AvePoint

AvePoint Perimeter

Release Notes

Table of Contents

AvePoint Perimeter 1.10

New Features and Improvements

- Administrator can now select to show anonymous shares or access code shares in the AvePoint Perimeter management console > Secure Share Options and Customizations.
- Updated the JQuery version to 3.3.1.
- Administrators now can select the **Delete from SharePoint permanently** option in the **Delete Option** field on the AvePoint Perimeter management console to allow users who have the Delete permission to permanently delete the secure shared files from SharePoint. With this option deselected, the shared files will be deleted and moved to the recycle bin.
- AvePoint Perimeter Secure Share can now be used to share objects from a SharePoint Online site.
- Removed the communication between the External Portal and SharePoint.
- You can now run the **PerimeterAgentPostInstall.exe** and **PerimeterManagerPostInstall.exe** via cmdlets to update the certificate for Perimeter Manager and Agent.

Known Issues

- In a SharePoint site where the **AvePoint Perimeter Secured Share** feature is active, when you select a document displayed in a Web part, if the toolbar type of the Web part is **Summary Toolbar** or **No Toolbar**, the **Secure Share** and **Manage Shared Files** buttons are not displayed or are disabled on the ribbon.

  Workaround:
  Edit the Web part and set the **Toolbar Type** to **Full Toolbar** or **Show Toolbar**.

- If your Perimeter administrator has enabled the Content Access Control for Secure Share and configured the location rules in the AvePoint Perimeter Management Console, users accessing the shared files through the Perimeter External Portal are required to provide their location information. If a user that uses Internet Explorer clicks **Continue** on the **Content Access Control** page and chooses to use a browser to provide location information, a confirmation window will appear asking for operations to allow Perimeter to track the physical location. If the user closes the confirmation window without selecting an option, the page will keep loading. This issue only exists when using Internet Explorer.
- When you access a library that has unique permissions with a user account that only has permissions to the library and does not have permissions to the site, access to the **Secure Share** window is denied.

- When opening a file with editing permissions using Office Web Apps on the AvePoint Perimeter External Portal, the controls cannot be properly rendered.
- When an XLSX file is edited in browser using the Excel Web App in the AvePoint Perimeter External Portal, the **Save a Copy** feature of the App does not work.
- When viewing document usage of the files within a shared folder using the **View Document Usage** feature in **Manage Shared Files**, the **View Document Usage** page does not display the user activities of the files residing in the sub folders under the selected folder.
- When opening a PDF file in the browser on the AvePoint Perimeter External Portal and Internal Portal, the aspect ratio of the page will automatically change.
- When you open an XLS file containing a table header in the browser in the AvePoint Perimeter External Portal and Internal Portal, the content of the file cannot be displayed completely. Root cause: This issue is caused by an issue that occurs when the PDF file converted from the XLS file is converted into a PNG image through Aspose.
- When opening a PPTX file containing SmartArt graphics in the browser on the AvePoint Perimeter Internal Portal and External Portal, the SmartArt graphics in the file cannot be displayed in the viewing page, and some text may not be displayed as well. Root cause: This issue is caused by an issue that occurs while the PPTX file is converted into a PDF file through Aspose.
- In the **Federation Policy** interface of AvePoint Perimeter Manager, the ADFS server installed on Windows 2012 R2 operating system where AvePoint Perimeter Agent resides is not displayed in the **Scope** pane.
- In AvePoint Perimeter Portal, when you open a shared file online using Internet Explorer 10 and click **Print** in the viewing page and click to print the file, the printed file contains blank pages.
- In AvePoint Perimeter 1.2, when sending a device enrollment request for enrolling a Windows Phone device with AvePoint Perimeter 1.3 Windows Phone app installed, in the enrollment page of the AvePoint Perimeter 1.3 Windows Phone app, the user enters the Device Service URL and E-mail Address provided in the enrollment request and clicks **Enroll**, a message appears displaying that **If there is an error with the security certificate of the entered Device Service URL, click here to install the certificate**. After clicking **here**, a Server Error web page appears. The Windows Phone device fails to install the certificate.

  Workaround:

  Manually export the SSL certificate of the AvePoint Perimeter Gateway's website as cert.p7b and import it into the …AvePoint/Perimeter/Manager/files/ folder on the Gateway server. Click here in the message on the enrollment page of the Windows Phone app to re-try install the certificate.

