option according to your e-mail settings on the SMTP server.
3. **E-mail (SMTP) Port** – Enter the SMTP port. The default SMTP port is 25. For SSL authentication, the default port is 587.
4. **SMTP Server Username** – Enter the sender's username on the SMTP server
5. **Allow Anonymous** – Select whether or not the SMTP server you want to use is allowed to be accessed anonymously. If anonymous access is allowed, the **SMTP Server Password** is not required.
6. **Sender E-mail Address** – Enter the e-mail address for all Perimeter e-mails to be sent from.
7. **SMTP Server Password** – Enter the sender's password to log onto the SMTP server.
8. Click **Save** to save your configurations, or click **Cancel** to cancel the configurations.

9. After the outgoing e-mail settings are successfully configured, Perimeter will automatically send a confirmation e-mail to the configured **Sender E-mail Address**.

Configuring Notification E-mail Settings

In the **Notification E-Mail Settings** interface, perform the following steps to configure e-mail notification settings:

1. Select the **Notification Conditions** when the e-mail notifications will be sent.
 - If you select **Violation**, Perimeter will send e-mail notifications to inform recipients that SharePoint blocked access according to the Content Access Control rules.
 - If you select **Warning**, Perimeter will send e-mail notifications to inform recipients of access attempts that resulted in a warning according to the Content Access Control rules.

With at least one of the notification conditions selected, you need configure the settings in steps 2-3.
2. **Recipients** – Enter the e-mail addresses of the notification recipients.
3. **When to Send Notifications** – In the **When to Send Notifications** area, choose one of the following options:
 - **Send notifications immediately** – With this option selected, the e-mail notifications will be sent immediately when access to SharePoint is blocked or users are warned according the Content Access Control rules.
 - **Configure a schedule** – With this option selected, you can configure the schedule for sending the e-mail notifications as follows:
 - **Schedule Type** – Select the interval at which the **Send access warnings report e-mail & Send access violations report e-mail** timer job occurs: **By hour**, **By day**, **By week**, or **By month**.
 - **Interval** – Set up the frequency for the schedule by entering an integer in the text box.
 - **Start Time** – Specify the time of the day that Perimeter will check for blocked/warned access attempts. If you select **By month**, configure the **Specify the start time by day of the week** and **Specify the start time by date** fields. For more information, see the [Configuring Advanced Start Time Settings](#) section below.
4. Click **Save** to save your configurations, or click **Cancel** to cancel the configurations.

Configuring Advanced Start Time Settings

If you select **By month** when configuring a schedule, the following advanced start time settings are available:

- **Specify a start time by date** – If you select **Specify a start time by date**, configure the start time as below:
 - o ... : ... **on the ...**– Specify the time of one specific date of the month. For example, if you select **1AM:00 on the 2nd**, Perimeter will start the job at 1 o'clock AM on the 2nd day of the month.
- **Specify the start time by day of the week** – If you select **Specify the start time by day of the week**, configure the start time as below:
 - o ... : ... **on the ...**– Specify the time of one specific day of a specific week. For example, if you select **1AM:00 on the first Friday**, Perimeter will start the job at 1 o'clock AM on the first Friday of the month.

Configuring ADFS Authentication

If you want to allow the users beyond your organizational boundaries to use their own organizational credentials to access Perimeter, you can enable and configure the ADFS Authentication in the Perimeter Management Console.

To enable and configure the ADFS Authentication settings, complete the following:

1. Navigate to **Configure > Application Settings > ADFS Authentication**.
2. In the **ADFS Information** section, select the **Enable ADFS Authentication** option in the **ADFS Authentication** field to enable the ADFS Authentication.
3. Provide the following information in the **ADFS Information** section.
 - **Relying Party Identifier** – Enter the identifier of the Replying Party Trust.
 - **Federation Metadata Trust** – Enter the URL path of the Federation Metadata Trust.
4. In the **Token-decrypting Certificate** section, click **Select Certificate** to browse the token-decrypting certificate.
5. If you want to add ADFS users to the Perimeter Management Console, add the claims and you can also set up the claim priority. Complete the steps below:
 - a. click the **Add a Rule** link in the **Claim Configuration** section. A rule record will be added to the table.
 - b. In the **Auto** field, the **ManualInput** option and the **Select** option are provided in the list. If you want to display all of the available claim types in the **Claim Type** list and select one from the list, select the **Select** option; If you want to manually enter the claim type in the **Claim Type** box, select **ManualInput**.
 - c. If you selected a claim type from the list, the claim name will be automatically populated into the **Claim Type** box; if you entered a claim type, enter the claim name into the **Claim Type** box.

- d. To add another rule, repeat steps a to c.
6. Click **Save** to save the ADFS Authentication settings and exit this page; Click **Cancel** to exit this page without saving any changes.

Configuring Account Lockout Policy

To customize the account lockout policy in the configuration file, complete the steps below:

1. Go to the `\bin\config` folder under the External Portal and Gateway installation path and the Manager installation path. The default installation path of External Portal and Gateway is ...`\AvePoint\Perimeter\GatewayPortal`; the default installation path of Manager is ...`\AvePoint\Perimeter\Manager`.
2. Open the **AppSettings.config** file using Notepad.
3. Find or add the following nodes under the `<appsettings></appsettings>` node.
 - `<add key="MaxLoginLockTrial" value="5"/>` – Edit the number for the **value** attribute. After the configured number of failed login attempts, the user will be locked out.
 - `<add key="LoginLockDuration" value="5"/>` – Edit the number for the **value** attribute to specify the time duration of the account being locked. The unit of time is **Minute**.
 - `<add key="LoginAttemptTimeRange" value="5"/>` – Edit the number for the **value** attribute. The account will be locked if the failed login attempts within the specified time range reached the value configured for the **MaxLoginLockTrial** attribute. The unit of time is **Minute**.
4. Save your configurations and close the file.

Log Manager

Use the **Log Manager** to manage and collect logs that are generated by Perimeter Manager and Agents. In the **Log Manager**, you can configure the log level and settings for the log files for each Manager service and Agent.

To access **Log Manager** for Perimeter, navigate to the **Configure** menu, click **Log Manager**.

Configuring Log Settings

To configure the log settings in the **Log Manager** interface, complete the following steps:

1. Click **Log Settings** on the ribbon. You can configure the log settings for the Manager or Agent services by clicking the Manager Service or Agent tab.
2. In either tab, you will see the name of the service. To configure settings for logs, select the desired services and configure the following options:

- **Service Host** – The server where the service resides.
- **Log Level** – Logs could be configured to generate on each of the following levels.
 - **Information** – Logs of this level record the basic information of Perimeter, such as the jobs that you have run, the operations you have performed and important processes of jobs. Information level logs also contain all of the logs from **Warning** and **Error** levels.
 - **Debug** (default) – Logs of this level record the detailed information related to the internal operations such as the communication between Perimeter Manager and Perimeter Agent, the operations in the database, the output message of the data.

 Logs of this level are used for finding out all the details of the jobs, and it is recommended that the level is set to **Debug** before troubleshooting. Debug level logs also contain all of the logs from **Information**, **Warning** and **Error** levels.
 - **Error** – Logs of this level record the error messages for jobs. Not all the errors could lead to the failure of the jobs, some of the errors have already been dealt with and the logs will record the detailed information.
 - **Warning** – Logs of this level record exceptions for jobs. **Warning** level logs also contain all of the logs from **Error** level.

***Note:** After changing the log levels, the changes will not affect the previous logs but will affect the newly generated logs.

- **Size of Each Log File** –The default size for a log is 5 MB. You can adjust the size according to your requirements by entering a different number into the text box.
- **Total Log File Limit** – The maximum number of all the log files in the Logs folder under the installation folder of each Manager Service. For each Agent server, the Total Log File Count is the maximum number of all the log files which can be generated by each **.exe** file. The Agent logs are stored in the Logs folder under the installation folder of each Agent.

When the number of log files exceeds the threshold, the oldest log files will be deleted.

3. When you are finished configuring **Log Settings**, click **Save** to save all changes and return to the **Log Manager** interface.

To configure the log settings for multiple services in bulk, complete the following steps:

1. Select all of the desired services and click **Batch Log Settings** on the ribbon.
2. On the **Batch Log Settings** pop-up window, configure the **Log Level**, **Size of Each Log File**, and **Total Log File Limit**.
3. When you are finished configuring **Log Settings**, click **Save** to save all changes and return to the **Log Manager** interface.

Collecting Logs

In order to collect logs in **Log Manager**, select your desired services or Agents by clicking the corresponding checkboxes and clicking **Collect** on the ribbon to initiate the job for collecting logs for the selected services or Agents. To view the job details, navigate to **Job Monitor**.

Configuring Monitoring Settings

In the **Monitor** interface, you can view and manage the **Timer Job Definition** of the built-in timer jobs and view the **Timer Job Status**.

Monitoring Timer Job Definition

To access **Timer Job Definition**, navigate to the **Configure** menu and then click **Timer Job Definition** under the **Monitor** heading.

In **Timer Job Definition**, you can view and manage built-in batch timer jobs. These batch timer jobs are used to monitor the agents' health, calculate session summary data for **All Access Logs** in **Dashboard** based on real-time access logs, update the last modified time of shared SharePoint files, calculate the data displayed in the dashboards of the AvePoint Perimeter Internal Portal, monitor the status of each Agent, and prune the expired data based on predefined retention periods.

***Note:** **Health monitoring** timer job will send the **AvePoint Perimeter Agent Health Analyzer Report** to the contact you configured in the **General Settings**, if the potential issues that might affect your usage of Agents are detected.

The timer jobs' basic information and their schedules are predefined. You can edit and enable/disable the timer Jobs.

Editing Timer Jobs

To edit a timer job, complete the steps below:

1. Click the timer job title to access the **Edit Timer Job** interface and edit the following configurations:
 - **Basic Information** – Enter the **Job Title** and **Description** for the timer job you are editing.
 - **Schedule Settings** – Specify how frequently this timer job runs.
 - o **Schedule Type** – Select the interval at which the timer job occurs: **By minute**, **By hour**, **By day**, **By week**, or **By month**.
 - o **Interval** – Set up the frequency for the schedule by entering an integer in the text box.

- o **Start Time** – Specify the time of the day that Perimeter will check for blocked/warned access attempts. If you select **By month**, configure the **Specify the start time by day of the week** and **Specify the start time by date** fields. For more information, see the [Configuring Advanced Start Time Settings](#) section in this guide.
- 2. Click **Save** to save your configurations or click **Save and Run Now** to save the configurations and run the timer immediately.

Disabling and Enabling Timer Jobs

To disable, enable, and run a timer job immediately:

- **Disable** – If a timer job's value for the **ENABLED** column is **Yes**, you can disable it. To disable an enabled timer job, select the timer job you want to disable by selecting the corresponding checkbox, then click **Disable** on the ribbon or click the open menu button (***) next to the job title and then click **Disable** in the pop-up menu.
- **Enabled** – If a timer job's value for the **ENABLED** column is **No**, you can enable it. To enable a disabled timer job, select the timer job you want to enable by selecting the corresponding checkbox, then click **Enabled** on the ribbon or click the open menu button (***) next to the job title and then click **Enable** in the pop-up menu.
- **Run Now** – To run an enabled timer job immediately, select the corresponding checkbox, then click **Run Now** on the ribbon or click the open menu button (***) and then click **Run Now** in the pop-up menu.

Monitoring Timer Job Status

To access **Timer Job Status**, navigate to **Configure** menu and then click **Timer Job Status** under the **Monitor** heading. In **Timer Job Status**, you can check whether timer jobs are successful or failed.

You can view the timer jobs' statuses using the following three tabs:

- **Scheduled Jobs** – Allows you to exclusively view timer jobs that are scheduled to run in the future.
- **Running Jobs** – Displays all current running timer jobs.
- **Job History** – Displays all previous timer jobs.

Configuring Windows Phone Log Location

Windows Phone Logs in the **Configure** menu provides you with the **Diagnostic Logs Location** feature. Within this interface, you can configure a diagnostic logs location for storing uploaded diagnostic logs of AvePoint Perimeter Windows Phone apps. Using the **Upload Logs** feature in the AvePoint Perimeter Windows Phone apps, end-users can upload the diagnostic log files of their AvePoint Perimeter

Windows Phone apps to the configured diagnostic logs location. Perimeter administrators can view the uploaded log files in this location.

Upon completion of the installation, the default diagnostic logs location of your Perimeter management system is the ...\\AvePoint\\Perimeter\\Manager\\files directory on the AvePoint Perimeter Manager server. To customize the diagnostic logs location, refer to the section below.

In **Diagnostic Logs Location**, configure the Universal Naming Convention (UNC) path for the location to store all of the uploaded diagnostic logs of the AvePoint Perimeter Windows Phone apps within this Perimeter management system and the credentials for accessing the UNC path.

1. To access **Diagnostic Logs Location**, navigate to the **Configure** menu, and then click **Diagnostic Logs Location** under the **Windows Phone Logs** heading. To configure the diagnostic logs location for this Perimeter management system, complete the following settings:
2. In the **UNC Path** text box, enter the UNC path for the location where you want to store the uploaded log files of AvePoint Perimeter Windows Phone apps. Note that the UNC path should be entered in the following format: \\admin-PC\\c\$\\data or \\admin-PC\\ shared folder.
3. In the **Username** and **Password** text boxes, enter the credentials of the account used to access the UNC path configured above. Note that the entered account must have **Write** permissions to the UNC path configured above.
4. Click **Validation Test** to test the entered information is valid.
5. Click **OK** to save the shared file location or click **Cancel** to exit the current page without saving any configuration.

Job Monitor Interface

Job Monitor allows you to view the status or details of jobs, download reports, and manage jobs all from a central interface. You can view the following types of jobs in Job Monitor: Access Violation Notification, Access Warning Notification, Bulk Device Enrollment, Log Collection, and AD User Synchronization.

- Access Violation Notification and Access Warning Notification jobs send scheduled notifications for access violations and access warnings based on the settings you configured in **Notification E-mail Settings**. For more information, refer to [Configuring Notification E-mail Settings](#).
- Bulk Device Enrollment jobs send device enrollment requests in bulk based on the settings configured in **Bulk Device Enrollment**. For more information, refer to [Sending Device Enrollment Requests in Bulk](#).
- Log Collection jobs collect logs based on the settings in **Log Manager**. For more information, refer to [Collecting Logs](#).
- AD User Synchronization jobs synchronize Active Directory users based on the settings you configured in **Synchronize AD User**. For more information, refer to [Synchronizing Active Directory Users](#).


In the viewing pane of Job Monitor, you can view the following information of each job: **JOB ID**, **TYPE**, **PROGRESS**, **STATUS**, **START TIME** and **FINISH TIME**.

When a job completes or completes with exception, you can perform the following operations on the job:

- **Download** – To download the job details of a particular job, select the corresponding checkbox next to the **JOB ID** and then click **Download** > **Download Job Details** on the ribbon. Your browser will ask if you would like to open or save the file. Click **Save** or **Save as** to save it to a designated location.

***Note:** This option is available for the following jobs: Bulk Device Enrollment, Log Collection, and AD User Synchronization.
- **Delete** –To delete job information, select the corresponding checkboxes next to THE **JOB ID** and click **Delete** on the ribbon.
- **Job Summary** – To view the summary of a job, select the corresponding checkbox next to the **JOB ID** and then click **Job Summary** on the ribbon. You can view the summary information in the **Job Summary** pop-up window.

Job Monitor also allows you to search for jobs by job type to further customize which jobs are displayed to you. Enter the keyword of your desired job type in the search box on the ribbon and click the search

() button. The matched results will be displayed in the viewing pane.

Monitoring User Activity and Locations via Burglar Alarm Rules

Using configured Burglar Alarm Rules, AvePoint Perimeter can identify and generate a report of suspicious user activity and send e-mail notifications to notify system administrators of this activity. With AvePoint Perimeter, Administrators can limit user activity and restrict allowable locations by applying **Burglar Alarm Rules** on SharePoint nodes, Perimeter will monitor the actions performed upon SharePoint documents, the usage of the AvePoint Perimeter Secured Share site collection feature, the number of failed login attempts to 2-factor authenticated nodes, and the locations where users log into 2-factor authenticated nodes.

Refer to the sections below for detailed information on monitoring user activities and locations using **Burglar Alarm Rules**.

To monitor user activities and locations within your SharePoint environment, first review [Types of Burglar Alarm Rules](#), then follow the procedures below:

1. [Configuring SharePoint Audit Settings for Document Activity Rules at the Web Application or Site Collection Level](#)
2. [Retrieving Audit Data for Document Activity Rules](#)
3. [Configuring Document Activity Collections](#)
4. [Configuring and Applying Burglar Alarm Rules](#)

Types of Burglar Alarm Rules

The following types of Burglar Alarm rules are available:

1. **Document Activity** – Monitors the frequency at which a user performs actions on documents within a user-defined time range. **Document Activity** offers the following two rules: **Single Activity** and **Activity Collection**.
 - **Single Activity** – Monitors how many times a user performs an action on documents within a user-defined time range.
 - **Activity Collection** – Monitors the total number of actions included in a user-defined document activity collection that are performed by a user on documents within a user-defined time range. A document activity collection includes multiple actions that can be monitored by an individual **Document Activity** rule. For detailed information on configuring a document activity collection, refer to [Configuring Document Activity Collections](#).

Using **Document Activity** rules, the following are the available actions that can be monitored:

- Track real-time data for the following user activities: Read online, Download, E-mail as Attachment, Read, Open in 3rd Party App, View Shared File in Portal, and Download Shared File from Portal.
- Track the retrieved SharePoint audit data for the following user activities: **Check Out, Check In, View, Delete, Update, Profile Change, Delete Child, Schema Change, Restore, Workflow, Copy, Move, and Search**. These activity types use the same definitions as the SharePoint audit events.

***Note:** To use the Document Activity rules for monitoring the activities mentioned above, you must first enable the corresponding SharePoint audit events in the desired SharePoint nodes, and retrieve the required audit data. For details instructions, refer to [Configuring SharePoint Audit Settings for Document Activity Rules at the Web Application or Site Collection Level](#) and [Retrieving Audit Data for Document Activity Rules](#).

2. **Failed Login Attempts** – Monitors how many times a user failed to log into 2-factor authenticated SharePoint sites by the rule **2-Factor Authentication Failure**. AvePoint Perimeter identifies suspicious user activity monitored by the **Failed Login Attempts** rule using the real-time data of 2-factor authentication failures.
3. **Secured Share** – Monitors the usage of the **AvePoint Perimeter Secured Share** feature using the following rules:
 - **Shared by Same User** – This rule monitors how many files a user shares with others via the **Secured Share** feature within a user-defined time range.
 - **Shared with Same User** – This rule monitors how many files are shared with a user via the **Secured Share** feature within a user-defined time range.

AvePoint Perimeter identifies suspicious activities monitored by the **Secured Share** rules using the real-time usage data of the **AvePoint Perimeter Secured Share** feature.

4. **Login Location** – Monitors the distance between the last two locations where a user was when logging into SharePoint sites with 2-factor authentication enabled. This rule uses the **Distance Between Locations** rule. AvePoint Perimeter identifies suspicious activities monitored by the **Login Location** rule using the real-time user location data.

Configuring SharePoint Audit Settings for Document Activity Rules at the Web Application or Site Collection Level

Document Activity Burglar Alarm rules with the same activity definitions as SharePoint audit events rely on SharePoint audit data. Therefore, before you can apply **Document Activity** Burglar Alarm rules, you must enable SharePoint audit events using **SharePoint Audit Settings**.

To access the **SharePoint Audit Settings** interface, navigate to the **Manage** menu and then click **SharePoint Audit Settings** under the **Audit** heading. In the **SharePoint Audit Settings** interface, expand

the scope tree to the Web application or site collection level to view the SharePoint audit settings on each node within your SharePoint farm.

- **SharePoint Audit Events** – This column displays the number of currently enabled SharePoint audit events in the Web application or site collection node.
- **Audit Settings Inherited?** – This column indicates if the site collection node is inheriting SharePoint audit settings from its parent node. For detailed information on inheriting and stop inheriting of SharePoint audit settings, refer to [Inheriting and Stop Inheriting of SharePoint Audit Settings](#).

To enable the SharePoint audit events, complete the following steps:

1. Expand the scope tree to the Web application or site collection level, select the node where you want to configure SharePoint audit settings by clicking the corresponding checkbox.

***Note:** Prior to configuring the audit settings on a site collection node, you must ensure the node is not inheriting audit settings from its parent node, with the **Audit Settings Inherited?** column displaying **No**. If the **Audit Settings Inherited?** column of a selected site collection node display **Yes**, you must click the **Stop Inheriting** on the ribbon to stop inheriting the audit settings from its parent.

2. Click **Configure** button on the ribbon to access the **Configure** interface for configuring SharePoint audit settings.
3. Complete the following steps in the **Configure** interface:

- a. **Audit Event Selection** – Select the audit events you want to monitor in the selected SharePoint node, or deselect the events you do not want to audit in the selected SharePoint node.

***Note:** If some SharePoint audit events are currently enabled in the selected site collection, the **Events Currently Enabled for Auditing** field is available, displaying the currently enabled audit events in this site collection.

- b. **Scheduling Settings** – Configure the schedule for applying the audit settings configured above by choosing one of the following options:
 - o **No schedule** – With this option selected, the configured audit settings will be applied once when you click **Apply Now** to save the configurations. After these settings are applied for the first time, they will not be applied automatically again. You can only manually apply the settings from the **Configure** interface.
 - o **Configure the schedule myself** – With this option selected, you can configure the schedule for applying the configured audit settings. A separate configuration area appears when you select this option and you can customize the schedule with the following options:
 - **Schedule Type** – Select the schedule type for applying the configured audit settings: **By minute**, **By hour**, **By day**, **By week**, or **By month**.

- **Interval** – Set up the frequency for the schedule by entering an integer in the text box.
- **Start Time** – Specify the time of the day when Perimeter applies the configured audit settings. If you select **By month**, configure the **Specify the start time by day of the week** and **Specify the start time by date** fields. For more information, see the [Configuring Advanced Start Time Settings](#) section in this guide.

***Note:** If the selected node is a Web application, and a new child site collection is created after the configured audit settings are applied to this Web application, the previously applied audit settings will not take effect on the newly created site collection. To ensure the audit settings can be automatically applied to the newly created site collection under a Web application, AvePoint recommends configuring a schedule for applying the audit settings to the Web application.

4. Click **Apply Now** to save the configurations and apply the configured audit settings on the selected node immediately, or click **Cancel** to close the page without saving the configurations.

Disabling All SharePoint Audit Events

In the **SharePoint Audit Settings** interface, you can disable auditing on Web application and site collection nodes. After the SharePoint audit events are disabled on the selected nodes, the SharePoint audit feature will no longer audit these nodes or any child nodes.

Complete the following steps:

1. Access the **SharePoint Audit Settings** interface.

On the scope tree, select the nodes where you want to disable all audit events.

- If the selection nodes have unique SharePoint audit settings, the **Disable All Events** button is available; proceed to step 2.
- If some of the selected nodes are inheriting audit settings from their parent nodes, the **Disable All Events** button is not available. To disable all audit events in a site collection node that is inheriting audit settings from its parent node, you must first click the **Stop Inheriting** button to break inheritance from its parent. Then, the **Disable All Events** button becomes available. To inherit or stop inheriting SharePoint audit settings, refer to [Inheriting and Stop Inheriting of SharePoint Audit Settings](#).

2. Click **Disable All Events** on the ribbon. A confirmation window appears.
3. Click **OK**.

Inheriting and Stop Inheriting of SharePoint Audit Settings

There are two node levels on the **Scope** tree in the **SharePoint Audit Settings** interface: Web application and site collection.

- If you configure SharePoint audit settings on a Web application node, the site collections within this Web application automatically inherit the audit settings applied to their parent node.
- If you configure SharePoint audit settings on a site collection node, the configured audit settings will only be applied to the selected node, without affecting other site collection or Web application nodes.

When configuring SharePoint audit settings for the first time, you can configure audit settings directly at either the Web application or site collection level. After you configure audit settings for a Web application, you can still directly configure audit settings of this Web application. However, if you want to configure unique audit settings for a site collection under this Web application, you must first break the site collection's inheritance of audit settings from its parent.

- To stop specific site collections' inheritance of audit settings from their parent nodes, select the corresponding nodes on the scope tree, with the **Audit Settings Inherited?** column displaying **Yes**, and click **Stop Inheriting** on the ribbon. The selected nodes stop inheriting audit settings from their parent nodes and the corresponding values in the **Audit Settings Inherited?** column become **No**. The previously inherited audit settings are kept in these site collection nodes and the changes of the audit settings applied on the parent nodes will not affect these nodes.
- If you have broken the audit settings inheritance on some site collection nodes, you can inherit the audit settings from their parent nodes again. On the scope tree, select the nodes which have broken the audit settings inheritance from their parent nodes, and click **Inherit** on the ribbon. The selected nodes inherit audit settings from their parent nodes again and the audit settings currently applied on the selected site collections are overwritten. The values in the **Audit Settings Inherited?** column of the selected nodes become **Yes**.

Retrieving Audit Data for Document Activity Rules

With the desired SharePoint audit events enabled in the nodes where you use the **Document Activity** Burglar Alarm rules, use the **Retrieve Audit Data** feature to configure the audit data retrieval settings and retrieve audit data from SharePoint nodes.

To access the **Retrieve Audit Data** interface, navigate to the **Manage** menu and then click **Retrieve Audit Data** under the **Audit** heading. In the **Retrieve Audit Data** interface, expand the scope tree to the Web application or site collection level to view the audit retrieval settings of your SharePoint farm.

- **Audit Data Retrieved** – Displays whether Perimeter has retrieved audit data from the Web application and site collection node in the farm.

- **Retrieval Schedule** – Displays whether you have configured the audit retrieval schedule for this farm.

To retrieve audit data from a SharePoint farm, you must first configure the audit retrieval settings for the farm to determine the data retrieval scope and schedule. If you select **Configure the schedule myself** in **Retrieval Schedule** and configure a schedule for retrieving audit data, Perimeter will run scheduled jobs to automatically retrieve audit data from the nodes selected in **Scope Selection**. If you select **No schedule**, your only option is to manually retrieve the data.

***Note:** The **Retrieve Audit Data** feature automatically excludes the following SharePoint objects and users while retrieving audit data from SharePoint farms:

- SharePoint system pages whose URLs contain **/_catalogs/**, **/SitePages**, or **_.000** or end with **/Forms** or **/Forms/AllItems.aspx**.
- The system accounts of the SharePoint farm whose SharePoint audit data is to be retrieved.
- The user configured in the **System Credentials** interface.

To customize the SharePoint objects or users whose SharePoint audit data will not be retrieved, refer to [Configuring Filter Rules for Excluding Specific Audit Data](#).

For detailed instructions, refer to the sections below.

Configuring Audit Retrieval Settings for a Farm

To configure the audit retrieval settings for a SharePoint farm where you want to retrieve audit data, complete the following steps:

1. On the **Scope** tree of the **Retrieve Audit Data** interface, select the farm for which you want to configure the audit data retrieval settings.
2. Click **Configure Settings** on the ribbon to access the **Audit Retrieval Settings** interface of the selected farm.
3. Configure the following settings in the **Audit Retrieval Settings** interface:
 - a. In the **Scope Selection** section, select the checkboxes of the Web application and/or site collection nodes where you want to retrieve audit data. To view the enabled audit events in a site collection, hover over **View enabled audit events** on the right of the site collection URL. A tooltip appears, displaying the enabled audit events of the node.

***Note:** Only the nodes with enabled SharePoint audit events are selectable on the scope tree.
 - b. In the **Schedule Settings** section, configure the schedule for retrieving audit data from the selected nodes by choosing one of the following options:

- o **No schedule** – With this option selected, you can only manually retrieve audit data from the selected nodes. To manually retrieve audit data, refer to [Manually Retrieving Data from a Farm](#).
 - o **Configure the schedule myself** – With this option selected, you can configure the schedule for retrieving audit data from the selected nodes. A separate configuration area appears when you select this option and you can customize the schedule with the following options:
 - **Schedule Type** – Select the schedule type for retrieving audit data from the selected nodes: **By minute**, **By hour**, or **By day**.
 - **Interval** – Set up the frequency for the schedule by entering an integer in the text box.
 - **Start Time** – Specify the time of the day when Perimeter starts to retrieve the audit data from the selected nodes.
4. Click **Save** or **Save and Retrieve Now** to save the configurations or click **Cancel** to exit this page without saving your configurations.
- Click **Save** to save the configurations and return to the **Retrieve Audit Data** interface.
 - Click **Save and Retrieve Now** to save the configurations and retrieve audit data from the selected nodes immediately.

Manually Retrieving Data from a Farm

If you selected **No schedule** in **Retrieval Schedule**, you can only manually retrieve audit data from the nodes selected in **Scope Selection** by completing the following steps:

1. Navigate to the **Retrieve Audit Data** interface.
2. On the **Scope** tree, select the farm node, where you want to manually retrieve audit data.
3. Click **Retrieve Now** on the ribbon to start a job to retrieve audit data.

Configuring Filter Rules for Excluding Specific Audit Data

To exclude specific SharePoint objects or users from being audited by the **Retrieve Audit Data** feature, follow the steps below to configure filter rules in the **UserConfig.xml** configuration file on the Perimeter Manager server.

1. Navigate to `...AvePoint\Perimeter\bin\Config\` directory on the Perimeter Manager server.
2. Open the **UserConfig.xml** file.
3. To add a filter rule for excluding SharePoint objects by URL, add the child node `<Rule value="" condition=""/>` within the `<AuditorDataExcludeRules>` node.
 - **Rule value** – Set the value of this attribute to the value that is contained by the desired URLs or at the end of the desired URLs.

- **condition** – Set the value of this attribute to either of the following conditions:
 - o **contains** – With this condition, this rule filters and excludes the URLs that contain the value of the **rule value** attribute.
 - o **endwith** – With this condition, this rule filters and excludes the URLs that end with the value of the **rule value** attribute.
- 4. To add a filter rule for excluding a SharePoint user by username, add the child node **<User name="" />** within the **< AuditorDataIgnoreUsers>** node and set the desired user's login name as the value of the **User name** attribute.

```
<AuditorDataExcludeRules>
  <Rule value="/_catalogs/" condition="contains"/>
  <Rule value="/Forms" condition="endwith"/>
  <Rule value="/Forms/AllItems.aspx" condition="endwith"/>
  <Rule value="/SitePages" condition="contains"/>
  <Rule value="_.000" condition="contains"/>
</AuditorDataExcludeRules>
<AuditorDataIgnoreUsers>
  <User name="Domain\user1" />
</AuditorDataIgnoreUsers>
```

Figure 6: Configuring the UserConfig.xml file.

5. Save the changes and close the file.

Configuring Document Activity Collections

In **Document Activity Collection**, you can configure document activity collections to include multiple document activities that can be monitored by individual Burglar Alarm Document Activities rules.

To access **Document Activity Collection**, navigate to the **Manage** menu and click **Document Activity Collection** under the **Audit** heading.

Adding a New Document Activity Collection

To configure a document activity collection in the Document Activity Collection interface, complete the following steps:

1. Click **Add** on the ribbon to access the **Add Document Activity Collection** interface.
2. In the **Basic Information** section, enter the name of the document activity collection you are about to create.
3. In the **Activity Type Selection** section, select the checkboxes of the activities that you want to add into this document activity collection.
4. Click **Save** to save the configurations and add the document activity collection, or click **Cancel** to exit this interface without adding the document activity collection.

Editing a Document Activity Collection

After a document activity collection is created, its name cannot be changed. You can only change the document activity types included in a previously created document activity collection, by completing the following steps:

1. In the **Document Activity Collection** interface, select the corresponding checkbox next to the desired document activity collection and click **Edit** on the ribbon to access the **Edit Document Activity Collection** page.
2. In the **Activity Type Selection** section, select the checkboxes of the activities that you want to include in this document activity collection, and deselect the checkboxes of the activities you do not want to include in this document activity collection.
3. Click **Save** to save the changes, or click **Cancel** to exit this interface without saving the changes.

Deleting Document Activity Collections

To delete a previously created document activity collection, select the corresponding checkbox and click **Delete** on the ribbon. Alternatively, you can click the open menu (***) button next to the document activity collection name and then click **Delete** in the menu. The document activity collection is deleted from the AvePoint Perimeter management system.

Configuring and Applying Burglar Alarm Rules

In **Burglar Alarm Rules**, you can configure and apply Burglar Alarm rules at Web application or site collection level to monitor end-user activities and locations across the AvePoint Perimeter management system. After the Burglar Alarm rules are applied to SharePoint nodes, Perimeter can retrieve the required data and then check whether there are suspicious activities based on the thresholds configured in the rules.

To access **Burglar Alarm Rules**, navigate to the **Manage** menu and click **Burglar Alarm Rules** under the **Audit** heading.

In the **Burglar Alarm Rules** interface, you can view the number of Burglar Alarm rules applied on each Web application or site collection node of a SharePoint farm, by expanding the scope tree to the Web application or site collection level. The **Burglar Alarm Rules** column displays the number of rules currently applied on each node.

To configure and apply Burglar Alarm rules to a Web application or site collection node, complete the following steps:

1. In the **Scope** pane, expand the farm tree to the Web application or site collection level.
2. Select the Web application or site collection node where you want to configure and apply Burglar Alarm rules and click **Configure** on the ribbon to access the **Configure** interface, or click the link in the **Burglar Alarm Rules** column next to the node.

3. In the **Burglar Alarm Configuration** section, configure the rules you want to apply to the selected node. For detailed instructions on configuring Burglar Alarm rules, refer to [Creating or Editing Burglar Alarm Rules](#).
4. In the **E-mail Notification Settings**, determine whether to send e-mail notifications immediately when Perimeter identifies suspicious activities based on the rules configured above. To send immediate e-mail notifications to the desired users, complete the following steps:
 - a. Select the **Send e-mail notification to the specified recipients immediately** checkbox. The **Recipients** text box and **Include the direct manager of the users who trigger alarms** checkbox appear below.
 - b. In the **Recipients** text box, enter the e-mail addresses of the recipients who will receive the e-mail notifications. Separate each e-mail address with semi-colons.
 - c. To send e-mail notifications to the direct manager of the users who trigger the Burglar Alarm rules, select **Include the direct manager of the users who trigger alarms**.

***Note:** To ensure Perimeter can properly retrieve the appropriate e-mail addresses for notifications, you must use the **Synchronize Active Directory Users** feature to synchronize all Active Directory users in your organization with Perimeter from the domain controller. For detailed information on using the **Synchronize Active Directory Users** feature, refer to [Synchronizing Active Directory Users](#).
5. Click **Save** to save the configurations and immediately apply the rules to the selected node, or click **Cancel** to exit this interface without saving the configurations.

***Note:** After you apply Burglar Alarm rules to a Web application, all of the site collections within the Web application will automatically inherit the rules applied to their parent node. The site collection's previously applied rules will be overwritten.

After the Burglar Alarm rules are applied to a SharePoint Web application or site collection, Perimeter will start real-time monitoring on the corresponding user activities and locations based on the configured settings. Once Perimeter identifies any suspicious activities, the activities that cross the rules' thresholds will be recorded in the **Burglar Alarm Report**, with detailed information. For detailed information on the **Burglar Alarm Report**, refer to [Burglar Alarm Report](#). Also, Perimeter provides the following notifications:

- **Burglar Alarm Notification** in Perimeter Manager – After Perimeter identifies new suspicious activities, a red dot will appear on the flag button for **Burglar Alarm Notification** on the upper right corner of the Perimeter Manager interface. To view the newly generated notifications, complete the following steps:
 - i. Click the flag button for **Burglar Alarm Notification** to access the **Burglar Alarm Notification** window.
 - ii. In this window, you can view the notifications for each triggered Burglar Alarm rule sorted by date.

- iii. To view the detailed information of the activities that trigger a particular Burglar Alarm rule, click the desired notification item to access the Burglar Alarm Report interface. For detailed information on the **Burglar Alarm Report**, refer to [Burglar Alarm Report](#).

- **Burglar Alarm: Suspicious Activity Alert** – If the **Send e-mail notification to the specified recipients immediately** checkbox is selected in the **Configure** interface of **Burglar Alarm Rules**, Perimeter will send immediate **Burglar Alarm: Suspicious Activity Alert** e-mail notifications on the identified suspicious activities to the entered **Recipients**.

Creating or Editing Burglar Alarm Rules

To create or edit Burglar Alarm rules in the **Configure** interface of the **Burglar Alarm Rules** feature, complete the following steps:

1. In the **Bugler Alarm Configuration** section, click **Add a Rule** to add a rule by completing the fields below.
 - **Alarm Type** – Select the alarm type of the rule you are about to add.
 - **Rule** – Select the rule you are about to add.
 - o With **Document Activity** selected in **Alarm Type**, you can select either of the following rules:
 - **Single Activity** – With this option selected, select the activity you want to monitor from the drop-down list on the right.
 - **Activity Collection** – With this option selected, select an existing document activity collection you want to monitor from the drop-down list on the right, or select **New Document Activity Collection** to create a new one. For details on creating a new document activity collection, refer to [Adding a New Document Activity Collection](#).
 - o With **Failed Login Attempts** selected in **Alarm Type**, **2-Factor Authentication Failure** is the only available rule.
 - o With **Secured Share** selected in **Alarm Type**, you can select the **Shared with Same User** or **Shared by Same User** rule.
 - o With **Login Location** selected in **Alarm Type**, **Distance Between Locations** is the only available rule.
 - **Threshold** – Configure the threshold for the rule you are about to add.
 - o With the **Single Activity**, **Activity Collection**, **2-Factor Authentication Failure**, **Shared by Same User**, or **Shared by Same User** selected in **Rule**, configure the threshold by entering an activity count integer into the text box. If a user performs the corresponding activity the number of times entered here within the user-defined time range, the corresponding rule will be triggered.

- o With **Distance Between Locations** selected in **Rule**, configure the maximum distance between locations in the threshold by entering a positive integer into the text box and selecting a unit from the drop-down list. If the distance between the locations of a user's last two logins reaches the distance configured here, the **Distance Between Locations** rule will be triggered.
 - **Condition** – The condition for all Burglar Alarm rules are **Within** and cannot be changed.
 - **Time Range** – Configure the time range the rule will cover for checking whether there are suspicious activities based on the configured threshold. Enter a positive integer in the text box and select a time unit from the drop-down list.
2. After configuring a rule, click **Add a Rule** to add another rule or delete a previously added rule by selecting the checkbox of the rule and clicking **Remove**.

Manage Menu

After configuring the configurations in the Configure menu, navigate to the **Manage** menu to invite end-users to enroll their mobile devices, publish SharePoint sites for accessing via enrolled devices and configure content access policies for SharePoint content via any devices. You can also use the Manage menu to manage the enrolled devices, end-users, device groups and locations configured for AvePoint Perimeter management system.

Enrolling a Device

If you have successfully configured **General Settings** and **Notification settings**, you can send device enrollment requests to invite users to enroll their mobile devices. You can manage the enrollment requests in the **Device Enrollment** interface.

Sending an Individual Device Enrollment Request

To send an enrollment request, follow the steps below:

1. Navigate to the **Manage** menu, and click **Device Enrollment** to enter the **Device Enrollment** interface.
2. Click **Enroll New Device** on the ribbon to enter the **Enroll New Device** interface and configure the following settings:
 - **User Type** – Specify the user type of the end-user you want to invite. Select **Internal** if the user is an internal user within your organization, or select **External** if the user is a user outside your organization. The **Ownership** section below will automatically load the available options according to your selection here.
 - **E-mail Address** – Enter the organization e-mail address of the end-user you want to invite.

***Note:** If you select **Internal** as the **User Type**, you must enter the user's e-mail address configured in the Active Directory Domain Controller.
 - **Username** – Enter the username of the end-user's account in the organization directory.
 - If you select **Internal** as the **User Type**, enter the username in the format: domain\username.
 - If you select **External** as the **User Type**, select the **Use e-mail address as username** checkbox to use the **E-mail Address** entered above as the username of the external user, or enter the username in the format: user@domain.com.
 - **Ownership** – Choose the type of ownership of the device to be enrolled.

If you selected **Internal** for **User Type**, you will have the following options for **Ownership**:

- **Work-issued** – The device is owned by the company.
- **Personal** – The device is owned by the internal user.
- **User to Provide** – Do not select the ownership of the device here. The end-user will provide this information when enrolling the device.

***Note:** If you select **External** for **User Type**, the **Ownership** is automatically set as **External** and cannot be changed.

- **Authentication Mode** – Specify the authentication method for this Perimeter Manager server during the mobile device enrollment process.
 - **Directory Credentials for Organization** – The user must provide the organization directory credentials (username and password) of the organization directory account during the mobile device enrollment process.
 - **One-Time Enrollment Code** – The user must provide the organization username and the One-Time Enrollment Code provided in the enrollment request during the mobile device enrollment process.
 - **2-Factor Authentication with both Directory Credentials and a One-Time Enrollment Code** – The user must provide both the organization credentials (username and password) and the One-Time Enrollment Code provided in the enrollment request during the mobile device enrollment process.
- **Expiration Time** – Specify when this enrollment request will expire.
 - **Request never expires** – This enrollment request never expires.
 - **Request expires on** – Select the expiration time for the enrollment request from the calendar.
 - **Request expires after** – Enter an integer in the text box and select **Days, Weeks, Months** or **Years** from the drop-down list. The enrollment request will expire after this period.
- **Recipient** – Enter the e-mail addresses of the recipients for this enrollment request. You can enter multiple e-mail addresses, separating them by semicolons.

***Note:** By default, the system administrator's e-mail address entered in **General Settings** is automatically filled in this field. The system administrator will receive an e-mail notification of each enrollment request.

- **Subject** – Enter the subject of the enrollment request e-mail.

3. **Enroll Another Device** – Select whether to continue to enroll another device after you are finished sending this enrollment request.

- If you select this option, click **Send** to send the enrollment request. Once the enrollment request has been sent out, you will stay on the **Enroll New Device** interface to configure a new enrollment request.

- If you do not select this option and click **Send** to send the enrollment request. Once the enrollment request has been sent out, you will exit this page and come back to the **Device Enrollment** interface.

If you don't want to save and send this enrollment request, click **Cancel** to exit the page without saving the configurations and sending the enrollment request.

Sending Device Enrollment Requests in Bulk

To send enrollment requests in bulk, complete the following steps:

1. Navigate to the **Manage** menu, and click **Device Enrollment** to enter the **Device Enrollment** interface.
2. Click **Bulk Device Enrollment** on the ribbon to enter the **Bulk Device Enrollment** interface.
3. Click the hyper link of **Download the bulk enrollment template** to download a bulk enrollment template.
4. Fill in the downloaded template with the required information of the users you want to invite.
5. When you finish configuring the template file, save it as a bulk enrollment file.
6. Click **Browse** button to locate and open the previously configured bulk enrollment file.
7. Click **Apply** on the ribbon to apply the selected bulk enrollment file and AvePoint Perimeter will initiate the job for sending enrollment requests to all of the users in this enrollment file.

Managing Enrollment Requests

In the Device Enrollment interface, you can manage and delete the previously created enrollment requests as below:


- **Resend Enrollment Request** – To resend the previously created enrollment requests, select the corresponding checkboxes and click **Resend Enrollment Request** on the ribbon.
- **Delete** – To delete the previously created enrollment request, select the corresponding checkboxes and click **Delete** on the ribbon.

End-User Device Enrollment

For end-users to enroll their device, they must receive an enrollment e-mail sent by AvePoint Perimeter Manager, as described in [Sending an Individual Device Enrollment Request](#).

***Note:** To use Perimeter App on a Windows Phone, you must download and install a certificate before logging into the Perimeter App. For details, refer to [Downloading and Installing Certificate on Windows Phone Before Login](#).

The following procedure assumes that AvePoint Perimeter is installed and running, and that the end-user has received the enrollment e-mail.

1. Obtain the free AvePoint Perimeter mobile app. Refer to the enrollment e-mail for a link to the appropriate app store.
2. Once the app is installed, open the app, click the scan () button to scan the QR code in the enrollment e-mail to automatically enter the **Device Service URL** and **E-mail Address** information provided in the enrollment e-mail, or manually enter the information into the corresponding text boxes.
3. Click **Enroll** to access the next page.
4. Enter the required authentication information according to the user type:
 - If enrolling an **Internal** user, enter the **Username** and **Password** and/or **One-Time Enrollment Code** authentication information provided in the enrollment e-mail.
 - If enrolling an **External** user, enter the **One-Time Enrollment Code** provided in the enrollment e-mail.

Downloading and Installing Certificate on Windows Phone Before Login

Complete the steps below to download and install the certificate on Windows Phone before logging into the Perimeter App:

1. Open the AvePoint Perimeter App on the Windows Phone. The login page appears.
2. There is a note under the **Enroll** button saying **If there is an error with the security certificate of the entered Device Service URL, click here to install the certificate**. Click **here**. The **Install certificate?** interface appears.

***Note:** Make sure the Perimeter Manager, Gateway, and Portals have internet access.
3. Click **Install**. You will be asked to open or save the downloaded file. Click **Open**.
4. After the certificate is automatically installed, click **OK**.

Managing Enrolled Devices

Once end-users receive the enrollment requests sent for AvePoint Perimeter Manager, they can follow the instructions in the enrollment request e-mails to download AvePoint Perimeter mobile app and enroll their devices into the AvePoint Perimeter management system.

You can access **Manage Enrolled Devices** to manage all of the enrolled devices. To access **Manage Enrolled Devices**, navigate to the **Manage** menu and then click **Manage Enrolled Devices** to enter the **Manage Enrolled Devices** interface.

In the **Manage Enrolled Devices** interface, you can view a list of all of the enrolled devices with basic information, including device name, device ID, platform, operation system, model, device owner, device ownership, registration time, last report time, last authentication time, and status. To filter the devices with criteria, you can use the search box in the upper-right corner to search by the desired device names

or use the **Advanced Search** feature to configure multiple search conditions. To use **Advanced Search**, refer to [Advanced Search](#).

In the **Manage Enrolled Devices** interface, you can follow the following operations to manage the enrolled devices.

- [Managing the Status of Enrolled Devices](#)
- [Viewing Enrolled Devices Details](#)
- [Deleting Enrolled Devices](#)

Managing the Status of Enrolled Devices

To manage the status of an enrolled device, you can perform the following actions:

Disabling a Device

When the **STATUS** of a particular device is **Active**, the **Disable** option is available on the ribbon. Disabled devices will not run the Perimeter app. To disable a particular device, follow the steps below:

1. Select the desired device by selecting the checkbox next to the corresponding **DEVICE NAME**.
2. Click **Disable** on the ribbon. The **Security Check** pop-up window appears.
3. In the **Security Check** window, enter the password of the current logon user and click **Confirm**. A pop-up window for the reason appears.
4. Enter the reason why you want to disable the AvePoint Perimeter app on this device in the text box and click **OK**.
5. Once the **Disable** action is complete, the **STATUS** of the device becomes **Disabled**.

Enabling a Device

To use the AvePoint Perimeter mobile app on a **Disabled** device, you need to enable the device. To enable a device, complete the following steps:

1. Select the desired device by selecting the checkbox next to the corresponding **DEVICE NAME**.
2. Click **Enable** on the ribbon. The **Security Check** pop-up window appears.
3. In the **Security Check** window, enter the password of the current logon user and click **Confirm**. A pop-up window for the reason appears.
4. In the pop-up window, enter the reason why you want to enable the AvePoint Perimeter app on this device and click **OK**.
5. Once the **Enable** action is completed, the **STATUS** of the device becomes **Active**.

Performing an Enterprise Wipe on a Device

If the device owner reports a loss of the device to the system administrator, you can use the **Enterprise Wipe** option to erase all of Perimeter's application data. To perform the Enterprise Wipe action, complete the following steps:

1. Select the desired device by selecting the checkbox next to the corresponding **DEVICE NAME**.
2. Click **Enterprise Wipe** on the ribbon. The **Security Check** pop-up window appears.
3. In the **Security Check** window, enter the password of the current logon user and click **Confirm**. A pop-up window for the recipient, subject and reason appears.
4. In the pop-up window, enter the recipient and subject for the notification e-mail of the Enterprise Wipe to be performed. Also, enter the reason why you want to enterprise wipe this device.
5. Click **Enterprise Wipe** to continue or click **No** to exit without performing any action.
6. Click **OK** to initiate this action or click **Cancel** to cancel this action.
7. Once an **Enterprise Wipe** action is initiated, the device's **STATUS** becomes **Enterprise Wipe Pending**. When the Enterprise Wipe action completes, the **STATUS** becomes **Inactive**.