AvePoint Perimeter 1.9.1

Release Date: February 2018

New Features and Improvements

- The deletion operation in the **AppSettings.config** file can now be defined for users who are granted the **Delete** permission to shared items and they may now define if items will be permanently deleted instead of moved to the recycle bin
- Added the option for internal users to decide whether or not to share anonymous access or passcode-verified access to SharePoint content via **Secure Share**.

Known Issues

- In a SharePoint site where the **AvePoint Perimeter Secured Share** feature is active, when you select a document displayed in a Web part, if the toolbar type of the Web part is **Summary Toolbar** or **No Toolbar**, the **Secure Share** and **Manage Shared Files** buttons are not displayed or are disabled on the ribbon.

  Workaround:
  Edit the Web part and set the **Toolbar Type** to **Full Toolbar** or **Show Toolbar**.

- If your Perimeter administrator has enabled the Content Access Control for Secure Share and configured the location rules in the AvePoint Perimeter Management Console, users accessing the shared files through the Perimeter External Portal are required to provide their location information. If a user that uses Internet Explorer clicks **Continue** on the **Content Access Control** page and chooses to use a browser to provide location information, a confirmation window will appear asking for operations to allow Perimeter to track the physical location. If the user closes the confirmation window without selecting an option, the page will keep loading. This issue only exists when using Internet Explorer.
- When you access a library that has unique permissions with a user account that only has permissions to the library and does not have permissions to the site, access to the **Secure Share** window is denied.
- When opening a file with editing permissions using Office Web Apps on the AvePoint Perimeter External Portal, the controls cannot be properly rendered.
- When an XLSX file is edited in browser using the Excel Web App in the AvePoint Perimeter External Portal, the **Save a Copy** feature of the App does not work.
- When viewing document usage of the files within a shared folder using the **View Document Usage** feature in **Manage Shared Files**, the **View Document Usage** page does not display the user activities of the files residing in the sub folders under the selected folder.

- When opening a PDF file in the browser on the AvePoint Perimeter External Portal and Internal Portal, the aspect ratio of the page will automatically change.
- When you open an XLS file containing a table header in the browser in the AvePoint Perimeter External Portal and Internal Portal, the content of the file cannot be displayed completely. Root cause: This issue is caused by an issue that occurs when the PDF file converted from the XLS file is converted into a PNG image through Aspose.
- When opening a PPTX file containing SmartArt graphics in the browser on the AvePoint Perimeter Internal Portal and External Portal, the SmartArt graphics in the file cannot be displayed in the viewing page, and some text may not be displayed as well. Root cause: This issue is caused by an issue that occurs while the PPTX file is converted into a PDF file through Aspose.
- In the **Federation Policy** interface of AvePoint Perimeter Manager, the ADFS server installed on Windows 2012 R2 operating system where AvePoint Perimeter Agent resides is not displayed in the **Scope** pane.
- In AvePoint Perimeter Portal, when you open a shared file online using Internet Explorer 10 and click **Print** in the viewing page and click to print the file, the printed file contains blank pages.
- In AvePoint Perimeter 1.2, when sending a device enrollment request for enrolling a Windows Phone device with AvePoint Perimeter 1.3 Windows Phone app installed, in the enrollment page of the AvePoint Perimeter 1.3 Windows Phone app, the user enters the Device Service URL and E-mail Address provided in the enrollment request and clicks **Enroll**, a message appears displaying that **If there is an error with the security certificate of the entered Device Service URL, click here to install the certificate**. After clicking **here**, a Server Error web page appears. The Windows Phone device fails to install the certificate.

  Workaround:

  Manually export the SSL certificate of the AvePoint Perimeter Gateway's website as cert.p7b and import it into the …AvePoint/Perimeter/Manager/files/ folder on the Gateway server. Click here in the message on the enrollment page of the Windows Phone app to re-try install the certificate.

AvePoint Perimeter 1.9

Release Date: December 14, 2017

New Features and Improvements

- In the Perimeter Management Console **License Manager** page, administrators can remove licenses from inactive users or assign the license and secure shares of inactive users to other users.
- Secure Share feature allows internal users to share anonymous access links or one-time access verification links of shared items with others. The links can be used to view or download the shared items without having to sign into the External Portal.
- The External Portal, mobile apps, and e-mail notifications can now be displayed in Italian.
- Health monitoring timer jobs can now monitor and report the health of the Agent servers and the permission of the service accounts. The contact configured in the General Settings of the Perimeter Management Console will receive an e-mail if any potential issues are detected.
- Administrators can configure the license expiration alert settings to start sending e-mail alerts for the specified number of days before the license expires.
- Secure Share now allows internal users to select a list view to share the SharePoint properties of the shared items, and the properties will be displayed on the Perimeter Portals and mobile apps.
- Internal users can share items into a virtual folder to categorize the secure shares for specific users. The virtual folder can be accessed on the External Portal or on the **Documents** page of the Perimeter mobile app.
- You can now resend secure share notification e-mails with users if the external user loses the gateway link to Perimeter.
- Secure Share feature now allows internal users to share items to Active Directory groups.

Known Issues

- In a SharePoint site where the **AvePoint Perimeter Secured Share** feature is active, when you select a document displayed in a Web part, if the toolbar type of the Web part is **Summary Toolbar** or **No Toolbar**, the **Secure Share** and **Manage Shared Files** buttons are not displayed or are disabled on the ribbon.

  Workaround:
  Edit the Web part and set the **Toolbar Type** to **Full Toolbar** or **Show Toolbar**.

- If your Perimeter administrator has enabled the Content Access Control for Secure Share and configured the location rules in the AvePoint Perimeter Management Console, users

accessing the shared files through the Perimeter External Portal are required to provide their location information. If a user that uses Internet Explorer clicks **Continue** on the **Content Access Control** page and chooses to use a browser to provide location information, a confirmation window will appear asking for operations to allow Perimeter to track the physical location. If the user closes the confirmation window without selecting an option, the page will keep loading. This issue only exists when using Internet Explorer.

- When you access a library that has unique permissions with a user account that only has permissions to the library and does not have permissions to the site, access to the **Secure Share** window is denied.
- When opening a file with editing permissions using Office Web Apps on the AvePoint Perimeter External Portal, the controls cannot be properly rendered.
- When an XLSX file is edited in browser using the Excel Web App in the AvePoint Perimeter External Portal, the **Save a Copy** feature of the App does not work.
- When viewing document usage of the files within a shared folder using the **View Document Usage** feature in **Manage Shared Files**, the **View Document Usage** page does not display the user activities of the files residing in the sub folders under the selected folder.
- When opening a PDF file in the browser on the AvePoint Perimeter External Portal and Internal Portal, the aspect ratio of the page will automatically change.
- When you open an XLS file containing a table header in the browser in the AvePoint Perimeter External Portal and Internal Portal, the content of the file cannot be displayed completely. Root cause: This issue is caused by an issue that occurs when the PDF file converted from the XLS file is converted into a PNG image through Aspose.
- When opening a PPTX file containing SmartArt graphics in the browser on the AvePoint Perimeter Internal Portal and External Portal, the SmartArt graphics in the file cannot be displayed in the viewing page, and some text may not be displayed as well. Root cause: This issue is caused by an issue that occurs while the PPTX file is converted into a PDF file through Aspose.
- In the **Federation Policy** interface of AvePoint Perimeter Manager, the ADFS server installed on Windows 2012 R2 operating system where AvePoint Perimeter Agent resides is not displayed in the **Scope** pane.
- In AvePoint Perimeter Portal, when you open a shared file online using Internet Explorer 10 and click **Print** in the viewing page and click to print the file, the printed file contains blank pages.
- In AvePoint Perimeter 1.2, when sending a device enrollment request for enrolling a Windows Phone device with AvePoint Perimeter 1.3 Windows Phone app installed, in the enrollment page of the AvePoint Perimeter 1.3 Windows Phone app, the user enters the Device Service URL and E-mail Address provided in the enrollment request and clicks

Enroll, a message appears displaying that **If there is an error with the security certificate of the entered Device Service URL, click here to install the certificate**. After clicking **here**, a Server Error web page appears. The Windows Phone device fails to install the certificate.

Workaround:

Manually export the SSL certificate of the AvePoint Perimeter Gateway's website as cert.p7b and import it into the …AvePoint/Perimeter/Manager/files/ folder on the Gateway server. Click here in the message on the enrollment page of the Windows Phone app to re-try install the certificate.