Cancelling an Enterprise Wipe

When the **Status** of the device is **Enterprise Wipe Pending**, you can cancel the **Enterprise Wipe** action on this device before it is executed. To do this, complete the following steps:

1. Select the desired device by selecting the checkbox next to the corresponding **DEVICE NAME**.
2. Click **Cancel Enterprise Wipe** on the ribbon. The **Security Check** pop-up window appears.
3. In the **Security Check** window, enter the password of the current logon user and click **Confirm**. A pop-up window for the reason appears.
4. In the pop-up window, enter the reason why you want to cancel the **Enterprise Wipe** action and click **OK**.
5. The **STATUS** of the device reverts back to the status before the **Enterprise Wipe** action was initiated.

Sending an Instant Message

When the **Status** of the device is **Active** or **Disabled**, you can use the **Send Instant Message** option to send an instant message to the device. To send an instant message to a device, complete the following steps:

1. Select the desired device by selecting the checkbox next to the corresponding **DEVICE NAME**.
2. Click **Send Instant Message** on the ribbon. The **Send Instant Message** window appears.
3. In the pop-up window, enter the **Title** and **Body** of the message you want to send.

4. Click **OK** to send the message or click **Cancel** to exit without sending the message.

Viewing Enrolled Devices Details

To view detailed information on an enrolled device, click on the **Device Name** to enter the **Device Details** interface. Alternatively, you can select the corresponding checkbox and then click **View Details** on the ribbon. In the **Device Details** interface, you can view the device details in these four tabs: **Basic Information**, **Usage Tracking**, **Location History** and **Action History**.

Viewing Basic Information

The following information is available from the **Basic Information** tab:

1. **General Information** – In the **General Information** section you can view the following information:
 - **Last Username** – The username of the last user who logged into the AvePoint Perimeter app using this device.
 - **Ownership** – The ownership type of this device. This is specified in the enrollment request or provided by the user while enrolling this device.
 - **Registration Time** – The last time when this device was logged into to the AvePoint Perimeter management system.
 - **Last Authentication Time** – The last time the user authenticated to the SharePoint sites using this device.
 - **Last Report Time** – The last time when this device communicated with AvePoint Perimeter Manager.
 - **Managed Status** – The status of this device in this management system. There are four possible statuses for an enrolled device.
 - **Active** – When the status is **Active**, The user can use this device to access SharePoint sites normally.
 - **Disabled** – When the status is **Disabled**, users cannot use the AvePoint Perimeter app on this device.
 - **Enterprise Wipe Pending**– When the status is **Enterprise Wipe Pending**, the AvePoint Perimeter Mobile app will erase all Perimeter app data.
 - **Inactive** – When the status is **Inactive**, this device has been deactivated. Users cannot log into the AvePoint Perimeter Mobile app using this device.
 - **Push Notification Enabled** – Whether this device is allowed to receive push notification from the Apple Push Notification Service (APNS) servers or Google Cloud Messaging (GCM) servers.
 - **Status Message** – The message provided by the administrator who performed the last operation on this device.

- **Mobile App Version** – the version of the AvePoint Perimeter mobile app installed on this device.
2. **Hardware Information** – In the **Hardware Information** section, you can view the following information:
- **Device ID** – The GUID of the device in the Manager Configuration database.
 - **Device Name** – The name of the device.
 - **Platform** – The platform of the device's operation system.
 - **Operation System** – The version of the device's operation system.
 - **Manufacturer** – The manufacturer of the device.
 - **Model** – The model of the device.
 - **Form Factor** – The form factor of the device which is used to refer to the size, style and shape of the device as well as the layout and position of the device's major components.
3. **Location Information** – In the **Location Information** section, you can view the following information:
- **Location Service Enabled** – Displays whether the Location Service is enabled on the device to allow the AvePoint Perimeter Mobile app to collect the device's geographical location information.
 - **Last Location** – Displays the name of the last location of the device.
 - If the location falls in the scope of a previously configured location in **Manage Locations**, the location name is displayed here.
 - If the device's last location doesn't fall in any scope configured in **Manage Locations**, **Undefined** is displayed here.
 - If the Location Service is disabled on the device, the AvePoint Perimeter app cannot collect the device's geographical location information, and **Unavailable** is displayed here.
 - **Location Last Updated Time** – The last time that the AvePoint Perimeter Mobile app reported the device's location to the AvePoint Perimeter management system.
 - **Last Latitude/Longitude** – The coordinates of the device's last location.
 - **Last Address** – The address provided by the Bing Maps for the device's last location.
 - **Accuracy** – The accuracy of the coordinates displayed in **Last latitude/Longitude**.
 - **Location Collection Exception** – Displays the exception details when an exception occurs while collecting the device latitude and longitude location via the device Location Services.
 - **Last Location Collection Exception Time** – Displays the time when the last exception occurs while collecting the device latitude and longitude location via the device Location Services.

In the **Basic Information** tab, you can also manage the status of a device by clicking the corresponding buttons on the ribbon. For more information on managing the status of a device, refer to [Managing the Status of Enrolled Devices](#).

Viewing Usage Tracking Details

To view the usage tracking details of a device, click the **Usage Tracking** tab. Here, you can view the activity the device has performed on the SharePoint items or documents, including the name of each accessed SharePoint object, the URL of the object, the activity performed on the object, the time of the activity and the device's location information.

With **Advanced Search**, you can search for items using search criteria. To use **Advanced Search**, refer to [Advanced Search](#).

***Note:** Perimeter keeps the Usage Tracking data for 60 days in the Manager Configuration database.

Exporting Usage Tracking Details

To export Usage Tracking data, click **Export** on the ribbon, select your desired data scope for the export report in the pop-up window, and then click **OK**. 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 Location History

To view the location history of a device, click the **Location History** tab. Here, you can view all of the location data collected for this device since its enrollment into this management system, including the update time of each location, the coordinates, and address of the device's geographical location. If the geographical location falls within the scope of a previously configured location in **Manage Locations**, both the **Location Name** and **Accuracy** of the location name are displayed.

Viewing Action History

To view the action history of a device, click the **Action History** tab. Here, you can view all of the actions performed on the device, including the start time, completed time, initiator, and status of each action. If the action failed, the exception details will be listed in the **Exception Details** column.

Deleting Enrolled Devices

Once a device has been Enterprise wiped, the device owner cannot log into the AvePoint Perimeter Mobile app using that device. You cannot reverse this action to activate this **Inactive** device via AvePoint Perimeter Manager.

As for the **Inactive** devices listed in the **Manage Enrolled Devices** interface, AvePoint recommends deleting the records of these devices for the AvePoint Perimeter management system. You can select the corresponding checkboxes of the devices you want to delete, click the open menu (*******) button on

the ribbon and then click **Delete** from the drop-down menu. Alternatively, you can click the open menu (*******) button next to the device name and then click **Delete** in the menu.

Publishing SharePoint Sites for Accessing via Enrolled Devices

To publish SharePoint sites (in both SharePoint on-premises and SharePoint Online), create device groups in **Manage Device Groups**, and then assign permissions to the device groups in **Site Access**.

Managing Device Groups

In **Manage Device Groups**, you can create and manage device groups based on predefined parameters. Device groups can be dynamic or static, and are primarily used to assign device permissions to SharePoint sites. To access **Manage Device Groups**, navigate to the **Manage** menu and click **Manage Device Groups** to enter the **Manage Device Groups** interface.

Adding New Device Groups

To add a new device group, complete the following steps:

1. Click **Add** on the ribbon to enter the New Device group interface.
2. In the **Basic Information** section, enter the device group name, an optional description, and the type for the device group to be created.
 - **Device Group Name** – Enter a name for the device group to be created.
 - **Description** – Enter an optional **Description** for the group for future reference.
 - **Type** – Select the type of the device group to be created.
 - **Dynamic** – If you select this option, Perimeter will automatically add the newly enrolled devices that meet the rules configured below after the device group is created.
 - **Static** – If you select this option, Perimeter will not check for newly enrolled devices after the device group is created. The devices in this group will not be added automatically.
3. In the **Rule Settings** section, configure the rules for adding devices into the device group.
 - After configuring a rule, click **Add a Rule** to add another rule, or click **Remove** to delete the rule.
 - If 2 or more rules are configured, determine the logical relationship in the **Conditions** text box. There are two logic choices: **And** and **Or**. The default logic is **And**.
 - **And** – Devices that meet all of the rules will be added into the device group.
 - **Or** – Devices that meet any one of the rules will be added into the device group.
4. Click **Preview Filter Results** to preview the devices that meet the configured rules.

5. Click **Save** to save the configurations and add the device group, or click **Cancel** to exit this interface without adding the device group.

Editing Device Groups

To edit a previously created device group, select the corresponding checkbox and click **Edit** on the ribbon, or click the open menu button next to the **DEVICE GROUP NAME** and then click **Edit** in the menu. You can edit the following configurations:

1. In the **Basic Information** section, enter the device group name, an optional description, and the type for the device group you are editing.
 - **Device Group Name** – Enter a name for the device group you are editing.
 - **Description** – Enter an optional **Description** for the group for future reference.
 - **Type** – Select the type of the device group you are editing.
 - **Dynamic** – If you select this option, Perimeter will automatically add the newly enrolled devices that meet the rules configured below after the device group is created.
 - **Static** – If you select this option, Perimeter will not check for the newly enrolled devices that meet the rules configured below after the device group is created. The devices in this group will not be added automatically.
2. In the **Rule Settings** section, configure the rules for adding devices into the device group.
 - After configuring one rule, click **Add a Rule** to add another rule, or click **Remove** following each rule to delete the rule.
 - If 2 or more rules are configured, determine the logical relationship in the **Conditions** text box. There are two logical choices: **And** and **Or**. The default logic is **And**.
 - **And** – Devices that meet all of the rules will be added into the device group.
 - **Or** – Devices that meet any one of the rules will be added into the device group.
3. Click **Preview Filter Results** to preview the devices that meet the configured rules.
4. Click **Save** to save the configurations to the device group, or click **Cancel** to exit this interface without editing the device group.

Deleting Device Groups

To delete a previously created device group, select the corresponding checkbox and click **Delete** on the ribbon. Alternatively, you can click the open menu button next to the **DEVICE GROUP NAME** and then click **Delete** in the menu. The device group is deleted from AvePoint Perimeter management system.

Configuring Site Access Permission for Enrolled Devices

To configure site access permission for previously created device groups, you must add the desired SharePoint sites as managed SharePoint sites into AvePoint Perimeter management system and then assign permission for these sites to the device groups.

Adding Managed SharePoint Sites

To add a new managed SharePoint site in **Site Access**, navigate to the **Manage** menu, and then click **Site Access** to enter the Site Access interface. Click **Add** on the ribbon, and then configure the following settings:

1. In the **Basic Information** section, select the **Site Type**, and then enter the **Site Display Name** and **Site URL/Site URL Prefix** for the managed SharePoint site to be added.
 - **Macro Site** assigns end-users permissions to access any sub-site under the same parent site while using the Perimeter app. To add a **Macro Site**, select the **Macro Site** checkbox and then complete the following settings:
 - **Site Display Name** – Enter a display name for the macro site to be added. This name will be displayed as the section name of the added sub-sites.
 - **Site URL Prefix** – Enter the desired parent site URL. This URL will be used as the prefix of the sub-site URL when the end-user adds a sub-site via the Perimeter app.

***Note:** If an end-user has been assigned permissions to a macro site and wants to access a particular sub-site under this macro site, the user should access the **Add a New Sub-Site** feature on the Perimeter app to configure the complete sub-site URL. To do this, enter the last part of the sub-site's URL after the **Site URL prefix**.
 - If you do not want to add a macro site, deselect the **Macro Site** checkbox and then enter the following:
 - **Site Display Name** – Enter a display name for the managed SharePoint site to be added.
 - **Site URL** – Enter the URL of the SharePoint site you want to add into the AvePoint Perimeter management system.

***Note:** You can only use the same **Site URL** for one managed SharePoint site.
2. In the **Authentication Mode** section, select the authentication method for this managed SharePoint site. **Automatic Authentication (Windows Classic Authentication or Form Based Authentication)** and **Web Login (Office 365 Authentication or ADFS Authentication)** are available for the **Authentication Mode**.
3. Click **Save** to save the configurations and add the managed SharePoint site into AvePoint Perimeter management system, or click **Cancel** to exit and go back to the **Site Access** interface without adding the managed SharePoint site.

Editing Managed SharePoint Sites

To edit a previously created managed SharePoint site, click **Edit** on the ribbon and then configure the following settings:

1. In the **Basic Information** section, select the **Site Type**, and then configure the **Site Display Name** and **Site URL/Site URL Prefix** for the managed SharePoint site you are editing.
 - If the site you are editing is a macro site, select the **Macro Site** checkbox and then configure the following settings:
 - **Site Display Name** – Enter a display name for the macro site you are editing.
 - **Site URL Prefix** – Enter the desired parent site URL.
 - If the site you are editing is not a macro site, deselect the **Macro Site** checkbox and then configure the following settings:
 - **Site Display Name** – Enter a display name for the managed SharePoint site you are editing.
 - **Site URL** – Enter the URL of the SharePoint site you want to add into AvePoint Perimeter management system.

***Note:** You can only use the same **Site URL** for one managed SharePoint site.
2. In the **Authentication Mode** section, select the authentication method for this managed SharePoint site. **Automatic Authentication (Windows Classic Authentication or Form Based Authentication)** and **Web Login (Office 365 Authentication or ADFS Authentication)** are available for the **Authentication Mode**.
3. Click **Save** to save the changes to the managed SharePoint site, or click **Cancel** to exit and go back to the **Site Access** interface without saving the changes.

Managing Site Access Permissions

After adding the managed SharePoint sites, you can navigate to the **Permission Assignment** interface to assign and manage site access permissions to the previously created device groups.

To access the **Permission Assignment** interface, select the corresponding checkbox of the desired managed SharePoint site in the **Site Access** interface and then click **Manage Permissions** on the ribbon. You will be brought to the **Permission Assignment** interface.

Assigning Site Access Permissions

To assign site access permissions to a previously created device group, click **Assign Permissions** on the ribbon. In the **Assign Permissions** interface, configure the following settings:

1. In the **Device Group Name** section, select the device group to which you want to assign the permission from the drop-down list.

2. In the **Permission Settings** section, choose the **Permission Level** and **Share Restriction** for the device group's permission.
 - **Permission Level** – Choose the permission level for reading SharePoint content.
 - **Online read only** – With this option selected, the users of the device group selected above can only access the SharePoint content online and cannot read the content using the stored offline data when disconnected to the Internet.
 - **Online and offline read** – With this option selected, the devices in the device group selected above can access SharePoint content both online and offline. When disconnected to the Internet, users can still read the offline data stored in the local device.
 - **Share Restriction** – Select the restrictions for sharing SharePoint content.
 - **Limited share** – With this option selected, the users of the device group selected above are restricted from sharing SharePoint content with others. They cannot perform the **E-mail Link**, **E-mail As Attachment**, and **Open In** actions on the SharePoint contents.

*Note: When Online read only is selected for Permission Level, this option is automatically selected and cannot be changed.
 - **Unlimited share** – With this option selected, the users of the device group selected above are allowed to share the SharePoint content with others.

They can perform the **Add to Favorites**, **E-mail Link**, **E-mail As Attachment**, and **Open In** actions on the SharePoint contents.
3. In the **Permission Expiration Time** section, specify when the permission you are about to assign to the device group will expire.
 - **Never expire** – This permission never expires.
 - **Expiration Time** – Select the expiration time from the calendar.
 - **Expire after** – Enter an integer in the text box and select **Days**, **Weeks**, **Months** or **Years** from the drop-down list. The permission will expire after this period.
4. **Assign Permission to Another Device Group**– Select whether to continue to assign permission to another device group.
 - If you select this option, click **Save** to save the configurations and assign permission to the selected device group. After the permission is successfully assigned, you can stay on the **Assign Permissions** page to assign permission to another device group.
 - If you do not select this option, click **Save** to save the configurations and assign permission to the selected device group. After the permission is successfully assigned, you will exit this page and go back to the **Manage Permissions** page.

If you don't want to assign permission to the selected device group, click **Cancel** to exit this page without assigning permission.

Editing Site Access Permissions

Here, you can control what users will see on their device and how/when content can be opened. To edit a previously assigned site access permission, select the corresponding checkbox in the **Permissions Assignment** interface, and click **Edit** on the ribbon. In the **Edit Permission** interface, configure the following settings:

1. In the **Permission Settings** section, select the **Permission Level** and **Share Restriction** for the device group's permission.
 - **Permission Level** – Select the permission level for reading SharePoint content.
 - **Online read only** – With this option selected, the users of the device group selected above can only access the SharePoint content online and cannot read the content using the stored offline data when disconnected to the Internet.
 - **Online and offline read** – With this option selected, the devices in the device group selected above can access SharePoint content both online and offline. When disconnected to the Internet, users can still read the offline data stored in the local device.
 - **Share Restriction** – Choose restrictions on sharing SharePoint content.
 - **Limited share** – With this option selected, the users of the device group selected above are restricted from sharing SharePoint content with others. They cannot perform the **Add to Favorites**, **E-mail Link**, **E-mail As Attachment**, and **Open In** actions on the SharePoint contents.

*Note: When Online read only is selected for Permission Level, this option is automatically selected and cannot be changed.
 - **Unlimited share** – With this option selected, the users of the device group selected above are allowed to share SharePoint content with others.

They can perform the **Add to Favorites**, **E-mail Link**, **E-mail As Attachment**, and **Open In** actions on the SharePoint contents.
2. In the **Permission Expiration Time** section, choose when the permission you are editing will expire.
 - **Never expire** – The permission never expires.
 - **Expiration Time** – Select the expiration time from the calendar.
 - **Expire after** – Enter an integer in the text box and select **Days**, **Weeks**, **Months** or **Years** from the drop-down list. The permission will expire after this period.
3. **Assign Permission to Another Device Group**– Select whether to continue to assign permission to another device group after saving the changes.
 - If you select this option, click **Save** to save the changes. After the permission is successfully updated, you can stay on the **Assign Permissions** page to assign permission to another device group.

- If you do not select this option, click **Save** to save the changes. After the permission is successfully updated, you will exit this page and go back to the **Manage Permissions** page.

If you don't want to save the changes to this permission, click **Cancel** to exit this page without saving the changes.

Removing Site Access Permissions

To remove previously created site access permissions for a particular device group, select the corresponding checkbox and click **Delete** on the ribbon. Alternatively, you can click the open menu button next to the **DEVICE GROUP NAME** and then click **Delete** in the menu.

Once the site access permission for a device group is deleted, the corresponding managed SharePoint site will be removed from the **SharePoint sites** list in the AvePoint Perimeter Mobile Apps on the devices in this device group, and the users will no longer be able to access the managed SharePoint site via the enrolled devices.

Configuring Content Access Control for SharePoint Content via Any Devices

To control SharePoint content access to your environment via any device, configure the Content Access Policy to create and configure the access control rules. This policy protects your SharePoint environment from potential security threats and information leaks. Prior to configuring the Content Access Policy, you must configure the location groups and locations for AvePoint Perimeter used by the Content Access Control rules in the Content Access Policy.

Configuring Location Groups

In **Manage Location Groups**, you can create and manage the location groups in which you can add multiple customized locations or geographic locations. These location groups can be used as filter conditions in the Content Access Policy rules to control content access. There are two types of location types in Perimeter:

- **User-defined Location Group** – Customized location groups consist of the locations you customized in **Manage Locations**, which involves manually inputting location information or selecting a location on the map.
- **Geographic Location Group** – Geographic location groups consist of the locations based on geo-political boundaries.

To access **Manage Location Groups**, navigate to the **Manage** menu and then click **Manage Location Groups**. In the **Manage Location Groups** interface, you can perform the following configurations:

Adding a New User-defined Location Group

To add a new location group, select a location group type by clicking **Add** on the ribbon. Select **User-defined Location Group** from the drop-down list to access the page for adding a new user-defined location group, and then complete the following settings:

1. In the **Basic Information** section, enter the name and an optional description for the location group you are about to create.
2. In the **Add Locations** section, select your desired customized locations from the **Add Locations to Group** drop-down list.
3. Click **Save** to add the location group and go back to the **Manage Location Groups** interface, or click **Cancel** to exit this page without saving the configurations.

Adding a New Geographic Location Group

With a populated Geolocation database, you can configure geographic location groups based on geographic and political boundaries. To add a new geographic location group, select a location group type by clicking **Add** on the ribbon. Select **Geographic Location Group** from the drop-down list, and then complete the following settings:

1. In the **Basic Information** section, enter the name and an optional description for the location group you are about to create.
2. In the **Add Location** section, select your desired geographic locations by selecting the corresponding **Region** and **District** from the drop-down lists.
3. Click **Save** to add the location group and go back to the **Manage Location Groups** interface, or click **Cancel** to exit this page without saving the configurations.

Editing Location Groups

To edit a previously added location group, configure the following settings:

1. Select the corresponding checkbox in the **LOCATION GROUP NAME** column
2. Click **Edit** on the ribbon.
3. In the page for editing the selected location group, refer to [Adding a New User-defined Location Group](#) and [Adding a New Geographic Location Group](#).
4. When you finish editing the location group, click **Save** to save the modifications and go back to the **Manage Location Groups** interface, or click **Cancel** to exit this page without saving the modifications.

Deleting Location Groups

To delete previously-added location groups, select the corresponding checkboxes in the **LOCATION GROUP NAME** column and then click **Delete** on the ribbon.

Configuring Locations

In **Manage Locations**, you can create and manage locations and location parameters used to control content access. To access **Manage Locations**, navigate to the **Manage** menu and click **Manage Location**. In the **Manage Locations** interface, you can perform the following configurations:

Adding New Locations

To add new locations, complete the following steps:

1. Click **Add** on the ribbon.
2. **Location Name** – Enter a name for the location you want to add.
3. **Location Group**– Select the groups from the drop-down list to add this location.
4. **Create Method**– Select a method for creating this location.
 - **Manually Input Coordinates**– Select this option to configure the required location information by manually inputting the coordinates.
 - **Address** – Enter the physical address of this location you are about to create for future reference.
 - **Latitude** – Enter the latitude of the central point of this location.
 - **Longitude** –Enter the longitude of the central point of this location.
 - **Radius Distance** –Specify the **Radius Distance** for the location you want to add. Enter an integer in the text box and select the unit for the drop-down list. The location to be added will cover the circle with this radius distance around the central point specified above.
 - **Pick up location from map** – Select this option to pick up the location from Bing Maps. Click **Open map** and complete the following settings to pick a location in the **Pick up location from map** pop-up window.
 - i. Choose the central point for the location you want to add. You can do this in the following three ways:
 - Click on a desired point on the Bing Maps to set a central point.
 - Enter a place name in the **Search Location** box to search for the place that you want to use as the central point.
 - Click **My Current Location** to set your current physical location as the central point.

Once the central point is set on the Bing Maps, you can view the coordinates for this central point in the **Latitude** and **Longitude** fields.
 - ii. Specify the **Radius Distance** for the location you want to add. Enter an integer in the text box and select the unit for the drop-down list. The location to be added

will cover the circle with this radius distance around the central point specified in the previous step.

- iii. Click **Save** to save the configuration or click **Cancel** to exit this pop-up window without saving the configurations.
 - iv. **Address** – Enter the real address of this location you are about to create for future reference.
5. Click **Save** to add the location or click **Cancel** to exit the page for adding a new location without saving the configurations.

Once the location is successfully added, you can view the newly-created location in the **Manage Locations** interface.

Editing Locations

To edit a previously-added location, configure the following settings:

1. Select the corresponding checkbox in the **LOCATION NAME** list.
2. In the **View Details** page, click **Edit** on the ribbon.
3. Enter a name for the location you are editing in the **Location Name** textbox.
4. **Location Group**– Select the groups from the drop-down list to add this location.
5. **Create Method**– Select a **Create Method** for the location you are editing.
 - **Manually Input Coordinates**– Select this option to configure the required location information by manually inputting the following information:
 - **Address** – Enter the physical address of this location for future reference.
 - **Latitude** – Enter the latitude of the central point of this location.
 - **Longitude** –Enter the longitude of the central point of this location.
 - **Radius Distance** –Specify the **Radius Distance** for the location you want to add. Enter an integer in the text box and select the unit from the drop-down list. The location to be added will cover the circle with this radius distance around the central point specified above.
 - **Pick up location from map** – Select this option to pick up the location from the Bing Maps. Click **Open map** and complete the following settings to pick a location in the **Pick up location from map** pop-up window.
 - i. Choose the central point for the location you are editing. You can do this in the following three ways:
 - Click on a desired point on the Bing Maps to set a central point.
 - Enter a place name in the **Search Location** box to search for the place that you want to use as the central point.

- Click **My Current Location** to set your current physical location as the central point.

Once the central point is set on the Bing Maps, you can view the coordinates for this central point in the **Latitude** and **Longitude** fields.

- ii. Specify the **Radius Distance** for the location you are editing. Enter an integer in the text box and select the unit from the drop-down list. The location you are editing will cover the circle with this radius distance around the central point specified in the previous step.
- iii. Click **Save** to save the changes to this location or click **Cancel** to exit the pop-up window for editing a location without saving the changes.
- iv. **Address** – Enter the real address of this location you are editing for future reference.

Click **Save** to save the changes to this location or click **Cancel** to exit the page for editing a location without saving the changes.

Deleting Locations

To delete a previously-added location, select the corresponding checkbox for the desired location in the **Manage Locations** interface and then click **Delete** on the ribbon.

Applying the Bing® Maps Key

If you want to use Bing Maps to detect location, a Bing Maps key is required. To request a Bing Maps Key, go to the [Create a Bing Maps Key](#) page.

To authenticate AvePoint Perimeter using Bing Maps Key, complete the following steps:

1. From within the Perimeter Manager, navigate to **Manage > Manage Locations**.
2. Click **Add** to add a new location.
3. In the Location Settings section, select **Pick up Location from map**, and click **Open map**. The **Pick up location form map** window appears.
4. Click **Configure Bing Maps Key** on the ribbon. The **Configure the Bing Maps Key** pop-up window appears.
5. In the **Configure the Bing Maps Key** pop-up window, enter your Bing Maps key into the text box.
6. Click **Save** to save the configuration.
7. Refresh the page to have the Bing Maps key take effect.

Configuring Content Access Policies

With locations configured in **Manage Locations and Manage Location Groups**, you can start to configure the Content Access Policy for SharePoint On-Premises and Active Directory Federation Services (ADFS) by using the **SharePoint Policy** and **Federation Policy** features.

Configuring a SharePoint Policy

To access **SharePoint Policy**, navigate to the **Manage** menu and then click **Content Access Policy**.

In the **SharePoint Policy** interface, you must first configure the Content Access Policy rules for your SharePoint On-Premises farms at the zone level. Perimeter provides four Content Access Policy features for the zone level: **2-Factor Authentication**, **Content Access Control**, **Content Access Logging** and **Web Services Blocking**. By default, the configurations at the zone level will be applied to all of the nodes under the zone.

If the **Content Access Control** feature is enabled for a particular zone, you can continue to configure the **Content Access Control** rules for the site collections below this zone individually.

Configuring SharePoint Policy Rules at Zone Level

To configure the Content Access Policy rules at zone level, expand the scope tree to the zone level, select the zone by clicking the corresponding option button and then click **Configure** to access the interface for configuring the **Content Access Policy** features for this zone.

You can configure the features for this zone by completing the following steps:

1. Select the features you want to configure for this zone by selecting the corresponding checkboxes and then click **Next** to configure the selected features.
2. Configure the rules for the features selected in the previous step. Refer to the section below to configure the following four features:

- **Configure settings for 2-Factor Authentication** – 2-Factor Authentication is a security process by which users provide two means of identification to access the SharePoint sites, one of which is the organization password and the other the access password generated by the enrolled device. If you activate this feature for a zone without configuring any 2-factor authentication rules, all visitors must authenticate to the sites within this zone using both the organization credentials and the access passwords generated by the enrolled devices. The default timeout period for 2-Factor authentication to the sites within this zone is 60 minutes. Users will be required to re-authenticate the access password to the site if there is no activity for 60 minutes from the last authentication time. If desired, you can configure your desired time out period in the **Configure a Timeout Period for 2-Factor Authentication** area of the **2-Factor Authentication** interface.

To allow specific users/groups to authenticate to this zone using any devices, you can configure rules to allow them to generate access password via the browser. To configure

the rules, complete the following steps in the **Rule Settings for 2-Factor Authentication** section:

- i. Click **Add a Rule** to configure a new rule.
- ii. **User** – Enter the user/group to receive the new rule.
- iii. **Allow User's Brower to Generate Access Password** – Choose whether to allow the specified user/group to generate an access password using any browser.

***Note:** To track the location of users/groups who are allowed to generate access password using browsers, AvePoint strongly recommends that the users turn on their browsers' location services to enable AvePoint Perimeter to track their physical location via the browser.

- To enable location services on Internet Explorer, ensure that the **Never allow websites to request your physical location** option in the **Privacy** tab of **Internet Options** is unselected.
- To enable the location service on Chrome, ensure the Ask me when a site tries to track my physical location (recommended) or Allow all sites to track my physical location option is selected.

- iv. **Description** – Enter an optional description for this rule.
- v. After configuring one rule, click **Add a Rule** to add another rule, or click the **Delete** button to delete the rule.

***Note:** If 2 or more rules are configured, configure the **Priority** of these rules. If the user/group who is trying to access the SharePoint sites meets the criteria in multiple rules, Perimeter will only apply the rule with the highest priority.
- vi. Click **Next** to save the configurations and continue to configure the next feature.

- **Rules for Content Access Control – Content Access Control** is used to control SharePoint access based on a user's username, access point's, platform and device model, and location information. If you activate this feature for a zone without configuring any Content Access Control rules, access to this zone is allowed for all users. Follow the steps below to configure the Content Access Control rules:

- i. Click **Add a Rule** to configure a new rule.
- ii. Specify the **Platform**, **Model**, **Location type**, **Location**, and **User** of the access attempts to which this rule is applied.
- iii. **Action** – Choose the action to control access to the SharePoint sites in this zone. You have the following options:
 - **Allow** – Allow the access to the SharePoint sites within this zone.
 - **Warning** – Prompt a warning message before the user login the SharePoint sites within this zone.

- **Block** – Block the access to the SharePoint sites within this zone.
 - iv. **Description** – Enter an optional description for this rule.
 - v. After configuring one rule, click **Add a Rule** to add another rule, or click the **Delete** button to delete the rule.
 - *Note:** If 2 or more rules are configured, configure the **Priority** of these rules. If the access attempt to the SharePoint sites meets the criteria in multiple rules, Perimeter will only apply the rule with the highest priority.
 - vi. Click **Next** to save the configurations and continue to configure the next feature.
- **Rule Settings for Content Access Logging**– Use **Content Access Logging** to choose whether or not to log users who access the selected URLs. If you activate this feature for a zone without configuring any Content Access Logging rules, all users who access sites within this zone are logged. Follow the steps below to configure the rules:
 - i. Click **Add a Rule** to configure a new rule.
 - ii. Enter the criterion for the URLs to which this rule is applied by filling in the **Condition** and **Value** fields.
 - iii. **Action** – Choose whether or not to log users who access the ULRs that meet the criterion configured in the previous step.
 - iv. **Description** – Enter an optional description for this rule.
 - v. After configuring one rule, click **Add a Rule** to add another rule, or click the **Delete** button to delete the rule.
 - *Note:** If 2 or more rules are configured, configure the **Priority** of these rules. If a URL meets the criteria in multiple rules, Perimeter will only apply the rule with the highest priority.
 - vi. Click **Next** to save the configurations and continue to configure the next feature.
 - **Rule Settings for Web Services Blocking** – Use **Block Web Services** to block the user clients from accessing SharePoint Web Services. If you activate this feature for a zone without configuring any rules, all access to SharePoint Web Services is blocked. You can configure rules to allow user clients access to SharePoint Web Services. Follow the steps below to configure the rules:
 - i. Click **Add a Rule** to configure a new rule.
 - ii. Enter the criterion for the user clients' **User Agent** to which this rule is applied by filling in the **Condition** and **Value** fields.
 - iii. **Action** – Choose to block or allow the user clients access.
 - iv. **Description** – Enter an optional description for this rule.

- v. After configuring one rule, click **Add a Rule** to add another rule, or click the **Delete** button to delete the rule.

***Note:** If 2 or more rules are configured, configure the **Priority** of these rules. If a user client meets the criteria in multiple rules, Perimeter will only apply the rule with the highest priority.

3. Click **Finish** to save the configurations and go back to the **SharePoint Policy** interface, click **Back** to change any of the previous configurations, or click **Cancel** to abandon all configurations and exit the interface for configuring the **Content Access Policy** features.

Configuring Content Access Control Rules at Site Collection Level

After the Content Access Control feature is configured for a Web application zone, the configurations at the zone level will be applied to all of the nodes under the zone. You can continue to configure the Content Access Control rules for individual site collections in the zone. When creating rules, be aware that the order the rules are in dictates the rule priority.

Prior to configuring Content Access Control rules for a site collection, you must ensure the Content Access Control feature has been configured for the zone where this site collection resides. To configure Content Access Control rules for a site collection, expand the scope tree to the site collection node, click **Content Access Control** in the **Feature** pane to enter the **Rules for Content Access Control** interface, and then complete the following steps to configure the rules for this feature:

1. Click **Add a Rule** to configure a new rule.
2. Specify the **Platform**, **Model**, **Location Type**, **Location**, and **User** of the access attempts to which this rule is applied.
3. **Action** – Choose the action for access to this site collection. You have the following options:
 - **Allow** – Allow the access to this site collection.
 - **Warning** – Prompt a warning message before the user logs into this site collection.
 - **Block** – Block the access to this site collection.
4. **Description** – Enter an optional description for this rule.
5. After configuring a rule, click **Add a Rule** to add another rule, or click the **Delete** button to delete the rule.

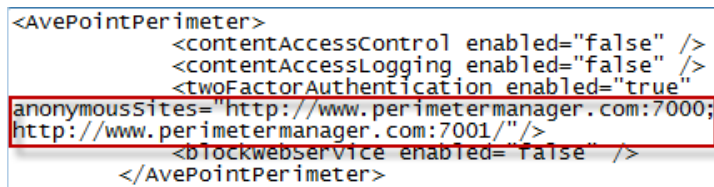
***Note:** If 2 or more rules are configured, configure the **Priority** of these rules. If the access attempt to the SharePoint sites meets the criteria in multiple rules, Perimeter will only apply the rule with the highest priority.

Click **Save** to save the configurations and go back to the **SharePoint Policy** interface, or click **Cancel** to abandon the configurations and exit this interface.

Configuring 2-Factor Authentication for the SharePoint Objects Allowing Anonymous Authentication

If a SharePoint object allows anonymous access, the 2-Factor Authentication feature (by default) does not take effect on users who anonymously access this object. You can enable the 2-Factor Authentication feature for those objects that allow anonymous access at the **Web application zone/site collection/site/list/item** level by making some additional configurations. To make the 2-Factor Authentication feature work properly for those objects you must first enable the 2-Factor Authentication feature for the Web application zone where the objects reside, and then configure the SharePoint zone's **Web.config** file by completing the following steps:

1. With the 2-Factor Authentication feature enabled for the Web application zone where the objects reside, navigate to the physical path of the zone's IIS website and open the **Web.config** file with Notepad.
2. Locate the **<twoFactorAuthentication>** node.
3. Add the URLs of the objects into the value for "anonymousSites" as shown in the screenshot below:



```
<AvePointPerimeter>
  <contentAccessControl enabled="false" />
  <contentAccessLogging enabled="false" />
  <twoFactorAuthentication enabled="true"
  anonymousSites="http://www.perimetermanager.com:7000;
  http://www.perimetermanager.com:7001/" />
  <blockwebservice enabled="false" />
</AvePointPerimeter>
```

Figure 7: Configuring the <twoFactorAuthentication> node in the Web.config file.

***Note:** You can add multiple URLs in the node by separating them with a semicolon.

Save the modification and close the file. The 2-Factor Authentication will now work properly on these objects. The visitors must provide the access password in the **Authentication** page to authenticate the objects.

Viewing and Managing Agent Status for Content Access Policy Features

If you have configured a Content Access Policy feature for a Web application zone, this feature will be enabled on each AvePoint Perimeter Agent for this zone. You can view the **Agent Status** for each Content Access Policy feature on the zone's AvePoint Perimeter Agents.

To view and manage the Agent status for Content Access Policy features on a zone, complete the following steps:

1. Select the desired zone on the scope tree by clicking the corresponding checkbox and hover the cursor over **Agent Status** on the ribbon to load the drop-down list for the four features.
2. Click on the feature name for which the Agent status you want to view and manage. Then you will be brought to the **Agent Status** interface.

3. In the **Agent Status** interface, you can view the **Agent Name** of each Agent for the selected zone and the status of the selected feature on this Agent.
4. You can manage the Agent status with the following options:
 - **Deactivate** – If the status for a feature is **Active** on an Agent, you can deactivate this feature by clicking **Deactivate** on the ribbon. The status becomes **Inactive**, and this feature on the Agent is deactivated.
 - **Activate** – If the status for a feature is **Inactive** on an Agent, you can activate this feature by clicking **Activate** on the ribbon. The status becomes **Active**.

Configuring the Federation Policy

The **Federation Policy** provides **2-Factor Authentication** and **Authentication Control** for your Active Directory Federation Services (ADFS) authentication process.

To access **Federation Policy**, follow the steps below:

1. Navigate to the **Manage** menu and then click **Federation Policy**. In the **Federation Policy** interface, you can configure **2-Factor Authentication** and **Authentication Control** rules for your ADFS servers at the relying party level.
 2. To configure the Federation Policy for a relying party, complete the following steps:
 3. Expand the scope tree to the relying party level and select the desired relying party by selecting the corresponding option button.
 4. Click **Configure** on the ribbon.
 5. In the **Enable Federation Policy** section, select whether to enable the Federation Policy features for this relying party. When you select **Enable**, the 2-Factor Authentication and Authentication Control features are enabled for this relying party.
 - **Rules Settings for Rules for 2-Factor Authentication** –If you activate this feature for a relying party without configuring any 2-factor authentication rules, all visitors must provide both the organization credentials and the access passwords generated by the enrolled devices during the authentication process for this replying party. To allow users/groups to authenticate to this relying party using any devices, you can configure rules to allow them to generate access password via a browser. To configure the rules, complete the following steps:
 - i. Click **Add a Rule** to configure a new rule.
 - ii. Enter the **Claim Name** and **Claim Value** configured in this relying party's Issuance Transform Rules on the ADFS server to filter the users or groups who are allowed to or restricted from generate access password via using browsers via any device.
- *Note:** Wildcards ? and * are supported in the **Claim Value** text box. ? stands for any single character, and *stands for the character string of any length. If the

desired claim value contains ?, *, or /, add an escape character \ before the ?, *, or /.

- iii. **Allow User's Browser to Generate Access Password** – Choose whether to allow the specified user/group to generate an access password using any registered device's browser.

***Note:** To track the physical location of users/groups who are allowed to generate access password using browsers, users must turn on their browser location services.

- iv. **Description** – Enter an optional description for this rule.

- v. After configuring one rule, click **Add a Rule** to add another rule, or click the **Delete** button to delete the rule.

***Note:** If 2 or more rules are configured, configure the **Priority** of these rules. If a user who is trying to access this relying party meets the criteria in multiple rules, Perimeter will only apply the rule with the highest priority.

- **Rule Settings for Authentication Control** – This feature provides additional authentication control after the 2-Factor Authentication process for this relying party based on the access point's platform, device model and location, and the used account's claim name and claim value of the access attempt. If you activate this feature for the relying party without configuring any Authentication Control rules, all access attempts that pass the 2-factor authentication to this relying party will be allowed. You can configure rules to control access to this relying party by blocking or allowing particular access attempts based on the criteria. Follow the steps below to configure the Authentication Control rules:

- i. Click **Add a Rule** to configure a new rule.
- ii. Specify the **Platform, Model, Location Type, Location, Claim Name, and Claim Value** of the access attempts to which this rule is applied.
- iii. **Action** – Choose to **Allow** or **Block** access attempts by this relying party.
- iv. **Description** – Enter an optional description for this rule.
- v. After configuring one rule, click **Add a Rule** to add another rule, or click the **Delete** button to delete the rule.

***Note:** If 2 or more rules are configured, configure the **Priority** of these rules. If a user who is trying to access this relying party meets the criteria in multiple rules, Perimeter will only apply the rule with the highest priority.

- 6. Click Save to save the configurations and go back to the **Federation Policy** interface.

Managing Internal Users

Internal users are considered Active Directory end-users who belong to the same Active Directory domain with the SharePoint farms where the Perimeter management system is deployed.

In **Manage Internal Users**, you can view the detailed information of all of the registered internal users in this Perimeter management system, synchronize the Active Directory users into the management system and send an enrollment request to a particular user.

To access **Manager Internal Users**, navigate to the **Manage** menu, and then click **Manage Internal Users**. In **Manage Internal Users**, you can view a list of the user information collected when the internal end-users enroll their mobile devices, access the SharePoint sites managed by the Content Access Policy features, use the AvePoint Perimeter Pro Secured Share feature to share files, folders, and libraries with others from SharePoint sites, and when the administrators configure the Active Directory users as criteria for Content Access Policy rules. The user information in the **Manage Internal Users** interface includes the username, e-mail address, the number of enrolled devices, the last time when this user shared SharePoint objects through the AvePoint Perimeter Secured Share feature, location name, and the coordinates of the user's last location.

Viewing User Details

To view the detailed information of a particular user, click the desired username in the **Manage Users** interface to enter the **User Details** page. In the **Basic Information** tab, you can view the user's general information in the Active Directory and the latest location information of the enrolled device or browser used to access SharePoint sites managed by this management system. In the **Location History** tab, you can view the location data of all of the enrolled devices or browsers used by this user to access SharePoint sites managed by this management system.

In the **Mange Users** interface, you can also perform the following operations:

- **View device details of a specified user** – To view the detail information of the enrolled devices belonging to a particular user, click the link in the **Enrolled Devices** column to enter the **Manage Enrolled Devices** interface. The enrolled devices belonging to the user are listed. View and manage the enrolled devices by referring to [Managing Enrolled Devices](#).
- **Send enrollment request to a specified user** – To send an enrollment request to a selected user in the list, select the desired user by clicking the corresponding checkbox and then click **Enroll New Device** on the ribbon. Alternatively, you can click the open menu button next to the username and click **Enroll** in the menu. Then you will be brought to the **Enroll New Device** interface to configure a new enrollment request send to this user. Refer to [Sending an Individual Device Enrollment Request](#) for more information.

Synchronizing Active Directory Users

To synchronize Active Directory users into AvePoint Perimeter management system, click **Synchronize AD users** on the ribbon to enter the **Synchronize Active Directory Users** interface and complete the following steps:

1. **Domain Controller Address** – Enter the address of the domain controller of the LDAP directory from where you want to synchronize the Active Directory users.
2. **Username** – Enter the username of the Active Directory account you want to use to synchronize the Active Directory users. Make sure that the account specified here have read permission in your corporate directory. The Perimeter Agent will use this account when authenticating to the **cooperate** directory.
3. **Password** – Enter the **password** for the account specified above.
4. **Domain Scope** – Choose the domain scope from which the Active Directory user will be synchronized into AvePoint Perimeter management system.
 - **Import users from all domains in the same forest and the trusted domains** – Select this option to import the Active Directory users from all domains in the same forest and the trusted domains
 - **Configure the search roots list myself** – Select this option to configure which users will be synchronized using the LDAP Distinguished Names (DN).
5. **Schedule Settings** – In the **Schedule Settings** section, choose one of the following options:
 - **Synchronize immediately** – With this option selected, the synchronization job will be initiated immediately when you click **Save**.
 - **Configure a schedule** – With this option selected, you can configure the schedule for synchronizing the Active Directory users as follows:
 - **Schedule Type** – Select the interval at which the synchronization job runs: **By hour**, **By day**, **By week**, or **By month**.
 - **Interval** – Set up the frequency for the schedule by entering an integer in the text box.
 - **Start Time** – Specify the time of the day when Perimeter starts to synchronize the Active Directory users. If you select **By month**, configure the **Specify the start time by day of the week** and **Specify the start time by date** fields. For more information, see the [Configuring Advanced Start Time Settings](#) section.
6. Click **Save** to save the configurations and go back to the **Manage Users** interface. Click **Cancel** to abandon the configurations and exit the **Synchronize Active Directory Users** interface.

Managing External Users

External users are end-users who are outside your organization's Active Directory domain. Perimeter administrator can add external users through Perimeter Management Console, or external users can

manually register to the Perimeter management system by registering to the AvePoint Perimeter External Portal or enrolling their mobile devices. In **Manage External Users**, you can view the information Perimeter collects when the external users register to the AvePoint Perimeter External Portal, enroll their mobile devices to this AvePoint Perimeter management system, and use the Perimeter apps on their mobile devices.

To access **Manage External Users**, navigate to the **Manage** menu, and then click **Manage External Users**. In **Manage External Users**, you can view a list of the external users who have been added or have registered to the AvePoint Perimeter External Portal or enrolled their mobile devices into the AvePoint Perimeter management system. The user information in the **Manage External Users** interface includes the username, e-mail address, number of enrolled devices of each user, the information of the user's last location collected by the Perimeter mobile apps, and the user's status.

Adding External Users

In the **Manage External Users** interface of AvePoint Perimeter Manager, you can manually add an external user individually or add external users in bulk by importing a CSV file that contains all of the external users. To access the interface to manage external users, navigate to **Manage > Users/Accounts > Manage External Users**. Refer to the instructions below for adding an external user individually or adding external users in bulk.

Adding an External User Individually

Complete the steps below to add an individual external user.

1. In the **Manage External Users** interface, click **Add** on the ribbon and then select **Add User** from the drop-down list. The **Add** interface appears.
2. **Basic Information** – Enter the username, e-mail address, and the first name and last name of the external user that you want to add. All of the **Basic Information** fields are mandatory fields.
3. **Contact Information** – The settings in this section are optional. You can enter the **Phone Number**, **Country/Region**, **Organization**, **City**, and **Postal Code** for this external user.
4. **Custom Properties Information** – Enter the custom property information for this external user as needed.
5. Click **Save** to save this external user, or click **Cancel** to exit this interface.

Adding External Users in Bulk

Complete the steps below to add external users in bulk via a predefined CSV file.

1. In the **Manage External Users** interface, click **Add** on the ribbon and then select **Bulk Add** from the drop-down list. The **Bulk Add** interface appears.
2. In the **Step 1** field, click **Download the template** link to download a template file for adding external users in bulk.

3. The **Save As** window appears. Browse a location to store the template file. Click **Save**.
4. Open the template file using Excel. There are four mandatory columns:
 - **UserName** – Enter the User ID of the external user that you want to add.
 - **Email Address** – Enter the external user's e-mail address next to the User ID. When entering the e-mail address, follow the e-mail address format: **username@domain.com**.
 - **FirstName** – Enter user's first name.
 - **LastName** – Enter user's last name.
5. Enter the username, e-mail address, first name, last name, and the other optional user information into the template file.
6. Save the CSV file.
7. In the **Step 2** field, click the **Browse** button. Select the configured CSV file that contains all of the external users that you want to add in bulk. Click **Open**.
8. Click **Apply** on the ribbon to import the external users into AvePoint Perimeter Manager. After the import is complete, the **Manage External Users** interface will display for you to view the external users. The **Status** of the newly added external users will be **Pending Registration** before they sign up to the Perimeter External Portal.

Viewing User Details

To view the detailed information of an external user, click the desired username in the **Manage External Users** interface to enter the **User Details** page.

- In the **Basic Information** tab, you can view the user's general information configured when the user registered to the AvePoint Perimeter External Portal and the latest location information of the enrolled device.
- In the **Location History** tab, you can view the location data collected by the Perimeter mobile apps on the user's enrolled devices.

To view the detailed information of the enrolled devices belonging to an external user, click the link in the **Enrolled Devices** column to enter the **Manage Enrolled Devices** interface. The enrolled devices belonging to the external user are listed. View and manage the enrolled devices by referring to [Managing Enrolled Devices](#).

Editing an External User Profile

To edit the profile of a specific external user, complete the following steps:

1. Select the desired user by selecting the checkbox next to the username and clicking **Edit Profile** on the ribbon to access the Edit Profile page of the selected user.
2. In the **Edit Profile** page, you can edit the following information of the user:

- **Basic Information** – Edit the **First Name** and **Last Name** of the selected user.
 - **Contact Information** – Edit the phone number, address information, and postal code of the selected user.
 - **Custom Properties Information** – Edit the custom properties of the selected user configured in the **SecureShareConfig.xml** file in the **bin\Config** folder under the installation path of the AvePoint Perimeter Manager.
3. When you finish editing the profile of the selected user, click **Save** to save the modifications and return to the **Manager External Users** interface. Click **Cancel** to exit this page without saving the modifications.