AvePoint Perimeter 1.8.1

Release Date: June 13, 2017

New Features and Improvements

- General improvements for enhanced functionality.

Known Issues

- In a SharePoint site where the **AvePoint Perimeter Secured Share** feature is active, when you select a document displayed in a Web part, if the toolbar type of the Web part is **Summary Toolbar** or **No Toolbar**, the **Secure Share** and **Manage Shared Files** buttons are not displayed or are disabled on the ribbon.

  Workaround:
  Edit the Web part and set the **Toolbar Type** to **Full Toolbar** or **Show Toolbar**.

- If your Perimeter administrator has enabled the Content Access Control for Secure Share and configured the location rules in the AvePoint Perimeter Management Console, users accessing the shared files through the Perimeter External Portal are required to provide their location information. If a user that uses Internet Explorer clicks **Continue** on the **Content Access Control** page and chooses to use a browser to provide location information, a confirmation window will appear asking for operations to allow Perimeter to track the physical location. If the user closes the confirmation window without selecting an option, the page will keep loading. This issue only exists when using Internet Explorer.
- When you access a library that has unique permissions with a user account that only has permissions to the library and does not have permissions to the site, access to the **Secure Share** window is denied.
- When opening a file with editing permissions using Office Web Apps on the AvePoint Perimeter External Portal, the controls cannot be properly rendered.
- When an XLSX file is edited in browser using the Excel Web App in the AvePoint Perimeter External Portal, the **Save a Copy** feature of the App does not work.
- When viewing document usage of the files within a shared folder using the **View Document Usage** feature in **Manage Shared Files**, the **View Document Usage** page does not display the user activities of the files residing in the sub folders under the selected folder.
- When opening a PDF file in the browser on the AvePoint Perimeter External Portal and Internal Portal, the aspect ratio of the page will automatically change.
- When you open an XLS file containing a table header in the browser in the AvePoint Perimeter External Portal and Internal Portal, the content of the file cannot be displayed

completely. Root cause: This issue is caused by an issue that occurs when the PDF file converted from the XLS file is converted into a PNG image through Aspose.

- When opening a PPTX file containing SmartArt graphics in the browser on the AvePoint Perimeter Internal Portal and External Portal, the SmartArt graphics in the file cannot be displayed in the viewing page, and some text may not be displayed as well. Root cause: This issue is caused by an issue that occurs while the PPTX file is converted into a PDF file through Aspose.
- In the **Federation Policy** interface of AvePoint Perimeter Manager, the ADFS server installed on Windows 2012 R2 operating system where AvePoint Perimeter Agent resides is not displayed in the **Scope** pane.
- In AvePoint Perimeter Portal, when you open a shared file online using Internet Explorer 10 and click **Print** in the viewing page and click to print the file, the printed file contains blank pages.
- In AvePoint Perimeter 1.2, when sending a device enrollment request for enrolling a Windows Phone device with AvePoint Perimeter 1.3 Windows Phone app installed, in the enrollment page of the AvePoint Perimeter 1.3 Windows Phone app, the user enters the Device Service URL and E-mail Address provided in the enrollment request and clicks **Enroll**, a message appears displaying that **If there is an error with the security certificate of the entered Device Service URL, click here to install the certificate**. After clicking **here**, a Server Error web page appears. The Windows Phone device fails to install the certificate.

  Workaround:

  Manually export the SSL certificate of the AvePoint Perimeter Gateway's website as cert.p7b and import it into the …AvePoint/Perimeter/Manager/files/ folder on the Gateway server. Click here in the message on the enrollment page of the Windows Phone app to re-try install the certificate.