Managing the Status of External Users

To manage the status of an external user, you can perform the following actions:

Disabling an External User

When the **STATUS** of an external user is **Active**, the **Disable** option is available on the ribbon. A disabled user cannot log into the AvePoint Perimeter External Portal or run the Perimeter app on an enrolled mobile device. To disable an external user, follow the steps below:

1. Select the desired external user by selecting the checkbox next to the corresponding **USERNAME**.
2. Click **Disable** on the ribbon.
3. Once the **Disable** action is completed, the **STATUS** of the user becomes **Disabled**.

Enabling an External User

To allow a **Disabled** external user to log into the AvePoint Perimeter External Portal and use the Perimeter mobile app on an enrolled device, you need to enable the user. To enable an external user, complete the following steps:

1. Select the desired external user by selecting the checkbox next to the corresponding **USERNAME**.
2. Click **Enable** on the ribbon.

Once the **Enable** action is completed, the **STATUS** of the user becomes **Active**.

Deleting an External User

To delete an external user from the AvePoint Perimeter management system, select the corresponding checkbox of the user you want to delete and click **Delete** on the ribbon.

Resending Activation E-mails

Using the **Resend Activation E-mail** feature, you can resend an **AvePoint Perimeter External Portal - Account Activation** e-mail to a user who requests a new activation e-mail for activating AvePoint Perimeter External Portal account. A user might need a new activation e-mail in either of the following situations:

- After submitting the **Account Registration** information for AvePoint Perimeter External Portal, the user does not receive an **AvePoint Perimeter External Portal - Account Activation** e-mail.
- The user received the **AvePoint Perimeter External Portal - Account Activation** e-mail, but the activation URL in the received e-mail expires.

To resend the **AvePoint Perimeter External Portal - Account Activation** e-mail to particular users, complete the following steps:

1. Select the corresponding checkboxes of the desired users.
2. Click **Resend Activation E-mail**. A confirmation window appears.
3. Click **OK** to resend the activation e-mails to the selected users.

Activating an External User

If an external user has signed up to the Perimeter External Portal but this user has not yet activated the account, the Perimeter administrator can activate the user account through the Management Console as well as resend the activation e-mail to the external user.

To activate the external user accounts that have been signed up in the Perimeter External Portal but are pending activation, complete the steps below:

1. Select an external user account that is in the **Pending** status.
2. Click **Activate** on the ribbon. A confirmation window appears.
3. Click **OK** to activate the user account. The external user will not receive notification of the account activation through the Perimeter Management Console.

Managing Login Accounts

In the **Manage Login Accounts** interface, you can view information on each account that logs into sites that are controlled by this Perimeter management system. An end-user of AvePoint Perimeter may use different login names to log into sites with different authentication methods, such as Windows Authentication and Claims Bases Authentication. You can assign this end-user multiple login accounts.

To access **Manage Login Account**, navigate to the **Manage** menu, and then click **Manage Login Accounts**. In the Manage Login Accounts interface, you can view a list of account information collected

when they login the sites controlled by this management system. The account information in this interface includes this account's **Login Name**, the accessed site's **Application Type** and **Application URL**, the access point's **Last Location**, **Last Region**, and **Last District**, and the **User** that is assigned to the account.

Viewing Login Account Details

To view the detailed information of a login account, click the desired **LOGIN NAME** in the **Manage Login Accounts** interface to enter the **Login Account Details** page.

- In the **Basic Information** tab, you can view the following information on the account:
 - **General Information** – Displays this account's general information in the Active Directory.
 - **Location Information** – Displays the latest location information of the enrolled device or browser used to access the sites managed by this management system.
 - **Account Claims Information** – Displays this account's Claims information used for Claims Based Authentication.

***Note:** This section is available when the account is used to authenticate to a Claims Bases Authentication site.
- In the **Location History** tab, you can view the location data of all of the enrolled devices or browsers used by this user to access the sites managed by this management system.

Assigning a User for Login Accounts

To assign a user for a particular login account, click **Assign User** on the ribbon to access the **Assign User for Login Account** page and then complete the following steps:

1. In the **Select a User** search box, enter the keyword of the username of the desired end-user you want to assign for the selected login accounts.
2. Select the desired user by clicking the matched results in the drop-down list.
3. Click **Save** on the ribbon to assign the selected user for this login account and go back to the **Manage Login Accounts** interface, or click **Cancel** to exit this page without assigning the selected user.

Sharing Files with Groups of Users via Virtual Views

To share a set of SharePoint files based on predefined criteria with a group of users in bulk, create user access groups containing both internal users and external users in **Manage User Access Groups**, create virtual views of SharePoint files, and then assign permissions to the user access groups in **Virtual Views**.

Managing User Access Groups

In **Manage User Access Groups**, you can create and manage user access groups based on predefined parameters. User access groups can be dynamic or static, and are primarily used to assign shared permissions to the SharePoint files in virtual views. To access **Manage User Access Groups**, navigate to the **Manage** menu and click **Manage User Access Groups** to enter the **Manage User Access Groups** interface.

Add New User Access Groups

To add a new user access group, complete the following steps:

1. Click **Add** on the ribbon to enter the **New User Access Group** interface.
2. In the **Basic Information** section, enter the user access group name, an optional description, and the type for the user access group to be created.
 - **User Access Name** – Enter a name for the user access group to be created.
 - **Description** – Enter an optional **Description** for the group for future reference.
 - **Type** – Select the type of the user access group to be created.
 - **Dynamic** – If you select this option, Perimeter will automatically add the new users that meet the rules configured below after the user access group is created.
 - **Static** – If you select this option, Perimeter will not automatically check for new users after the user access group is created. The users in this group will not be added automatically.
3. In the **Rule Settings** section, configure the rules for adding users into the user access group.
 - After configuring a rule, click **Add a Rule** to add another rule, or click **Remove** following each rule to delete the rule.
 - If 2 or more rules are configured, determine the logical relationship in the **Conditions** text box. There are two logic choices: **And** and **Or**. The default logic is **And**.
 - **And** – Users that meet all of the rules will be added into the user access group.
 - **Or** – Users that meet any one of the rules will be added into the user access group.

***Note:** You must ensure that each internal user you add into this user access group has an e-mail address configured in the Active Directory Domain Controller. Otherwise, the internal users will not receive e-mail notifications for shared virtual views that are shared with this user access group.
4. Click **Preview Filter Results** to preview the users that meet the configured rules.
5. Click **Save** to save the configurations and add the user access group, or click **Cancel** to exit this interface without adding the user access group.

Editing User Access Groups

To edit a previously created user access group, complete the following steps:

1. Select the corresponding checkbox next to the desired user access group and click **Edit** on the ribbon to access the **Edit User Access Group** page.
2. In the **Basic Information** section, enter the user access group name, an optional description, and the type for the user access group you are editing.
 - **User Access Name** – Enter a name for the user access group you are editing.
 - **Description** – Enter an optional **Description** for the group for future reference.
 - **Type** – Select the type of the user access group you are editing.
 - **Dynamic** – If you select this option, Perimeter will automatically add the new users that meet the rules configured below after the user access group is created.
 - **Static** – If you select this option, Perimeter will not check for the new users that meet the rules configured below after the user access group is created. The users in this group will not be added automatically.
3. In the **Rule Settings** section, configure the rules for adding users into the user access group.
 - After configuring one rule, click **Add a Rule** to add another rule, or click **Remove** following each rule to delete the rule.
 - If 2 or more rules are configured, determine the logical relationship in the **Conditions** text box. There are two logics choices: **And** and **Or**. The default logic is **And**.
 - **And** – Users that meet all of the rules will be added into the device group.
 - **Or** – Users that meet any one of the rules will be added into the device group.

***Note:** You must ensure that each internal user you add into this user access group has an e-mail address configured in the Active Directory Domain Controller. Otherwise, the internal users will not receive e-mail notifications for shared virtual views that are shared with this user access group.

4. Click **Preview Filter Results** to preview the users that meet the configured rules.
5. Click **Save** to save the configurations to the user access group, or click **Cancel** to exit this interface without editing the user access group.

Deleting User Access Groups

To delete a previously created user access group, select the corresponding checkbox and click **Delete** on the ribbon. Alternatively, you can click the open menu button next to the **USER ACCESS GROUP NAME** and then click **Delete** in the menu. Then the user access group is deleted from AvePoint Perimeter management system.

Viewing Users of a User Access Group

To view the users included in a user access group in the **Manage User Access Groups** interface, click the open menu (***) button of the desired user access group, and then click **View All Users** in the menu. A pop-up window appears, and all of the users included in this group are displayed in the window.

Configuring Virtual Views for Sharing Files in Bulk

To share a set of SharePoint files with the users in the previous created user access groups, you must add the desired SharePoint files into virtual views and then share the virtual views with the user access groups by assigning permissions for the virtual views to the user access groups.

Adding Virtual Views

To add a new virtual view in **Virtual Views**, navigate to the **Manage** menu, and then click **Virtual Views** to enter the **Virtual Views** interface. Click **Add** on the ribbon, and then configure the following settings:

1. In the **Basic Information** section, configure the following information of the virtual view you want to create.
 - **Virtual View Display Name** – Enter the name of the virtual view you want to create.
 - **Site URL** – Enter the URL of the site where the files you want to add into the virtual view.

*Note: You must ensure the SharePoint Search Service crawling is started for the entered site.
 - **Authentication Method** – Select the authentication method used by the SharePoint zone where this entered site resides. **Windows Authentication**, **Forms-Based Authentication**, and **Trusted Identity Provider** are available for the **Authentication Method**.
 - **Username and Password** – Enter the credentials of the SharePoint user used to retrieve the metadata properties of the all of the files within the entered site above. You must ensure the entered user has at least **Read** permission to the site.
2. Click **Validation Test** to verify whether the entered information above is valid.
3. In the **Virtual View Settings** section, complete the following steps to create folders in this virtual view and add SharePoint files into the folders based on metadata rules.
 - a. Click **New Folder** to add a new folder in the **Folder Name** column.
 - b. Enter the name of the new folder, and press **Enter** to save the name.
 - c. Refer to [Creating or Editing Metadata Rules for Folders in Virtual View Settings](#) to configure the metadata rules for adding files into this folder.
 - d. If desired, repeat steps a to c to add more folders into the virtual view.

4. Click **Save** to save the configurations and add the virtual view into AvePoint Perimeter management system, or click **Cancel** to exit and go back to the **Virtual Views** interface without adding the virtual view.

Editing Virtual Views

To edit a previously created virtual view in **Virtual Views**, select the corresponding checkbox and click **Edit** on the ribbon, or click the open menu button next to the **VIRTUAL VIEW DISPLAY NAME** and then click **Edit** in the menu. You can edit the following configurations:

1. In the **Basic Information** section, configure the following information of the virtual view you are editing.
 - **Virtual View Display Name** – Enter the name of the virtual view you are editing.
 - **Site URL** – Enter the URL of the site where the files you want to add into this virtual view.

***Note:** You must ensure the SharePoint Search Service crawling is started for the entered site.
 - **Authentication Method** – Select the authentication method used by the SharePoint zone where this entered site resides. **Windows Authentication**, **Forms-Based Authentication**, and **Trusted Identity Provider** are available for the **Authentication Method**.
 - **Username** and **Password** – Enter the credentials of the SharePoint user used to retrieve the metadata properties of the all of the files within the entered site above. You must ensure the entered user has at least **Read** permission to the site.
2. Click **Validation Test** to verify whether the entered information above is valid.
3. In the **Virtual View Settings** section, you can add new folders or edit the existing folders for this virtual view.
 - To create a new folder in this virtual view, complete the following steps:
 - i. Click **New Folder** to add a new folder in the **Folder Name** column.
 - ii. Enter the name of the new folder, and press **Enter** to save the name.
 - iii. Refer to [Creating or Editing Metadata Rules for Folders in Virtual View Settings](#) to configure the metadata rules for adding files into this folder.
 - To rename a folder, select the checkbox next to the desired folder in the **Folder Name** column, click **Rename**, and enter the new folder name in the text box in the **Folder Name** column.
 - To delete a folder, select the checkbox next to the folder, and click **Delete**.
 - To modify the rule settings for a folder, refer to [Creating or Editing Metadata Rules for Folders in Virtual View Settings](#).

4. Click **Save** to save the configurations to the virtual view, or click **Cancel** to exit and go back to the **Virtual Views** interface without saving the modifications of the virtual view.

Creating or Editing Metadata Rules for Folders in Virtual View Settings

To create or edit metadata rules for a specific folder in a virtual view, select the desired folder in the **Folder Name** column and click **Configure** on the ribbon. The **Configure Metadata Rules** window appears. Complete the following steps to create or edit the rules for the selected folder:

1. In the **Configure Metadata Rules** window, configure the rules for adding files into the folder.
 - a. Click **Add a Rule** to add a rule by completing the fields below, or click **Remove** to delete the rule.
 - o **Level** – Select the file property which the rule is configured for from the drop-down list.
 - o **Condition** – Select the condition for the rule.
 - o **Rule and Value** – Designate the value used to filter the file property selected in the **Level** field.
 - If you select **Value**, enter the value used to filter the file property in the **Value** textbox.
 - If you select **User**, select the user property you want to use to filter file property in the **Value** drop-down list. The value of the selected user property is based on the user who is accessing this virtual view via AvePoint Perimeter External Portal or AvePoint Perimeter mobile app. In this way, the filter results of this rule are based on the user who is accessing this virtual view.
 - b. To add more rules, repeat the previous step.
 - o If 2 or more rules are configured, determine the logical relationship in the **Conditions** text box. There are two logic choices: **And** and **Or**. The default logic is **And**.
 - **And** – Files that meet all of the rules will be added into the folder.
 - **Or** – Files that meet any one of the rules will be added into the folder.
2. Click **Preview Filter Results** to preview the files that meet the configured rules.
 - If you select **Value** in the **Rule** drop-down list in all of the rules, the **Preview Filter Results** window appears. The files that meet the configured rules are displayed in the window.
 - If you select **User** in the in the **Rule** drop-down list in one or more rules, the **Select a User** window appears. Select a user whose property values will be used as the values for previewing the filter results of the corresponding rules.
 - i. Enter the keyword of the desired username in the **User** search box.

- ii. Select the desired user in the drop-down list.
 - iii. Click **OK** to save the configuration and access the **Preview Filter Results** window.
3. Close the **Preview Filter Results** window and return to the **Configure Metadata Rules** window.
4. Click **Save** to save the rules for the folder and return to the **Add Virtual View/Edit Virtual View** interface.

After the rules are successfully saved for a specific folder, the **Rules** column displays the number of rules configured for the folder.

***Note:** By default, the **Virtual Views** feature trims the duplicated files recognized by SharePoint Search API in the search results of the configured metadata rules. To include the duplicated files in the search results, complete the following settings:

1. Go to the `\bin\config` folder under the Manager installation path. The default Manager installation path is `...C:\Program Files\AvePoint\Perimeter\Manager`.
2. Open the **AppSettings.config** file using **Notepad**.
3. Set the value of the **trimSPSearchDuplicate** attribute to **false**. The default value of the **trimSPSearchDuplicate** attribute is **true**.
4. Save the change and close the file.

Sharing Virtual Views with User Access Groups

After creating virtual views, you can navigate to the **Manage Permissions** interface to share the virtual views to the previously created user access groups by assigning permissions for the virtual views to the user access groups.

To access the **Manage Permissions** interface, select the corresponding checkbox of the desired virtual view in the **Virtual Views** interface and then click **Manage Permissions** on the ribbon. The **Manage Permissions** interface appears.

Sharing Virtual Views with User Access Groups via Assigning Permissions

In the **Manage Permissions** interface, to share the selected virtual view to a previously created user access group, click **Assign Permissions** on the ribbon. In the **Assign Permissions** interface, configure the following settings:

1. In the **User Access Group Name** section, select the user access group with which you want to share the virtual view from the drop-down list.
2. In the **Notification Settings** section, select notification settings for the sharing of the virtual view.
 - To send e-mail notifications to the users included in the selected user access group, select the **Send notifications to users in the user access group** checkbox.

- To send e-mail notifications with a custom message to the users included in the selected user access group, select the **Send notifications to users in the user access group** checkbox and enter the custom message in the text box below.
3. In the **Permission Settings** section, choose the **Permission Level** for the user access group's permissions to the copies of the files included in the shared virtual view stored in the previously configured **Shared File Location**. For detailed instructions on selecting the permission level, refer to [Secured Share Permission Levels](#). The users in the access group assigned with Edit permission level can edit the copies of the files and the modifications will be synchronized back to the original file in the SharePoint site.
 4. In the **Permission Expiration Time** section, specify when this sharing of the virtual view will expire. Enter an expiration date in the **Expiration Time** text box or select the expiration date from the calendar.
 5. In the **Assign permission to another user access group section**, select whether to continue to assign permission to another user access group after saving the configurations here.
 - If you select this option, and click **Save** to save the configurations and assign permission to the selected user access group. After the permission is successfully assigned, you can stay on the **Assign Permissions** page to assign permission to another user access group.
 - If you do not select this option, and click **Save** to save the configurations and assign permission to the selected user access group. After the permission is successfully assigned, you will exit this page and go back to the **Manage Permissions** page.

If you don't want to assign the permission to the selected user access group, click **Cancel** to exit this page without assigning the permissions.

Editing a User Access Group's Permissions for a Virtual View

To edit the previously assigned permissions for a specific virtual view, select the corresponding checkbox in the **Manage Permissions** interface, and click **Edit** on the ribbon. In the **Assign Permissions** interface, configure the following settings:

1. In the **Notification Settings** section, select notification settings for the sharing of the virtual view.
 - To send e-mail notifications to the users included in the selected user access group, select the **Send notifications to users in the user access group** checkbox.
 - To send e-mail notifications with a custom message to the users included in the selected user access group, select the **Send notifications to users in the user access group** checkbox and enter the custom message in the text box below.
2. In the **Permission Settings** section, choose the **Permission Level** for the user access group's permissions to the copies of the files included in the shared virtual view stored in the previously configured **Shared File Location**. For detailed instructions on selecting the permission level, refer to [Secured Share Permission Levels](#).

3. In the **Permission Expiration Time** section, specify when this sharing of the virtual view will expire. Enter an expiration date in the **Expiration Time** text box or select the expiration date from the calendar.
4. In the **Assign permission to another user access group section**, Select whether to continue to assign permission to another user access group after saving the changes.
 - If you select this option, and click **Save** to save the changes and assign permission to the selected user access group. After the permission is successfully updated, you can stay on the **Assign Permissions** page to assign permission to another user access group.
 - If you do not select this option, and click **Save** to save the changes and assign permission to the selected user access group. After the permission is successfully updated, you will exit this page and go back to the **Manage Permissions** page.

If you don't want to save the changes to the selected permissions, click **Cancel** to exit this page without saving the changes.

Removing User Access Groups' Permissions for Virtual Views

To remove user access groups' permissions for a particular virtual view in the **Manage Permissions** interface, select the corresponding checkboxes next to the **USER ACCESS GROUP NAME** column and click **Delete** on the ribbon. Alternatively, you can click the open menu button next to the **USER ACCESS GROUP NAME** and then click **Delete** in the menu.

Once the user access groups' permissions for the selected virtual view have been deleted, the users in the user access groups cannot access the files in the virtual view via the AvePoint Perimeter External Portal or the Perimeter apps on mobile apps.

Managing Shared Files

In **Manage Shared Files**, you can view and manage all of the SharePoint objects (including files, folders, and libraries) shared through the **AvePoint Perimeter Secured Share** feature and view the usage details of each shared file.

To access **Manage Shared Files**, navigate to the **Manage** menu and click **Manage Shared Files** to enter the **Manage Shared Files** interface.

In the **Managed Shared Files** interface, you can view all of the sharing events within the SharePoint farms where the **AvePoint Perimeter Secured Share** feature is in use, including the name, size (only available for shared files), last modified time, last shared time, and the location and URL of each shared object in SharePoint, the user who shares the object, the user who is shared the object with, the permission settings, and the expiration time of each sharing event. To filter the sharing events with criteria, you can use the search box in the upper-right corner to search by the desired file names or use the **Advanced Search** feature to configure multiple search conditions. To use **Advanced Search**, refer to [Advanced Search](#).

In the **Manage Shared Files** interface, you can follow the following operations to manage the shared objects.

- [Viewing Sharing History](#)
- [Viewing Document Usage](#)
- [Changing Shared Permission Settings](#)
- [Removing Users' Shared Permissions](#)

Viewing Sharing History

To view all of the sharing events for when a specific SharePoint object is shared with the same user in **Manage Shared Files**, complete the following steps:

1. Select the corresponding sharing event which contains the desired object in the **NAME** column and the user in the **SHARED WITH** column.
2. Click **View History** on the ribbon. The **View Sharing History** interface appears.
3. View the sharing history in the **View Sharing History** interface.

In the **View Sharing History** interface, you can view the detail information of the sharing events that the selected object is shared with the same user, including the user who shared the object, the user who is shared with, the permission settings, and the time of each shared event.

The display pane of **View Sharing History** has a number of configurable settings so that you can customize how the sharing events are displayed by performing the following operations:

- **Manage Columns** – Manage which columns are displayed in the list using the **Manage Columns** drop-down list, so that only the information you want to see is displayed.
- **Filter the column**– Filter which events in the list are displayed based on the values in the **Shared By** column. Click the Open Menu (☑) button next to the column name **SHARED BY**, select the checkboxes in the drop-down menu, and click **OK** to have the corresponding events shown in the list.
- **Sorting the column** – To sort the events in the list, click the column name of the **SHARED BY/PERMISSION LEVEL/TIME SHARED/EXPIRATION TIME/SHARE UPDATES** column and then select to sort the events in ascending or descending order.
- **Search for keywords** – Filter the events by the keyword in the desired internal user name within the **SHARED BY** column. Enter the desired keyword in the text box and click the search button.
- **Advanced Search** – Search for the events you want to view with the criteria specified in **Advanced Search**. To use **Advanced Search**, refer to [Advanced Search](#).


Viewing Document Usage

Using the **View Document Usage** feature in **Manage Shared Files**, you can view the usage of a specific shared file or all of the files included in a shared folder/library performed by users via the AvePoint Perimeter External Portal, AvePoint Point Internal Portal, and AvePoint Perimeter mobile apps. To do this, complete the following steps:

1. Select the corresponding sharing event which contains the desired file/folder/library in the **NAME** column.
2. Click **View Document Usage** on the ribbon. The **Document Usage Tracking** interface appears.

In the **Document Usage Tracking** interface, you can view the details of the selected user's activities on the selected shared file or the files in the selected shared folder/library, including the time, the user who accessed the file, the action performed, the source of the access, the platform, model and, operating system of the access point, the browser used by the user, the user's location, and the shared file's URL in each activity.

The display pane of **Document Usage Tracking** has a number of configurable settings so that you can customize how the activities are displayed by performing the following operations:

- **Manage Columns** – Manage which columns are displayed in the list using the **Manage Columns** drop-down list, so that only the information you want to see is displayed.
- **Filter the column** – Filter which activities in the list are displayed based on the values in the **SHARED WITH/PLATFORM** column. Click the Open Menu () button next to the column names, select the checkboxes in the drop-down menu, and click **OK** to have the corresponding events shown in the list.
- **Sorting the column** – To sort the activities in the list, click the column name of **THE TIME ACCESSED/SHARED WITH/ACTION** column and then select to sort the events in ascending or descending order.

Changing Shared Permission Settings

To change the permission settings in a specific sharing event, complete the following steps:

1. Select the desired sharing event in the **Manage Shared Files** interface.
2. Click **Change Permissions** on the ribbon. The **Change Permissions** pop-up window appears.
3. Edit the following permission settings of the sharing event:
 - **Permission Level** – Select the desired permission level for the user with whom the object has been shared from the drop-down list. For details on selecting the permission level, refer to [Secured Share Permission Levels](#).
 - **Expiration Time** – Specify the expiration time of this sharing. Enter an expiration time in the text box or select an expiration date using the calendar.

- **Share Updates** – Select whether to share the updates of the shared object with the user as well.
4. Click **Save** to save the changes to this sharing event, or click **Cancel** to exit this window without saving the changes.

Secured Share Permission Levels

Refer to the section below for detailed information on the specific permissions included in each permission level for secured shared files/folders/libraries that are available in the **Change Permissions** pop-up window.

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:** Only the files with the file types listed in the [Supported File Types for Online Viewing on the 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** or **Edit** permission level to ensure that the users can download the shared files.

Removing Users' Shared Permissions

To remove a specific user's permissions for a shared object, complete the following steps:

1. Select the corresponding sharing event which contains the desired object in the **NAME** column and the user in the **SHARED WITH** column in the **Manage Shared Files** interface.
2. Click **Remove Permissions** on the ribbon. The confirmation window appears.
3. Click **OK** to remove the user's permissions for the selected object, or click **Cancel** to exit this window without removing the user's permissions.

If the user's permissions for the selected object have been removed, the user cannot access the copy of this object via the AvePoint Perimeter External Portal or AvePoint Perimeter mobile apps.

Customizing the Size of the Online Read DWG File

When a user opens a **.dwg** file in the AvePoint Perimeter External Portal/AvePoint Perimeter mobile app, this **.dwg** file is automatically converted into a **.png** image and then displayed in the viewing page.

The default size for of the converted **.dwg** image is 425 x 310 pixels. To change the size of the image, following the steps below:

1. Go to the `\bin\config` folder under the Manager installation path. The default Manager installation path is `...\Program Files\AvePoint\Perimeter\Manager`.
2. Open the **AppSettings.config** file using **Notepad**.
3. Set the values of the **dwgConvertPdfWidth** and **dwgConvertPdfHeight** attributes to your desired width and height of the converted **.dwg** file.

```
<add key="androidSenderAuthToken" value="AIZA5yBLOkYc4yQrPYL2dtikyauA-jCLFPuxy0c" />
<add key="sessionTimeoutMinutes" value="30" />
<add key="keepMeSignInHours" value="8" />
<add key="trimSPSearchDuplicate" value="true" />
<add key="PortalEnrollDeviceDisable" value="false" />
<add key="calculateActionExecuteTime" value="false" />
<add key="minuteBucketLength" value="5" />
<add key="userLocationValidHour" value="4" />
<add key="authenticationDate" value="300" />
<add key="wifiConnectionUploadInterval" value="5" />
<add key="mobileConnectionUploadInterval" value="15" />
<add key="locExpireTime" value="10" />
<add key="locExpireTimeLong" value="30" />
<add key="minLocUpdateInterval" value="5" />
<add key="dwgConvertPdfWidth" value="425" />
<add key="dwgConvertPdfHeight" value="310" />
</appSettings>
```

Figure 8: Configuring the values of the **dwgConvertPdfWidth** and **dwgConvertPdfHeight** attributes.

4. Save the change and close the file.
5. Repeat the same configurations in the **AppSettings.config** file on the server with External Portal and Gateway installed.

Report Menu

In the **Report** menu, you can view reports of **Access Points**, **Access Logs**, **Event Logs**, **Access Violation Logs**, **Access Warning Logs**, **Burglar Alarm Report**, and **Daily Audit Tracking**. These reports provide you with detailed information on the access points and login sessions to the SharePoint sites managed by AvePoint Perimeter. In addition, you can report on the logs generated by the **Content Access Control** and **Content Access Logging** features in **Content Access Policy**, and the **Burglar Alarm Rules** feature.

***Note:** In the **Access Points** report, you can view all of the access data managed by the AvePoint Perimeter management system after the Content Access Policy features are enabled on the SharePoint sites. Perimeter keeps all access data for 30 days in the Manager Configuration database. After 30 days, the data is automatically deleted.

Access Points

Access Points report displays the event logs based on the access points to the SharePoint sites managed by the AvePoint Perimeter management system, including the access point name, platform, model, operating system, registration time, last login user, last login time and last login session duration of each access point.

Viewing Access Points Report

The report display pane has a number of configurable settings so that you can customize how the report displays the data. For **Access Points**, the following settings can be configured in the report display pane:

- **Manage Columns** – Manage which columns are displayed in the list using the **Manage Columns** drop-down list, so that only the information you want to see is displayed.
- **Filter the column** – Filter which items in the list are displayed. Click the Open Menu (▼) button next to the column name, select the checkboxes in the drop-down menu, and click **OK** to have the corresponding items shown in the list.
- **Sorting the column** – Sort the items in the list in ascending or descending order based on THE **REGISTRATION TIME/LAST LOGGED LOGIN/LAST SESSION DURATION (MINUTES)** column by clicking the column name.
- **View All Sessions** – Select the access point in the report pane and click **View All Sessions** on the ribbon to jump to the **Access Logs** page and view the details about all of the login sessions of this access point.

Access Logs

Access Logs report display all of the login session logs for the participating SharePoint servers, including the session ID, username, start time and duration of each login session and the platform, model, operating system, browser, and location and device name of the used device in the session.

Viewing Access Logs

The report display pane has a number of configurable settings so that you can customize how the report displays the data. For **Access Logs**, the following settings can be configured in the report display pane:

- **Manage Columns** – Manage which columns are displayed in the list using the **Manage Columns** drop-down list, so that only the information you want to see is displayed.
- **Filter the column** – Filter which items in the list are displayed. Click the Open Menu (▼) button next to the column name, select the checkboxes in the drop-down menu, and click **OK** to have the corresponding items shown in the list.
- **Sorting the column** – Sort the items in the list in ascending or descending order based on the **START TIME/LAST ACTIVE TIME/DURATION (MINUTES)** column by clicking the column name.
- **Open menu (***)** – Select the login session in the report pane, and click the open menu button (***), the **Visited Content** option appears. Click this option or click **Visited Content** on the ribbon to jump to the **Event Logs** page to view the event logs for the login session.

Event Logs

Event Logs report displays the logs of all end-user activities within the Perimeter management system, including:

- All the access to the SharePoint content monitored by the **Content Access Logging** rule via any devices.
- All the login attempts (successful logins and login failures) to the 2-factor authenticated SharePoint sites via any devices.
- All the access to the content within the managed SharePoint sites via AvePoint Perimeter mobile apps.
- All the access to the files shared through the AvePoint Perimeter Secured Share feature and the Virtual Views feature via AvePoint Perimeter External Portal or AvePoint Perimeter mobile apps.

This report displays the session ID, http method, start time, access point name, username, accessed URL, activity, the source of each content access, the platform and location of the device/browser used to access the content.

Viewing Event Logs

The report display pane has a number of configurable settings so that you can customize how the report displays the data. For **Event Logs**, the following settings can be configured in the report display pane:

- **Manage Columns** – Manage which columns are displayed in the list using the **Manage Columns** drop-down list, so that only the information you want to see is displayed.
- **Filter the column** – Filter which item in the list is displayed. Click the Open Menu (▼) button next to the column name, select the checkboxes in the drop-down menu, and click **OK** to have the corresponding items shown in the list.
- **Sorting the column** – Sort the items in the list in ascending or descending order based on the **START TIME/LAST ACTIVE TIME/DURATION (MINUTES)** column by clicking the column name.
- **Advanced Search** – Search for the items you want to view with the criteria specified in **Advanced Search**. To use **Advanced Search**, refer to [Advanced Search](#).

Exporting Event Logs

To export the Event Logs report, click **Export** on the ribbon, select your desired data scope for the export report in the pop-up window, and then click **OK**. Your browser will prompt you to open or save the CSV file. Click **Save** or **Save as** to save it to a designated location.

Access Violation Logs

Access Violation Logs report display the logs for all content blocked by the Content Access Control rules. In Access Violation Logs, you can view the time, access point name, username, access point's location, access point's platform, URL to access of each blocked content access, and the Content Access Control rule affecting access.

Viewing Access Violation Logs

The report display pane has a number of configurable settings so that you can customize how the report displays the data. For **Access Violation Logs**, the following settings can be configured in the report display pane:

- **Manage Columns** – Manage which columns are displayed in the list using the **Manage Columns** drop-down list, so that only the information you want to see is displayed.
- **Filter the column** – Filter which item in the list is displayed. Click the Open Menu (▼) button next to the column name, select the checkboxes in the drop-down menu, and click **OK** to have the corresponding items shown in the list.
- **Sorting the column** – Sort the items in the list in ascending or descending order based on the **START TIME** of the access attempts by clicking the column name.
- **Viewing Content Access Control rule details** – To view the details of the Content Access Control rule, click the link in the **Content Access Control Rule** column. The **Rule Details** page appears. You can view the action and criterion of this rule.
- **Advanced Search** – Search for the items you want to view with the criteria specified in **Advanced Search**. To use **Advanced Search**, refer to [Advanced Search](#).

Exporting Access Violation Logs

To export the Access Violation Logs report, click **Export** on the ribbon, select your desired data scope for the export report in the pop-up window and then click **OK**. Your browser will ask if you would like to open or save the CSV file. Click **Save** or **Save as** to save it to a designated location.

Access Warning Logs

Access Warning Logs report displays the logs for all content that generated access warnings. In **Access Warning Logs**, you can view the time, access point name, username, access point's location, access point's platform, URL to access of each blocked content access, and the **Content Access Control** rule affecting access.

Viewing Access Warning Logs

The report display pane has a number of configurable settings so that you can customize how the report displays the data. For **Access Warning Logs**, the following settings can be configured in the report display pane:

- **Manage Columns** – Manage which columns are displayed in the list using the **Manage Columns** drop-down list, so that only the information you want to see is displayed.
- **Filter the column** – Filter which items in the list are displayed. Click the Open Menu (▼) button next to the column name, select the checkboxes in the drop-down menu, and click **OK** to have the corresponding items shown in the list.
- **Sorting the column** – Sort the items in the list in ascending or descending order based on the **START TIME** of the access attempts by clicking the column name.
- **Viewing Content Access Control rule details** – To view details on the Content Access Control rule, click the link in the **Content Access Control Rule** column. The **Rule Details** page appears. You can view the action and criterion of this rule.
- **Advanced Search** – Search for the items you want to view with the criteria specified in **Advanced Search**. To use **Advanced Search**, refer to [Advanced Search](#).

Exporting Access Warning Logs

To export the Access Warning Logs report, click **Export** on the ribbon, select your desired data scope for the export report in the pop-up window, and then click **OK**. Your browser will prompt you to open or save the CSV file. Click **Save** or **Save as** to save it to a designated location.

2-Factor Authentication Logs

The **2-Factor Authentication Logs** report displays all 2-factor authentication attempts to all 2-factor authenticated sites (both SharePoint on-premises sites and ADFS-authenticated sites) controlled by this

Perimeter management system. In ADFS-authenticated sites, the authentication attempts may also be controlled by the **Authentication Controls** rules configured in **Federation Policy**. For more information on Federation Policy, refer to [Configuring the Federation Policy](#).

This report displays the authentication time, the URL to be accessed, status of each 2-factor authentication access attempt, username and login account of the end-user who wants to access the 2-factor authenticated site, the platform, operating system, browser/application, location information, location collection exception and device name of the device used to access the site, the additional Authentication Control rule applied to the ADFS authenticated site, and the comments about the failed access attempt.

Viewing 2-Factor Authentication Logs

The report display pane has a number of configurable settings so that you can customize how the report displays the data. For **2-Factor Authentication Logs**, the following settings can be configured in the report display pane:

- **Manage Columns**– Manage which columns are displayed in the list using the **Manage Columns** drop-down list, so that only the information you want to see is displayed.
- **Filter the column** – Filter which items in the list are displayed. Click the Open Menu (▼) button next to the column name, select the checkboxes in the drop-down menu, and click **OK** to have the corresponding items shown in the list.
- **Sorting the column** – Sort the items in the list in ascending or in descending order based on the **AUTHENTICATION TIME** of the access attempts by clicking the column name.
- **Search for keywords** –Filter the access attempt displayed by the keyword you designate. The keyword must be contained in a column value. Enter the desired keyword in the text box and click the search button.
- **Advanced Search** – Search for the items you want to view with the criteria specified in **Advanced Search**. To use **Advanced Search**, refer to [Advanced Search](#).

Exporting 2-Factor Authentication Logs

To export the 2-Factor Authentication Logs report, click **Export** on the ribbon, select your desired data scope for the export report in the pop-up window and then click **OK**. Your browser will ask if you would like to open or save the CSV file. Click **Save** or **Save as** to save it to a designated location.

Burglar Alarm Report

Burglar Alarm Report displays the logs of all end-user activities that trigger Burglar Alarm rules applied on SharePoint nodes within this AvePoint Perimeter management system. Each triggered Burglar Alarm rule is listed in the **Burglar Alarm Report** interface, including the user who triggers the rule, alarm type, rule name, applied scope, time range of the rule, and the number of the events that trigger the rule.

Viewing Burglar Alarm Report

The report display pane has a number of configurable settings so that you can customize how the report displays the data. For **Burglar Alarm Report**, the following settings can be configured in the report display pane:

- **Manage Columns** – Manage which columns are displayed in the list using the **Manage Columns** drop-down list, so that only the information you want to see is displayed.
- **Filter the column** – Filter which records in the list are displayed. Click the Open Menu (▼) button next to the **Username** column name, select the checkboxes in the drop-down menu, and click **OK** to have the corresponding records shown in the list.
- **Sorting the column** – Sort the records in the list in ascending or in descending order based on the **START TIME** or **END TIME** of the time range of the trigger rule by clicking the column name.
- **Search for keywords** – Filter the records displayed by the keyword you designate. The keyword must be contained in a column value. Enter the desired keyword in the text box and click the search button.
- **Advanced Search** – Search for the records you want to view with the criteria specified in **Advanced Search**. To use **Advanced Search**, refer to [Advanced Search](#).
- **View Details** – To view the detailed information on how a particular user triggers a Burglar Alarm rule, select the record of the desired user and rule and click **View Details** on the ribbon. The **View Details** page appears, displaying the detailed information on the selected user's activities that triggered the selected Burglar Alarm rule during the user-defined time range.

Exporting Burglar Alarm Report

To export the **Burglar Alarm Report**, click **Export** on the ribbon, select your desired data scope for the export report in the pop-up window and then click **OK**. Your browser will ask if you would like to open or save the CSV file. Click **Save** or **Save as** to save it to a designated location.

Daily Audit Tracking

The **Daily Audit Tracking** report displays the number of each end-user's activities within a designated day or date range within the AvePoint Perimeter management system, including detailed information of each activity.

Viewing Daily Audit Tracking Report

By default, the report display pane of **Daily Audit Tracking** displays the audit tracking records of all active end-users within the current day, including the user's username, user type, and number of events performed by the user. You can customize how the report displays the data using the following configurable settings in the report display pane.

- **Manage Columns** – Manage which columns are displayed in the list using the **Manage Columns** drop-down list, so that only the information you want to see is displayed.
- **Filter the column** – Filter which records in the list are displayed. Click the Open Menu (▼) button next to the **USERNAME** column name, select the checkboxes in the drop-down menu, and click **OK** to have the corresponding records shown in the list.
- **Sorting the column** – Sort the records in the list in ascending or in descending order based on **USERNAME** by clicking the column name.
- **Search for keywords** – Filter the records displayed by the keyword you designate. The keyword must be contained in a column value. Enter the desired keyword in the text box and click the search button.
- **Audit Filter** – Search for the records you want to view with the criteria specified in **Audit Filter**. To use **Audit Filter**, refer to [Using the Audit Filter](#).
- **View Details** – Using the **View Details** feature, you can view the details of a selected audit tracking record, including each activity performed by a particular user within the selected time range. For details, refer to [Viewing Activity History](#).

Using the Audit Filter

In **Daily Audit Tracking**, you can set filter criteria to extend or limit the records displayed in the report via the **Audit Filter** feature, by completing the following steps:

1. Click **Audit Filter** above the Report Display pane to access the **Audit Filter** window.
2. **Filter by User** – Filter the records by user type and/or username/user access group name.
 - **User Type** – Filter the records by user type.
 - o **All Users** – Select this option to include all end-users in the report.
 - o **Internal** – Select this option to only include internal users in the report.
 - o **External** – Select this option to only include external users in the report.
 - **User/Group Filter** – Filter the records by username/user access group name within the users of the user type selected above.
 - o **Include All Users** – Select this option to all users of the user type(s) selected above in the report.
 - o **Specify users/user access groups to include** – Select this option to only include designated users/user access groups in the report by entering the usernames/group names into the text box or selecting the users/groups via the people picker. Separate each user/group name with semi-colons.
3. **Filter by Date Range** – Filter the records by date range.
 - To view the records within a day of the current week, select the option of the corresponding day from the drop-down list.

- To customize the date range of the records to be displayed in the report, select the **Custom Date Range** option and select a desired date range using the calendar.
4. Click **Filter** to apply the configured filter criteria. All audit tracking records that meet the criteria are listed in the report. To reset all filter criteria, click **Reset**. To return to the viewing pane without applying the filter criteria, click **Cancel**.

Viewing Activity History

To view the details of the audit tracking record of a designated user within the selected date range, complete the following steps:

1. Select the corresponding audit tracking record of the desired user in the **Daily Audit Tracking** interface.
2. Click **View Details** on the ribbon. The **Activity History** interface appears.

In the **Activity History** interface, you can view the detailed information of each activity included in the selected audit tracking record, including the accessed URL, location, activity name, and time of each activity.

To export the content in the **Activity History** interface click **Export** on the ribbon. Your browser will ask if you would like to open or save the CSV file. Click **Save** or **Save as** to save it to a designated location.

Exporting Daily Audit Tracking Report

To export the content displayed in the **Daily Audit Tracking** report, click **Export** on the ribbon. Your browser will ask if you would like to open or save the CSV file. Click **Save** or **Save as** to save it to a designated location.

Advanced Search

In **Usage Tracking**, **Event Logs**, **Access Violation Logs**, **Access Warning Logs**, **2-Factor Authentication Logs**, **Burglar Alarm Report**, **Manage Enrolled Devices**, **Manage Shared Files**, and **View Sharing History**, you can filter the content you want to view based on the criteria specified in **Advanced Search**. To use **Advanced Search**, complete the following steps:

1. Click **Advanced Search** on the ribbon. The **Advanced Search** pop-up appears.
2. Configure the search criteria for the items you want to view. Select the **Level**, **Rule**, **Condition** from the corresponding drop-down lists and enter a **Value** for this rule.
 - After configuring a rule, click **Add a Rule** to add a new rule, or click the **Remove** button following each rule to delete the rule.
 - If 2 or more rules are configured, determine the logical relationship in the **Conditions** text box. There are two logic choices: **And** and **Or**. The default logic is **And**.
 - **And** – Items that meet all of the rules will be displayed.

- **Or** – Items that meet any one of the rules will be displayed.

You can click **Validate** to check the syntax of the statement specified in the **Conditions** text box.

3. Click **Search** to search items based on the entered criteria, or click **Reset** to clear the current configurations and specify new search criteria.

Uninstalling AvePoint Perimeter

The AvePoint Perimeter Uninstallation Wizards guide you through the uninstallation process. In order to complete the uninstallation successfully, the Uninstallation Wizard must be run by a local administrator.

Uninstalling AvePoint Perimeter Manager

To uninstall AvePoint Perimeter Manager, complete the following steps:

1. Open the Windows **Start Menu** on the AvePoint Perimeter Manager server, and navigate to **All Programs > AvePoint Perimeter**.
2. Open the **Manager** folder and click **AvePoint Perimeter Manager Uninstall**.
3. If desired, select **Remove Manager Configuration Database** to remove the corresponding Manager Configuration database during the Manager uninstallation.
4. Click **Uninstall Manager** to start the uninstallation process.
5. View the uninstallation process via the process bar in the Perimeter Manager Uninstallation Wizard. Once the uninstallation completes, click **Finish** to exit the uninstallation wizard.

***Note:** The application pool created by AvePoint Perimeter Manager Installation is deleted during the Manager uninstallation.

***Note:** The SharePoint audit events enabled via the **SharePoint Audit Settings** feature in Perimeter Manager will not be disabled during Manager uninstallation. To disable the enabled SharePoint audit events in a site collection, go to **Site collection audit Settings** of the site collection.

Uninstalling External Portal and Gateway

To uninstall AvePoint Perimeter External Portal and Gateway from a server, complete the following steps:

1. Open the Window **Start Menu** on the External Portal and Gateway server and navigate to **Control Panel > Programs > Uninstall a program**.
2. Locate and right-click **AvePoint Perimeter Manager (External Portal and Gateway)** in the list.
3. Click **Uninstall/Change** to access the **AvePoint Perimeter External Portal and Gateway Uninstallation Wizard**.
4. Click **Uninstall External Portal and Gateway** to start the uninstallation process.
5. View the uninstallation process via the process bar in the **AvePoint Perimeter External Portal and Gateway Uninstallation Wizard**. Once the uninstallation completes, click **Finish** to exit the uninstallation wizard.

***Note:** The application pool created by AvePoint Perimeter External Portal and Gateway Installation Wizard is deleted during the uninstallation.

Uninstalling AvePoint Perimeter WOPI Host Server

To uninstall AvePoint Perimeter WOPI Host Server from a server, complete the following steps:

1. Open the Window **Start Menu** on the server where the WOPI Host Server is installed and navigate to **Control Panel > Programs > Uninstall a program**.
2. Locate and right-click AvePoint Perimeter Manager (WOPI Host Server) in the list.
3. Click **Uninstall/Change** to access the **AvePoint Perimeter WOPI Host Server Uninstallation Wizard**.
4. Click **Uninstall WOPI Host Server** to start the uninstallation process.
5. View the uninstallation process via the process bar in the **AvePoint Perimeter WOPI Host Server Uninstallation Wizard**. Once the uninstallation completes, click **Finish** to exit the uninstallation wizard.

***Note:** The application pool created by AvePoint Perimeter WOPI Host Server Installation Wizard is deleted during the uninstallation.

Uninstalling AvePoint Perimeter Agents

Prior to uninstalling AvePoint Perimeter Agents, ensure that the Agent is not running any jobs. If an Agent is running a job, the Agent will fail the currently running job and stop the currently running processes. To uninstall AvePoint Perimeter Agent, complete the following steps:

1. Open the Windows **Start Menu** on the AvePoint Perimeter Agent server, and navigate to **All Programs > AvePoint Perimeter**.
2. Open the **Agent** folder and click **AvePoint Perimeter Agent Uninstall**.
3. Click **Uninstall Agent** to start the uninstallation process.
4. View the uninstallation process via the process bar in the **AvePoint Perimeter Agent Uninstallation Wizard**. Once the uninstallation completes, click **Finish** to exit the uninstallation wizard.

Uninstalling the AvePoint Perimeter App from Your Device

For information on uninstalling the AvePoint Perimeter app from your iOS/Android/Windows Phone device, refer to your device's instruction manual.

Appendix A: Publishing the External Portal and Gateway

You can publish the External Portal and Gateway to the Internet through one of two methods: publishing the External Portal and Gateway directly to the Internet using port mapping, or publishing the External Portal and Gateway to the Internet via reverse proxy. AvePoint recommends the latter option (publishing the External Portal and Gateway via reverse proxy) to provide additional system security.

Publishing the External Portal and Gateway Directly

To publish the External Portal and Gateway directly to the Internet, configure port mapping between the public URL and the internal URL on the router. The router will forward all of the requests to the public URL, and users can then access the External Portal and Gateway using the public URL.

Publishing the External Portal and Gateway via Reverse Proxy

To publish the External Portal and Gateway via reverse proxy, you need a reverse proxy server that is mapped to the public URL that can forward requests from the public URL to the back-end External Portal and Gateway server.

The following sections explain how to publish the External Portal and Gateway via reverse proxy according to Microsoft's guidelines, which may differ from your organization's best practices.

Configuring the Reverse Proxy for the External Portal and Gateway Overview

To properly configure the reverse proxy for the External Portal and Gateway, complete the following steps in the order shown. Click the link to jump to the corresponding section.

1. [Installing Application Request Routing Feature and URL Rewrite Feature](#)
2. [Creating the Reverse Proxy's Website and Modifying the Web.config File](#)
3. [Disabling IIS Compression](#)
4. [Exporting and Importing the AvePoint Perimeter Certificate](#)

Installing Application Request Routing Feature and URL Rewrite Feature

Application Request Routing feature and the **URL Rewrite** feature must be installed on the proxy server. **Application Request Routing** feature is a prerequisite for **URL Rewrite**. You can download it from this [site](#). After the installation of Application Request Routing, complete the steps below to configure this feature in Internet Information Services (IIS) Manager:

1. Restart IIS after the installation.
2. Navigate to **Internet Information Services (IIS) Manager**.

3. In the **Connections** pane, click the server node.
4. In the **Home** pane, double-click **Application Request Routing Cache** under the **IIS** category.
5. In the **Actions** pane, select **Server Proxy Settings....**
6. Make sure the **Enable proxy** option is selected, so that any request in the server rewritten to a server that is not a local machine will be routed to the correct place automatically without any further configurations.

To install **URL Rewrite** and ensure compatibility, AvePoint recommends using **Web Platform Installer 3.0** to install **URL Rewrite** automatically. After **URL Rewrite** installs, you can find this feature in the Windows Internet Information Services (IIS) Manager. No further configurations on **URL Rewrite** feature is required.