AvePoint Perimeter 1.8

Release Date: May 2, 2017

New Features and Improvements

- Load balance can now be configured for WOPI Host Servers.
- In Perimeter External Portal, users who have the Edit permission to the shared folder or library can now create new folders.
- Perimeter portals can now be displayed in German if the display language of your browser used to access Perimeter portals is German.
- When configuring outgoing e-mail settings, administrators can now choose whether or not to allow anonymous access to the SMTP server.
- The Perimeter administrator can now define a time duration in a configuration file to set up a default expiration time for each secure share. When internal users use Secure Share to share the items in a SharePoint site, a default expiration time will be automatically populated in the **Secure Share** window and internal users can also customize the expiration time in the **Secure Share** window.
- When searching on the Perimeter Portals using the Search box, you can now select a search scope for whether or not to include the search results in sub-folders.
- If the authentication type for logging into the Perimeter Internal Portal is set to Windows Authentication, internal users can automatically log into the Internal Portal with their Windows accounts.
- Users can now upload multiple files in bulk to the Perimeter External Portal. If Google Chrome is the browser used to browse the Perimeter External Portal, users can drag and drop a folder to upload the folder and the files within it to the External Portal.
- Users can now enroll a mobile device to multiple External Portals using the Perimeter mobile app for iOS or Android platform and swift between different portals in Perimeter mobile app to view and manage the shared items.
- The Perimeter mobile apps are now available in German for iOS devices and Android platforms.
- You can now deploy and use Perimeter in an environment with SQL Server 2016.
- Administrators can now activate external user accounts in the Perimeter Management Console after external users register in the Perimeter External Portal.
- Perimeter administrators can now enable features through a configuration file to allow users to register to External Portal when no items have been shared with them. With this feature enabled, the users that do not have access to the items can submit access

requests to them and the requests will be sent to the internal user who shared the items for approving.

Known Issues

- In a SharePoint site where the **AvePoint Perimeter Secured Share** feature is active, when you select a document displayed in a Web part, if the toolbar type of the Web part is **Summary Toolbar** or **No Toolbar**, the **Secure Share** and **Manage Shared Files** buttons are not displayed or are disabled on the ribbon.

  Workaround:
  Edit the Web part and set the **Toolbar Type** to **Full Toolbar** or **Show Toolbar**.

- If your Perimeter administrator has enabled the Content Access Control for Secure Share and configured the location rules in the AvePoint Perimeter Management Console, users accessing the shared files through the Perimeter External Portal are required to provide their location information. If a user that uses Internet Explorer clicks **Continue** on the **Content Access Control** page and chooses to use a browser to provide location information, a confirmation window will appear asking for operations to allow Perimeter to track the physical location. If the user closes the confirmation window without selecting an option, the page will keep loading. This issue only exists when using Internet Explorer.
- When you access a library that has unique permissions with a user account that only has permissions to the library and does not have permissions to the site, access to the **Secure Share** window is denied.
- When opening a file with editing permissions using Office Web Apps on the AvePoint Perimeter External Portal, the controls cannot be properly rendered.
- When an XLSX file is edited in browser using the Excel Web App in the AvePoint Perimeter External Portal, the **Save a Copy** feature of the App does not work.
- When viewing document usage of the files within a shared folder using the **View Document Usage** feature in **Manage Shared Files**, the **View Document Usage** page does not display the user activities of the files residing in the sub folders under the selected folder.
- When opening a PDF file in the browser on the AvePoint Perimeter External Portal and Internal Portal, the aspect ratio of the page will automatically change.
- When you open an XLS file containing a table header in the browser in the AvePoint Perimeter External Portal and Internal Portal, the content of the file cannot be displayed completely. Root cause: This issue is caused by an issue that occurs when the PDF file converted from the XLS file is converted into a PNG image through Aspose.
- When opening a PPTX file containing SmartArt graphics in the browser on the AvePoint Perimeter Internal Portal and External Portal, the SmartArt graphics in the file cannot be displayed in the viewing page, and some text may not be displayed as well. Root cause:

This issue is caused by an issue that occurs while the PPTX file is converted into a PDF file through Aspose.

- In the **Federation Policy** interface of AvePoint Perimeter Manager, the ADFS server installed on Windows 2012 R2 operating system where AvePoint Perimeter Agent resides is not displayed in the **Scope** pane.
- In AvePoint Perimeter Portal, when you open a shared file online using Internet Explorer 10 and click **Print** in the viewing page and click to print the file, the printed file contains blank pages.
- In AvePoint Perimeter 1.2, when sending a device enrollment request for enrolling a Windows Phone device with AvePoint Perimeter 1.3 Windows Phone app installed, in the enrollment page of the AvePoint Perimeter 1.3 Windows Phone app, the user enters the Device Service URL and E-mail Address provided in the enrollment request and clicks **Enroll**, a message appears displaying that **If there is an error with the security certificate of the entered Device Service URL, click here to install the certificate**. After clicking **here**, a Server Error web page appears. The Windows Phone device fails to install the certificate.