Creating the Reverse Proxy's Website and Modifying the Web.config File

To create the reverse proxy's IIS website and modify the **Web.config** file, complete the following steps:

1. Create a new IIS website on the proxy server using the **https** binding.
2. Navigate to the physical path of the newly created IIS website, create a blank **Web.config** file, and open the file using Notepad.
3. Modify the file:
 - If the newly created IIS website is a root site without a sub-path, for example: *https://url:port/*, modify the **Web.config** file as shown below:
 - i. Copy and paste the following configuration information to the file.

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <system.webServer>
    <rewrite>
      <rules>
        <rule name="ReverseProxyInboundRule1" stopProcessing="true">
          <match url="(.*)" />
          <conditions>
            <add input="{CACHE_URL}" pattern="^(https?)/" />
          </conditions>
          <action type="Rewrite" url="{C:1}://{ip address}:<port>/{R:1}" />
        </rule>
      </rules>
    </rewrite>
    <urlCompression doStaticCompression="false"
doDynamicCompression="false" />
  </system.webServer>
</configuration>
```

- ii. Change the values in **<ip address>**:**< port>** to the IP address of the External Portal and Gateway server and the Manager Service port, respectively.
 - iii. Save the modifications and then close the file.
- If the newly created IIS website is a sub-site with a sub-path, for example: *https://url:port/perimeter*, modify the **Web.config** file as shown below:
 - i. Copy and paste the following configuration information to the file.

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <system.webServer>
    <rewrite>
      <outboundRules>
        <rule name="RewriteRelativePaths" preCondition="IsHTML">
          <match filterByTags="A, Area, Base, Form, Frame, Head, IFrame, Img,
Input, Link, Script" pattern="^/(.*)" negate="false" />
          <action type="Rewrite" value="/perimeter/{R:1}" />
        </rule>
        <rule name="RewriteRedirect" preCondition="IsHTML">
          <match serverVariable="RESPONSE_Location" pattern="^/(.*)" />
          <action type="Rewrite" value="/perimeter/{R:1}" />
        </rule>
      <preConditions>
        <preCondition name="IsHTML">
          <add input="{RESPONSE_CONTENT_TYPE}" pattern="^text/html" />
        </preCondition>
      </preConditions>
    </outboundRules>
    <rules>
      <rule name="ReverseProxyInboundRule1" stopProcessing="true">
        <match url="(.*)" />
        <conditions>
          <add input="{CACHE_URL}" pattern="^(https?)/" />
        </conditions>
        <action type="Rewrite" url="{C:1}://{ip address}< port>/{R:1}" />
      </rule>
    </rules>
  </rewrite>
  <urlCompression doStaticCompression="false"
doDynamicCompression="false" />
</system.webServer>
</configuration>
```


- ii. Change the values in < **ip address**>:< **port**> to the IP address of the External Portal and Gateway server and the Manager Service port, respectively.
- iii. Save the modifications and then close the file.

Disabling IIS Compression

To disable the IIS Compression feature of both the External Portal and Gateway's website and the reverse proxy's website, complete the following steps:

1. Navigate to the **Internet Information Service (IIS) Manager** of the server where the External Portal and Gateway's website resides.
2. Select the website of the External Portal and Gateway in the left pane, and double-click **Compression** in the **IIS** section of the right pane to configure the **Compression** feature.

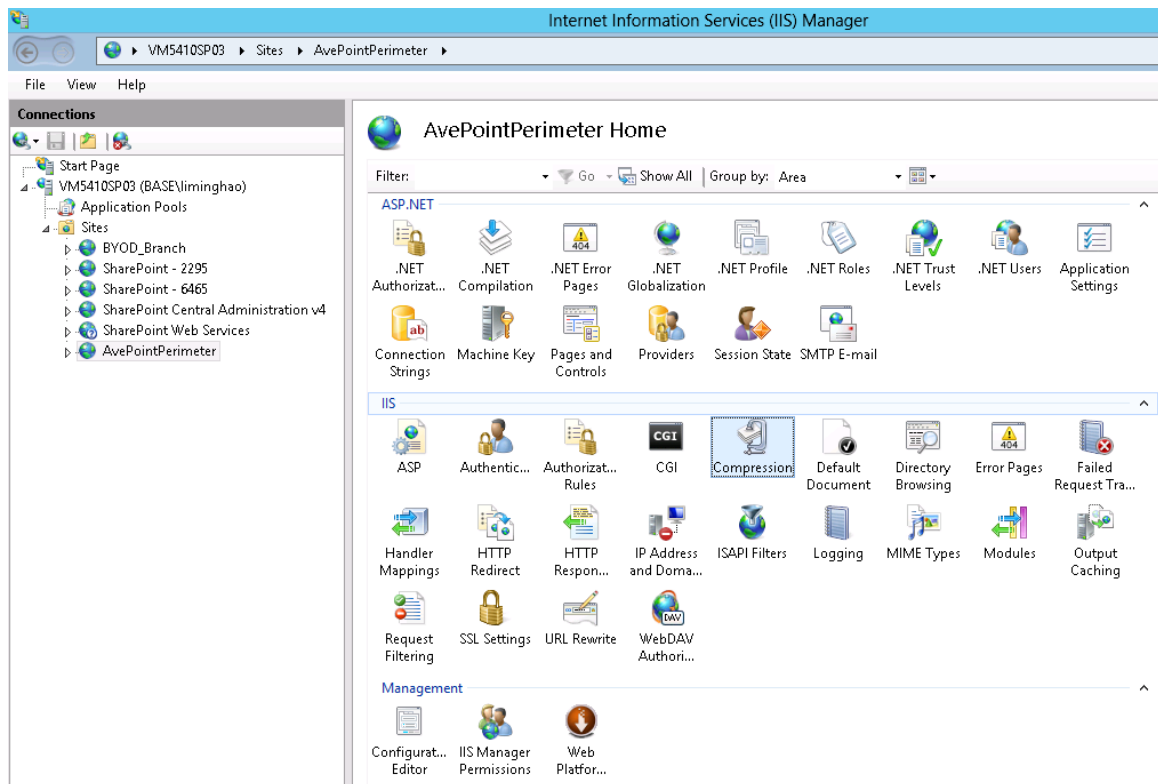


Figure 9: The Compression icon.

3. In the **Compression** page, deselect the **Enable dynamic content compression** checkbox and the **Enable static content compression** checkbox, and click **Apply**. This disables the Compression feature of the External Portal and Gateway's website.

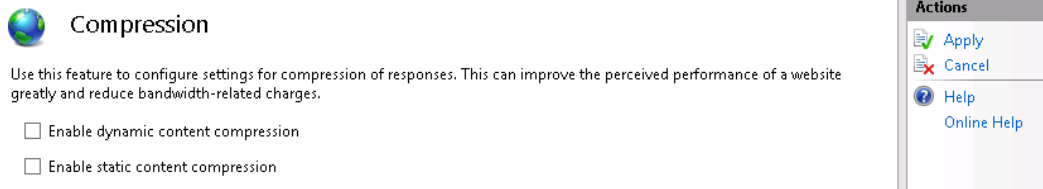


Figure 10: Configuring compression settings.

4. Navigate to the **Internet Information Service (IIS) Manager** of the server where the reverse proxy's website resides.
5. Select the website of the reverse proxy in the left pane, and double-click **Compression** in the **IIS** section of the right pane to configure the **Compression** feature.
6. In the **Compression** page, deselect the **Enable dynamic content compression** checkbox and the **Enable static content compression** checkbox, and click **Apply**. This disables the Compression feature of the reverse proxy's website.

Exporting and Importing the AvePoint Perimeter Certificate

To export the External Portal and Gateway's website certificate and import it into the proxy server, complete the following steps:

1. Navigate to **the Internet Information Site (IIS) Manager** and click the local host in the left pane.
2. Click **Sites** to view all of the websites on this server and right-click on the External Portal and Gateway's website.
3. Click **Edit Bindings...** in the menu.

4. The **Site Bindings** pop-up window appears. Click **Edit ...** to open the **Edit Site Bindings** window.

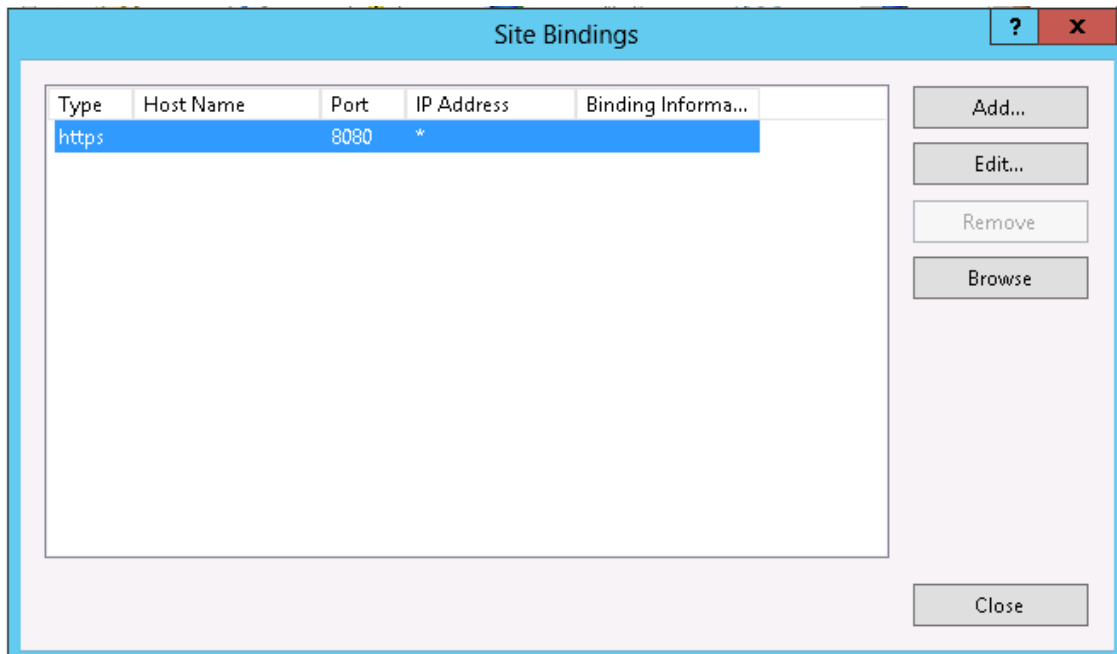


Figure 11: The Site Bindings pop-up window.

5. In the **Edit Site Bindings** window, select the certificate for AvePoint Perimeter and click **View...** to open the **Certificate** window.
6. Go to the **Details** tab and click **Copy to File...** to export the cer. file. The **Certificate Export Wizard** appears.

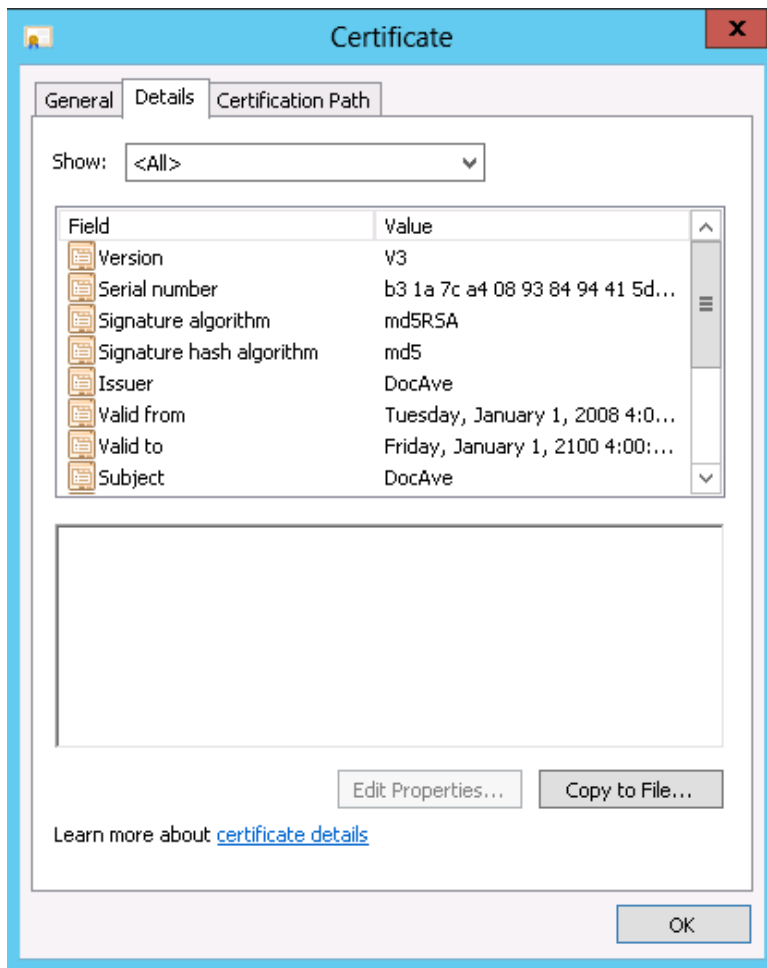


Figure 12: The Certificate Window Copy to File... button.

7. In the welcome page of this wizard, click **Next**.
8. In the **Export Private Key** page, select **No, do not export the private key**, and click **Next**.
9. In the **Export File Format** page, select **DER encoded binary X.509 (.CER)**, and click **Next**.
10. In the **File to Export** page, enter the name of the file you are about to export, and click **Next**.
11. Click **Finish**. A pop-up window appears, informing you that the export successfully completed.
12. Import the exported certificate file into the proxy server.
13. Navigate to the proxy server.
14. Click **Run...** from the **Start** menu.
15. Enter **mmc** in the **Open** text box. Then click **OK**. The **Console** page appears.
16. Click **Add/Remove Snap-in...** in the **File** menu. The **Add or Remove Snaps-ins** window appears.

17. Select **Certificates** from the **Available Snap-ins** list and click **Add**. The **Certificate snap-in** window appears.

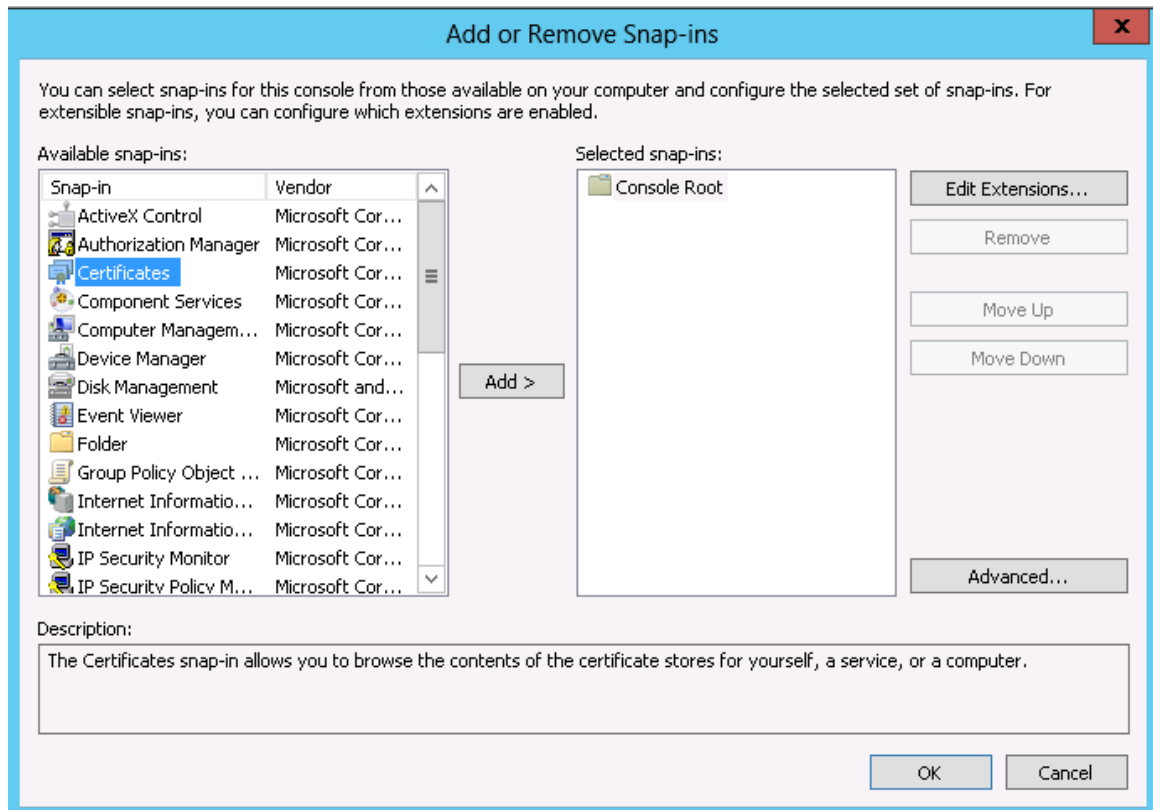


Figure 13: The Add or remove Snap-ins window.

18. In the **Certificate** snap-in page, select **Computer account**, and click **Next**.
19. In the **Select Computer** page, select **Local Computer:** (the computer this console is running on), and click **Finish**. The **Certificates** snap-in appears in the **Selected snap-ins** list.
20. Click **OK** on the **Add or Remove Snap-ins** page.
21. Click **Certificates (Local Computer)** under the **Console Root**.
22. Expand the **Trusted Root Certificate Authorities** folder to load the **Certificate** folder.

23. Right-click on the **Certificates** folder, and select **All Tasks> Import...** on the menu.

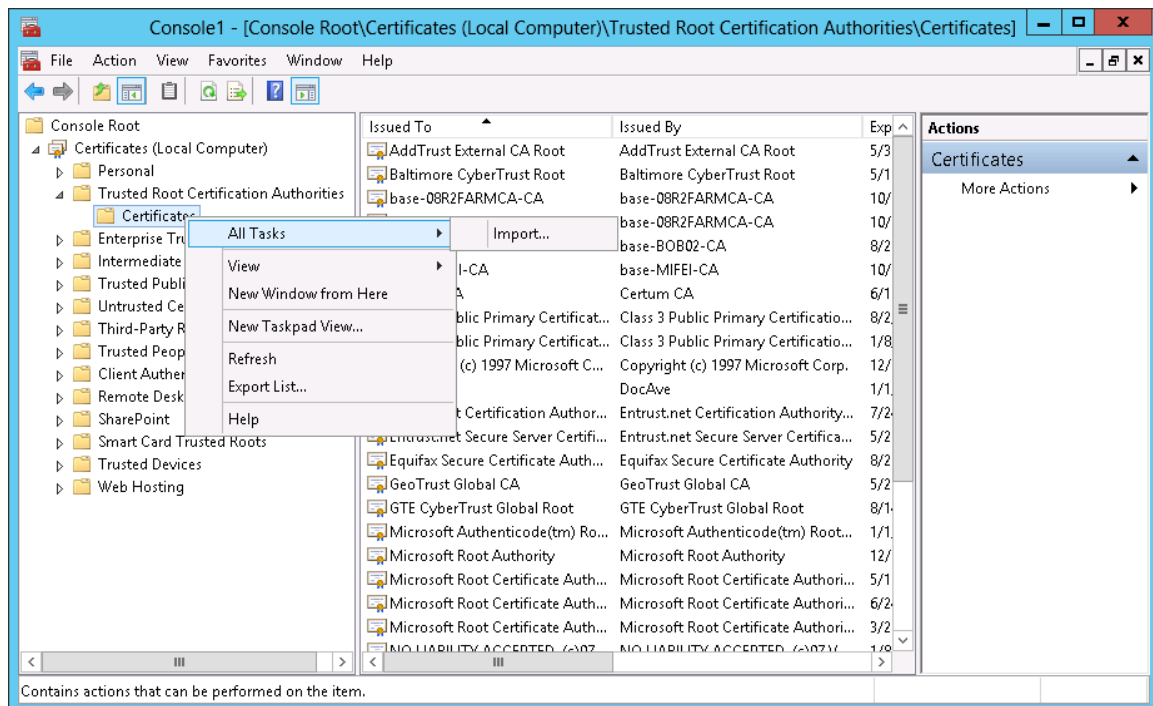


Figure 14: Selecting All Tasks > Import...

24. Click **Next** on the welcome page of the **Certificate Import Wizard**.
25. In the **File to Import** page, enter the file name of the exported certificate file for the External Portal and Gateway's website, and click **Next**.
26. In the **Certificate Store** page, select **Place All Certificates in the following store**.
27. Select **Trusted Root Certification Authorities** in the **Certificate store** text box, and click **Next**.
28. Click **Finish** on the **Completing Certificate Imported Wizard** page. The External Portal and Gateway's certificate is imported to the reverse proxy server.

Verifying the External and Gateway Server Certificate

The AvePoint Perimeter mobile app communicates with AvePoint Perimeter Manager via the Gateway. The server certificate on the External and Gateway server or reverse proxy (if the External and Gateway is published via reverse proxy) should be a valid certificate obtained from a commercial certificate authority. A self-signed certificate can be used as well, although it is not recommended. The AvePoint Perimeter mobile app supports importing a self-signed server certificate during device enrollment.

By default, during the Manager Installation, a default self-signed certificate with the current host name is already deployed for the AvePoint Manager and Gateway. The certificate will work for AvePoint Manager, but may not be valid for the Gateway due to stricter server certificate validation on the AvePoint Perimeter mobile app.

The AvePoint Manager Installation Wizard generates and deploys a default server certification for the Gateway.

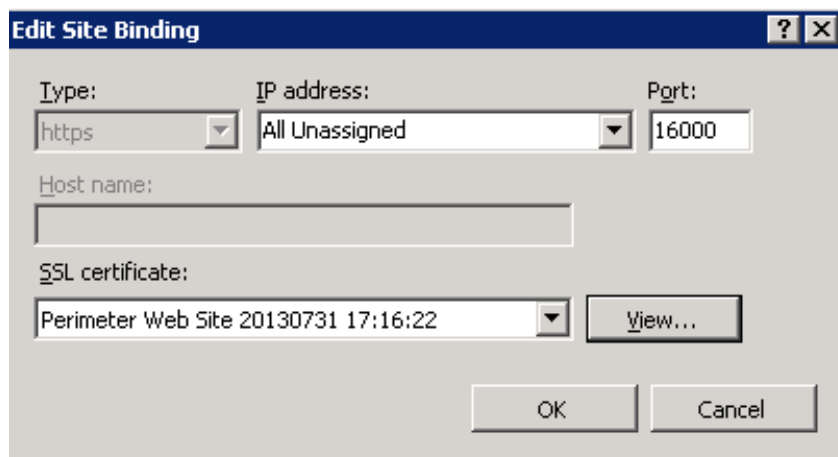


Figure 15: Portal and Gateway Server Certificate.

Figure 16 displays the **Certificate Information** page for the Gateway Server Certificate.

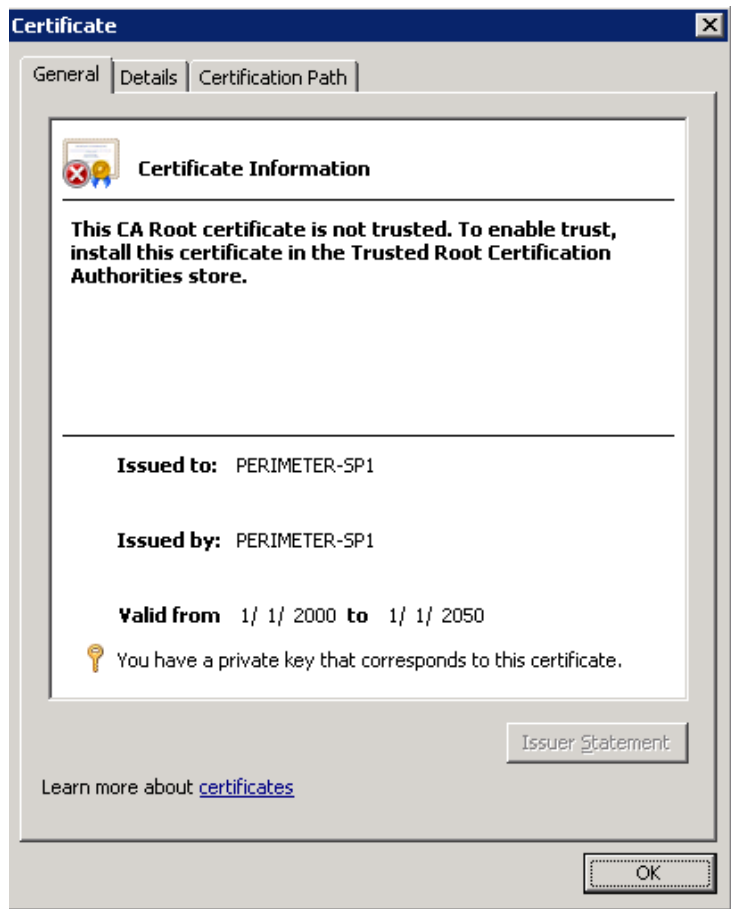


Figure 16: Certificate Information page for the Portal and Gateway Server Certificate.