  Workaround:

  Manually export the SSL certificate of the AvePoint Perimeter Gateway's website as cert.p7b and import it into the …AvePoint/Perimeter/Manager/files/ folder on the Gateway server. Click here in the message on the enrollment page of the Windows Phone app to re-try install the certificate.

AvePoint Perimeter 1.7.1 for Mobile App

Release Date: November 18, 2016

New Features and Improvements

- When you upload a file to a shared folder or library through the AvePoint Perimeter Mobile app, you can now change the file name.
- If the mail app you use supports opening e-mail attachment in another app, you can tap **Copy to Perimeter** button to save the attachment to a shared folder or library through Perimeter Mobile app for iOS or Android. You can also change the file name before saving it.
- You can now save the cache for files that you edited while in Airplane Mode, and then automatically synchronize the edits to the SharePoint sites when the network is available.

AvePoint Perimeter 1.7

Release Date: November 3, 2016

New Features and Improvements

- AvePoint Perimeter now supports SharePoint 2016.
- If users are assigned with Edit permission to a virtual view, the edits made by this user can be saved back to SharePoint.
- There is now support for defining a password policy for external users to control the password strength and expiration.
- An SAP Jam group owner can now configure the SAP Jam group to integrate it with the AvePoint Perimeter External Portal. Therefore, in Perimeter External Portal, group owners can assign the shared SharePoint folder to all of the members in the SAP Jam group where this user is a group owner.
- External users can now log into the AvePoint External Portal using a username in addition to e-mail address.
- In the Perimeter Management Console, Perimeter administrators can manage and configure all of the rules and policies for the usage of Secure Share feature in the **Secure Share Control Policy** page. In this page, administrators 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.
- Perimeter administrators can configure Users and Groups Restriction rules in Perimeter Management Console to control the users and groups who can share SharePoint items with which permission level.
- Users can now drag and drop files into the AvePoint Perimeter External Portal for uploading.
- Users can now upload files from mobile devices via AvePoint Perimeter app.
- The **Document Attribute Based Restriction** rules now also work for folders, as well as documents.
- Support configuring a time range for sending update notifications in **AppSettings.config** file. The updates from the same user in the defined time range will trigger only one update notification.
- Support configuring rules in Users and Groups Restrictions to define the users or groups who can secure share items and the permission levels they can grant.

Known Issues

- In a SharePoint site where the **AvePoint Perimeter Secured Share** feature is active, when you select a document displayed in a Web part, if the toolbar type of the Web part is **Summary Toolbar** or **No Toolbar**, the **Secure Share** and **Manage Shared Files** buttons are not displayed or are disabled on the ribbon.

  Workaround:
  Edit the Web part and set the **Toolbar Type** to **Full Toolbar** or **Show Toolbar**.

- If your Perimeter administrator has enabled the Content Access Control for Secure Share and configured the location rules in the AvePoint Perimeter Management Console, users accessing the shared files through the Perimeter External Portal are required to provide their location information. If a user that uses Internet Explorer clicks **Continue** on the **Content Access Control** page and chooses to use a browser to provide location information, a confirmation window will appear asking for operations to allow Perimeter to track the physical location. If the user closes the confirmation window without selecting an option, the page will keep loading. This issue only exists when using Internet Explorer.
- When you access a library that has unique permissions with a user account that only has permissions to the library and does not have permissions to the site, access to the **Secure Share** window is denied.
- When opening a file with editing permissions using Office Web Apps on the AvePoint Perimeter External Portal, the controls cannot be properly rendered.
- When an XLSX file is edited in browser using the Excel Web App in the AvePoint Perimeter External Portal, the **Save a Copy** feature of the App does not work.
- When viewing document usage of the files within a shared folder using the **View Document Usage** feature in **Manage Shared Files**, the **View Document Usage** page does not display the user activities of the files residing in the sub folders under the selected folder.
- When opening a PDF file in the browser on the AvePoint Perimeter External Portal and Internal Portal, the aspect ratio of the page will automatically change.
- When you open an XLS file containing a table header in the browser in the AvePoint Perimeter External Portal and Internal Portal, the content of the file cannot be displayed completely. Root cause: This issue is caused by an issue that occurs when the PDF file converted from the XLS file is converted into a PNG image through Aspose.
- When opening a PPTX file containing SmartArt graphics in the browser on the AvePoint Perimeter Internal Portal and External Portal, the SmartArt graphics in the file cannot be displayed in the viewing page, and some text may not be displayed as well. Root cause: This issue is caused by an issue that occurs while the PPTX file is converted into a PDF file through Aspose.