Appendix B: AvePoint Perimeter and Location Data

See the FAQ below for details on how Perimeter handles location data.

How is the Location Services feature used?

From an end-user perspective, Perimeter uses the Location Services feature either in the user's device, or in their browser. In either case, the user usually opts into Perimeter working with this service.

The Location Services feature actually determines how the location is acquired (GPS, Wi-Fi, etc.) along with its accuracy, and the Perimeter app simply receives the final results. The user may not know they've opted into this, or, if the device is under organization control, the setting may be configured through a central policy.

What location data is obtained and when is it obtained?

The location data itself is generally just latitude and longitude (2 coordinates), and is only obtained when:

1. The application is used to authenticate the user (scan the QR code).
2. The user opens (accesses) a document stored in the application.

What does Perimeter do with the location data?

The location data (just the coordinates) is sent to the Perimeter server only; no data is sent to a 3rd party service. In short, user location data is either on the device, or with the customer's Perimeter installation.

Once the data is on the server, it becomes part of the audit log. In the audit log, it shows the user, device, browser, etc. along with the "location."

How long does Perimeter keep the location data?

The location data is automatically deleted from the database 30 days after it was initially obtained.

How do I secure this data on the backend?

It is up to you, the customer (Perimeter Administrator), to make sure this data is secure, as it can be used to track user movement. How the data is stored, and who has access to it, is an organizational decision.

Appendix C: Customizing AvePoint Perimeter E-mail Templates, E-mail Display Language, Web Pages, and Portals

After AvePoint Perimeter Manager and Agents are installed on your environment, refer to the sections below to customize e-mail templates and Web pages provided by the Perimeter system, and the look and feel of the Perimeter Internal and External Portals:

- [Customizing E-mail Templates](#)
- [Customizing E-mail Display Language](#)
- [Customizing the Look and Feel of Web Pages](#)
- [Customizing the Look and Feel of the Perimeter Management Console and Internal Portal](#)

Customizing E-mail Templates

For AvePoint Perimeter, you can customize the following e-mail templates:

- For the following e-mail templates, you can customize the logo image (area **1**), text in the body (area **3**), and look and feel of the top bar (area **2**), body (area **3**), and bottom bar (area **4**) as shown in [Figure 17](#) below.
 - o AvePoint Perimeter Outgoing E-mail Settings
 - o AvePoint Perimeter Device Enrollment
 - o AvePoint Perimeter -- Access Warning Scheduled Report
 - o AvePoint Perimeter -- Access Warning Real-Time Report
 - o AvePoint Perimeter -- Access Violation Scheduled Report
 - o AvePoint Perimeter -- Access Violation Real-Time Report
 - o AvePoint Perimeter External Portal - Account Activation
 - o AvePoint Perimeter External Portal - Reset Password Confirmation
 - o AvePoint Perimeter Secured Share Notification
 - o AvePoint Perimeter Shared Virtual View
 - o AvePoint Perimeter: Shared File Update
 - o AvePoint Perimeter: Shared File Has Been Downloaded
 - o AvePoint Perimeter: Secure Sharing Permissions Overwritten
 - o Action Needed: Files Locked for Editing

- o AvePoint Perimeter License Expiration Alert
- o Burglar Alarm: Suspicious Activity Alert

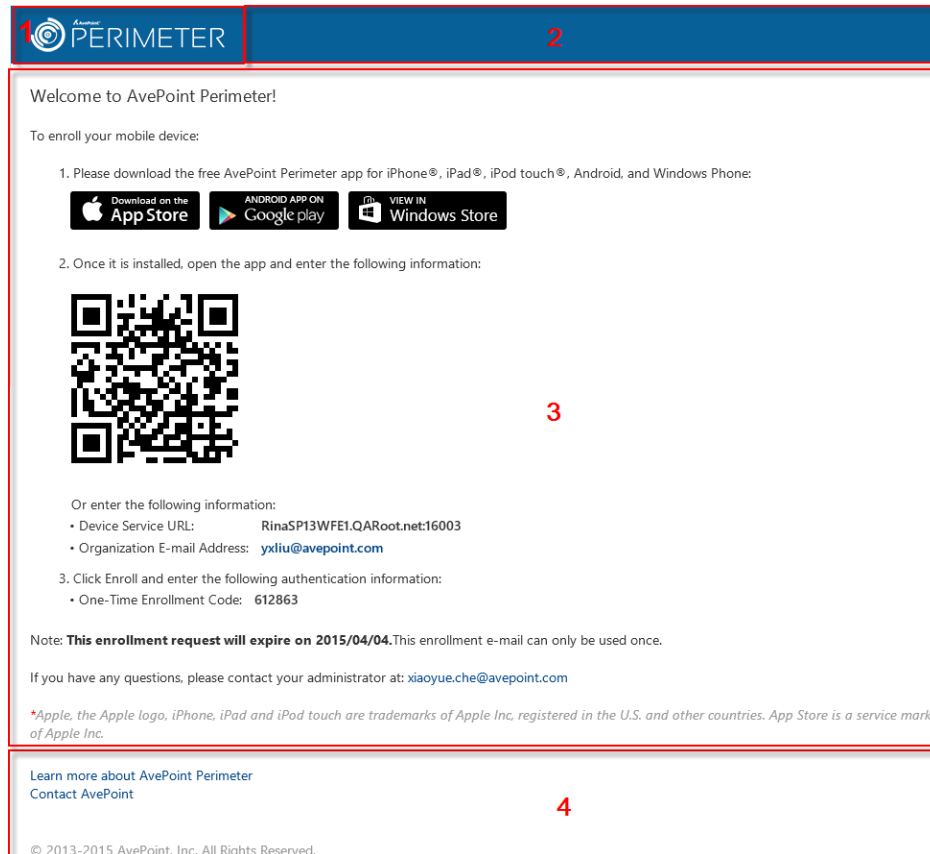


Figure 17: E-mail templates with logo image, text, and look and feel that can be customized.

- For the template for the customized e-mail notifications sent for Enterprise Wipe (shown in [Figure 18](#) below), you can customize the logo image (area 1), text in the body (area 4), and look and feel of the top bar (area 2), body (areas 3 and 4), and bottom bar (area 5).

***Note:** The subject and body text (in area 3) of this e-mail notification cannot be customized in the e-mail template since they should be entered by the administrator

who performs the **Enterprise Wipe** action on a device in the **Manage Enrolled Devices** interface.



Figure 18: An e-mail notification sent for Enterprise Wipe

Refer to the sections below to customize the text, logo image, and look and feel of e-mail templates.

Customizing the Logo Image of E-mail Templates

You can customize the logo image used in all of the e-mail templates by completing the following steps:

1. Navigate to the AvePoint Perimeter Manager server and go to ... \Perimeter\Manager\Content\themes\base\images directory.
2. Locate the **logo_without_portal_230x60.png** logo image file to view the dimensions of the logo image.
3. Resize the new image you want to use as the logo image in all of the e-mail templates to the same size as the original image, and save it as **logo_without_portal_230x60.png**.
4. Place the newly-configured image into the same directory as the original image and replace it on the Manager server, External Portal and Gateway server, and the WOPI Host Server.

***Note:** You must save the original image to another location, if you want to use the image in the future.

The customized logo image will be used in all of the e-mail templates.

Customizing Text and Link URL of the Text in E-mail Templates

You can customize the text in e-mail template and also you can change the link URL of the text, such as the URL for **Learn More** and **Contact AvePoint**. Complete the steps below to customize the text and the link URL:

1. Log into the AvePoint Perimeter Manager server and navigate to the **EmailResources** folder under the installation path of the AvePoint Perimeter Manager.

2. Copy the **email_core.en-US.resx** file, paste it into the same directory, and rename it as **customized_email_core.en-US.resx**.
3. Open the **customized_email_core.en-US.resx** file with Visual Studio (recommended) or Notepad.
4. Edit the desired text for the corresponding e-mail template in this file.
5. When you finish editing this file, save the modifications and close the file.
6. Copy this customized RESX file to same folder under the installation path of the External Portal and Gateway server and the WOPI Host Server.
7. If you want to change the link URL for **Learn More** or **Contact AvePoint** (the original name provided by AvePoint), continue with the steps below; otherwise, go to step [13](#).
8. Navigate to the `\bin\config` folder under the installation path of Perimeter Manager.
9. Open the **appsettings.config** file using Notepad.
10. Locate the following nodes, and replace the link URLs as desired:


```
<add key="learnMore" value="http://www.avepoint.com/perimeter/" />
```

```
<add key="contactUs" value="https://www.avepoint.com/contact-sales/" />
```
11. Save the configurations and close the **AppSettings.config** file.
12. Repeat the same configurations on the External Portal and Gateway server and the WOPI Host Server.
13. Restart **AvePoint Perimeter** and **AvePoint Perimeter External Portal and Gateway** IIS websites, or reset IIS. The customized text and the link URL will be applied in the corresponding e-mails.

Customizing the Look and Feel of E-mail Templates

The look and feel of e-mail templates within the Perimeter system is defined by CSS style codes in HTML files. These HTML files are stored in the `...\Views\EmailTemplates` directory on the Perimeter Manager server, External Portal and Gateway server, and WOPI Host Server.

- The look and feel of the top and bottom bars in every e-mail template is the same, which is defined in the CSS style codes that are stored in the HTML file named **LayoutEmailTemplate.html**.
- The look and feel of the body in each individual e-mail template is defined by CSS style codes that are stored in separate HTML files as listed in the table below.

E-mail Template	HTML File
AvePoint Perimeter Device Enrollment	EnrollTemplate.html
AvePoint Perimeter Outgoing E-mail Settings	OutgoingEmail.html
AvePoint Perimeter -- Access Warning Scheduled Report	WarningScheduleTemplate.html

E-mail Template	HTML File
AvePoint Perimeter -- Access Warning Real-Time Report	WarningPromptTemplate.html
AvePoint Perimeter -- Access Violation Scheduled Report	ViolationScheduleTemplate.html
AvePoint Perimeter -- Access Violation Real-Time Report	ViolationPromptTemplate.html
AvePoint Perimeter External Portal - Account Activation	RegisterEmailTemplate.html
AvePoint Perimeter External Portal - Reset Password Confirmation	ResetPasswordTemplate.html
AvePoint Perimeter Secured Share Notification	ShareEmailTemplate.html
AvePoint Perimeter Shared Virtual View	VirtualViewShareEmailTemplate.html
AvePoint Perimeter: Shared File Update (sent for updated shared objects from SharePoint)	ShareUpdateEmailTemplate.html
AvePoint Perimeter: Shared File Update (sent for updated or uploaded shared objects from the AvePoint Perimeter External Portal)	UploadOrEditFileTemplate.html
AvePoint Perimeter: Shared File Has Been Downloaded	UploadOrEditFileTemplate.html
AvePoint Perimeter: Secure Sharing Permissions Overwritten	ShareOverWriteEmailTemplate.html
Action Needed: Files Locked for Editing	LockStatusAlertEmailTemplate.html
Burglar Alarm: Suspicious Activity Alert	BurglarAlarmNotificationEmailTemplate.html
E-mail notification sent for Enterprise Wipe	EnterpriseWipeEmail.html

To customize the look and feel of an e-mail template's body, top bar or bottom bar, you can customize the CSS style codes in the corresponding HTML file.

1. Go to the ... \Perimeter\Manager\Views\EmailTemplates directory on the Perimeter Manager server.
2. Find the HTML file that contains the CSS style codes for the e-mail template's whose look and feel you want to customize, and open it using Notepad.
3. Edit the CSS style codes in the HTML file.
4. Save the changes and close the file.
5. Go to the External Portal and Gateway server and WOPI Host Server and copy the HTML file you configured to the View\EmailTemplates folder under the installation directory to replace the existing file.

The customized look and feel will be applied to the corresponding e-mail templates.

Customizing the E-mail Display Language

By default, the language in which the e-mail is displayed will be the same as the language of the server where Perimeter Manager is installed. However, you can customize the display language of e-mails in a configuration file.

To customize the e-mail display language, complete the steps below:

1. Log into the server where AvePoint Perimeter Manager is installed, and go to the ...\\AvePoint\\Perimeter\\Manager\\bin\\Config directory.
2. Open the **AppSettings.config** file with Notepad.
3. Add the following node to the configuration file, and set the value.

```
<add key="LanguageForEmail" value="French"/>
```

***Note:** The valid value options available are **English, Japanese, German, French, or Italian.**

4. Save and close the **AppSettings.config** file.

Customizing the Look and Feel of Web Pages

On the AvePoint Perimeter Agent servers, you can customize the look and feel of certain Web pages. Refer to the table below for detailed information of the Web pages you can customize, including the locations and file name for their ASPX files, CSS files and pictures:

Agent Type	Web page	ASPX File Location	CSS File Location	Picture Name
Agent for SharePoint on-premises	2-Factor Authentication	Authentication.aspx in the <i>Perimeter</i> folder under the installation path of the AvePoint Perimeter Agent	auth.css in the <i>Perimeter\\Content</i> folder under the installation path of the AvePoint Perimeter Agent	placeholder.png and topbar.png in the <i>Perimeter\\Content\\Images</i> folder under the installation path of the AvePoint Perimeter Agent
	Access Warning	Warning.aspx in the <i>Perimeter</i> folder under the	warning.css in the <i>Perimeter\\Content</i>	placeholder.png , topbar.png , warning.png , and

Agent Type	Web page	ASPX File Location	CSS File Location	Picture Name
		installation path of the AvePoint Perimeter Agent	t folder under the installation path of the AvePoint Perimeter Agent	warning_24x24.png in the <i>Perimeter\Content\Images</i> folder under the installation path of the AvePoint Perimeter Agent
	Access Violation	Blocked.aspx in the <i>Perimeter</i> folder under the installation path of the AvePoint Perimeter Agent	violation.css in the <i>Perimeter\Content</i> folder under the installation path of the AvePoint Perimeter Agent	placeholder.png , topbar.png , violation.png , and error_24x24.png in the <i>Perimeter\Content\Images</i> folder under the installation path of the AvePoint Perimeter Agent
	Authentication Fail Close	AuthNFailedClose.aspx in the <i>Perimeter</i> folder under the installation path of the AvePoint Perimeter Agent	violation.css in the <i>Perimeter\Content</i> folder under the installation path of the AvePoint Perimeter Agent	placeholder.png , topbar.png , violation.png , and error_24x24.png in the <i>Perimeter\Content\Images</i> folder under the installation path of the AvePoint Perimeter Agent
	Access Fail Close	AccessFailedClose.aspx in the <i>Perimeter</i> folder under the installation path of the AvePoint Perimeter Agent	violation.css	placeholder.png , topbar.png , violation.png , and error_24x24.png in the <i>Perimeter\Content\Images</i> folder under the installation path of the AvePoint Perimeter Agent

Agent Type	Web page	ASPX File Location	CSS File Location	Picture Name
Agents for ADFS Servers	2-Factor Authentication	MFASignIn.aspx in the <i>Perimeter</i> folder under the installation path of the AvePoint Perimeter Agent	auth.css	placeholder.png and topbar.png in the <i>Perimeter\Content\Images</i> folder under the installation path of the AvePoint Perimeter Agent
	Authentication Violation	Blocked.aspx in the <i>Perimeter</i> folder under the installation path of the AvePoint Perimeter Agent	violation.css	placeholder.png, topbar.png, violation.png, error_24x24.png in the <i>Perimeter\Content\Images</i> folder under the installation path of the AvePoint Perimeter Agent

Refer to the sections below to customize the look and feel of Web pages by editing the CSS files on the AvePoint Perimeter Agent servers.

Customizing the Look and Feel of Web Pages for SharePoint On-Premises Sites

Refer to the section below to customize the look and feel of Web pages for SharePoint on-premises sites by editing the CSS files.

1. Navigate to the *Perimeter\Content* folder under the installation path of the AvePoint Perimeter Agent.
2. Copy the corresponding CSS file for the desired Web page (for example, copy the **auth.css** file for the Web page for 2-Factor Authentication), paste it into the same directory, and rename it as **customized_original file name.css**, which is **customized_authn.css** in this case.
3. Navigate to the *Content* folder under the installation path of the AvePoint Perimeter Agent, and open the corresponding ASPX file (**Authentication.aspx** in this case) for the Web page you want to edit using your browser.
4. Press **F12** to open the developer tool of your browser.

5. Use the developer tool to locate and edit the elements you want to customize for this Web page.
6. When you finish customizing this Web page, save the modifications and close the page.

The customized settings will be applied to the corresponding Web page.

Customizing the Look and Feel of Web Pages for ADFS Authenticated Sites

Refer to the section below to customize the look and feel of Web pages for ADFS Authenticated sites by editing the CSS files.

1. Navigate to the *ADFS\Content* folder under the installation path of the AvePoint Perimeter Agent.
2. Copy the corresponding CSS file for the desired Web page (for example, copy the **auth.css** file for the Web page for 2-Factor Authentication), paste it into the same directory, and rename it as **customized_original file name.css**, which is **customized_authn.css** in this case.
3. Navigate to the *ADFS* folder under the installation path of the AvePoint Perimeter Agent, and open the corresponding ASPX file (**MFASignIn.aspx** in this case) for the Web page you want to edit using your browser.
4. Press **F12** to open the developer tool of your browser.
5. Use the developer tool to locate and edit the elements you want to customize for this Web page.
6. When you finish customizing this Web page, save the modifications and close the page.

The customized settings will be applied to the corresponding Web page.

Customizing Pictures in Web Pages

Refer to the section below to customize a picture in a designated Web page.

Customizing Pictures in Web Pages for SharePoint On-Premises Sites

Refer to the section below to customize a picture in a desired Web page for SharePoint on-premises sites:

1. Navigate to the *Perimeter\Content\Images* folder under the installation path of the AvePoint Perimeter Agent.
2. Get the dimensions of the picture you want to replace. For example, **topbar.png**.
3. Resize the new picture you want to put into the Web page to the same size as the original picture, and save it as **customized_organic file name.png**. (for example, **customized_topbar.png** in this case)
4. Place the newly-configured picture into the same directory as the original picture.

The customized picture will be display in the corresponding Web page.

Customizing Pictures in Web Pages for ADFS Authenticated Sites

Refer to the section below to customize a picture in a desired Web page for ADFS Authenticated Sites:

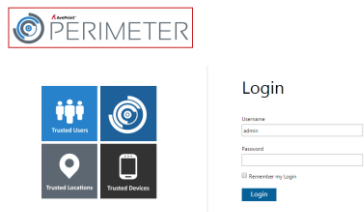
1. Navigate to the *ADFS\Content\Images* folder under the installation path of the AvePoint Perimeter Agent.
2. Get the dimensions of the picture you want to replace. For example, **topbar.png**.
3. Resize the new picture you want to put into the Web page to the same size as the original picture, and save it as **customized_original file name.png**. (For example, **customized_topbar.png** in this case.)
4. Place the newly-configured picture into the same directory as the original picture.


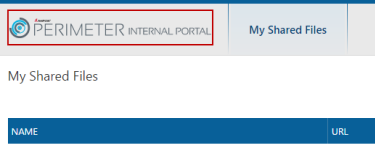
The customized picture will be display in the corresponding Web page.

***Note:** All of the customized settings will be overwritten during a patch installation or update of AvePoint Perimeter. Please make backups of your customized e-mail templates and Web pages to restore them after the patch installation or update.

Customizing the Look and Feel of the Perimeter Management Console and Internal Portal Login Page

On AvePoint Perimeter Manager server, you can define your own Perimeter logo and the look and feel for the login page of the Perimeter Management Console and Internal Portal. Refer to the table below for detailed information of the customizable elements on Perimeter Management Console and Internal Portal including the file names and locations.

Element	File Type	File Location	File Size
Logo in the Login interface of Management Console and Internal Portal: 	PNG	The logo_420x73.png file in the <i>... \AvePoint\Perimeter\Manager\Content\themes\base\images</i> directory.	420 × 73
Graphic displayed in the Login interface of Management Console and Internal Portal:	PNG	The login_460x350_en.png file in the <i>... \AvePoint\Perimeter\Manager\Content\themes\base\images</i> directory.	460 × 350


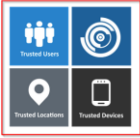

Element	File Type	File Location	File Size
			
Internal Portal Logo 	PNG	The logo_internal_portal_300x70.png file in the ... \AvePoint\Perimeter\Manager\Content\Images\Portal directory.	300 × 70
The CSS file of the Login page	CSS	The Login.css file in the ... \AvePoint\Perimeter\Manager\Content\themes\base\styles directory.	

Complete the steps below to replace the corresponding file to customize the look and feel for Perimeter Management Console and Internal Portal:

1. Go to the corresponding file location of the file you want to replace. Back up the file to a safe place and then remove it from the file location.
2. Place the file that you want to use to the file location with the same name of same size.

Customizing the Look and Feel of the Perimeter External Portal Login Page

On the server with Perimeter External Portal and Gateway installed, you can define your own Perimeter logo and the look and feel for the login page of the Perimeter External Portal. Refer to the table below for detailed information of the customizable elements on Perimeter External Portal including the file names and locations.

Element	File Type	File Location	File Size
Logo in the Login interface of Perimeter External Portal: 	PNG	The logo_420x73.png file in the <code>...\AvePoint\Perimeter\GatewayPortal\Content\themes\base\images</code> directory.	420 × 73
Graphic displayed in the Login interface of External Portal: 	PNG	The login_460x350_en.png file in the <code>...\AvePoint\Perimeter\GatewayPortal\Content\themes\base\images</code> directory.	460 × 350
External Portal Logo 	PNG	The logo_external_portal_300x70.png file in the <code>...\AvePoint\Perimeter\GatewayPortal\Content\Images\Portal</code> directory.	300 × 70
The CSS file of the Login page	CSS	The Login.css file in the <code>...\AvePoint\Perimeter\GatewayPortal\Content\themes\base\styles</code> directory.	

Complete the steps below to replace the corresponding file to customize the look and feel for Perimeter External Portal:

1. Go to the corresponding file location of the file you want to replace. Back up the file to a safe place and then remove it from the file location.
2. Place the file that you want to use to the file location with the same name of same size.

Notices and Copyright Information

Notice

The materials contained in this publication are owned or provided by AvePoint, Inc. and are the property of AvePoint or its licensors, and are protected by copyright, trademark and other intellectual property laws. No trademark or copyright notice in this publication may be removed or altered in any way.

Copyright

Copyright © 2013-2018 AvePoint, Inc. All rights reserved. All materials contained in this publication are protected by United States and international copyright laws and no part of this publication may be reproduced, modified, displayed, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of AvePoint, 525 Washington Blvd, Suite 1400, Jersey City, NJ 07310, USA or, in the case of materials in this publication owned by third parties, without such third party's consent. Notwithstanding the foregoing, to the extent any AvePoint material in this publication is reproduced or modified in any way (including derivative works and transformative works), by you or on your behalf, then such reproduced or modified materials shall be automatically assigned to AvePoint without any further act and you agree on behalf of yourself and your successors, assigns, heirs, beneficiaries, and executors, to promptly do all things and sign all documents to confirm the transfer of such reproduced or modified materials to AvePoint.

Trademarks

AvePoint®, DocAve®, the AvePoint logo, and the AvePoint Pyramid logo are registered trademarks of AvePoint, Inc. with the United States Patent and Trademark Office. These registered trademarks, along with all other trademarks of AvePoint used in this publication are the exclusive property of AvePoint and may not be used without prior written consent.

Microsoft, MS-DOS, Internet Explorer, Office, Office 365, SharePoint, Windows PowerShell, SQL Server, Outlook, Windows Server, Active Directory, and Dynamics CRM 2013 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe Acrobat and Acrobat Reader are trademarks of Adobe Systems, Inc.

All other trademarks contained in this publication are the property of their respective owners and may not be used without such party's consent.

Changes

The material in this publication is for information purposes only and is subject to change without notice. While reasonable efforts have been made in the preparation of this publication to ensure its accuracy, AvePoint makes no representation or warranty, expressed or implied, as to its completeness, accuracy, or suitability, and assumes no liability resulting from errors or omissions in this publication or from the use of the information contained herein. AvePoint reserves the right to make changes in the Graphical User Interface of the AvePoint software without reservation and without notification to its users.

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