- In the **Federation Policy** interface of AvePoint Perimeter Manager, the ADFS server installed on Windows 2012 R2 operating system where AvePoint Perimeter Agent resides is not displayed in the **Scope** pane.
- In AvePoint Perimeter Portal, when you open a shared file online using Internet Explorer 10 and click **Print** in the viewing page and click to print the file, the printed file contains blank pages.
- In AvePoint Perimeter 1.2, when sending a device enrollment request for enrolling a Windows Phone device with AvePoint Perimeter 1.3 Windows Phone app installed, in the enrollment page of the AvePoint Perimeter 1.3 Windows Phone app, the user enters the Device Service URL and E-mail Address provided in the enrollment request and clicks **Enroll**, a message appears displaying that **If there is an error with the security certificate of the entered Device Service URL, click here to install the certificate**. After clicking **here**, a Server Error web page appears. The Windows Phone device fails to install the certificate.

  Workaround:

  Manually export the SSL certificate of the AvePoint Perimeter Gateway's website as cert.p7b and import it into the …AvePoint/Perimeter/Manager/files/ folder on the Gateway server. Click here in the message on the enrollment page of the Windows Phone app to re-try install the certificate.

AvePoint Perimeter 1.6

Release Date: May 10, 2016

Supported Platforms

The AvePoint Perimeter mobile app is supported on Android, Apple, and Windows mobile devices.

New Features and Improvements

- Updated the Perimeter Apple Push notification certificate in AvePoint Perimeter 1.6.
- Added domain restrictions for Secure Share that define the domains that are allowed and blocked for users with whom files, folders, or libraries are shared. The domain users in the blocked list cannot have SharePoint files, folder, or libraries shared with them and they cannot register to the Perimeter External Portal.
- When sharing files, folders, or libraries via Secure Share in a SharePoint site, you can choose whether or not to send e-mail notifications to everyone with whom the file is currently shared once anyone updates the file or notify yourself once the file is downloaded by anyone else.
  When managing the shared files in Perimeter Internal Portal, as an internal user(a shared by user or site collection administrator), you can choose the notifications the shared by user will receive by selecting **Notify shared by users once this file is updated** option or the **Notify shared by users once this file is downloaded** option. In addition, you can choose whether or not to notify the shared with users when others in the sharing event update the file.
- When configuring the Virtual View folder, you can select the **Within** and **Older Than** options from the rule conditions list to include or exclude the SharePoint files created in a specific time period.
- 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 to the internal/external users that are from the designated location or location group or whose IP addresses lie in the designated range.
- Retention settings can now be enabled for deleting the cache of the shared files that have not been accessed within a configured time period. By default, the cache data of the shared files that are not edited, accessed, or downloaded within 30 days will be deleted from the Shared File Location with retention enabled. You can customize the time period in the **AppSettings.config** file.
- Users can be blocked from accessing shared content through the AvePoint mobile app if their locations or IP addresses are blocked according to Content Access Control for Secure Share rules.

- Users with whom files are shared can now click the link in the AvePoint Perimeter Secured Share Notification to render the shared folder directly in the AvePoint Perimeter External Portal.
- An IP location database can now be configured to allow Perimeter to locate users via IP address for secure share content access control.
- The uploaded or updated file is now displayed in the e-mail that is sent to notify users with whom a file is shared when anyone updates or uploads this file.
- Support displaying the user who shared files, folders, or a library with others by where the e-mail is from, by setting the value of the **IsEmailsenderisshareby** attribute in the **AppSettings.config** file to true.
- In the AvePoint Perimeter Internal Portal, site collection administrators can click the Unlock option in the settings drop-down list to unlock a shared file that is checked out or currently being edited by anyone.

Known Issues

- In a SharePoint site where the **AvePoint Perimeter Secured Share** feature is active, when you select a document displayed in a Web part, if the toolbar type of the Web part is **Summary Toolbar** or **No Toolbar**, the **Secure Share** and **Manage Shared Files** buttons are not displayed or are disabled on the ribbon.

  Workaround:

  Edit the Web part and set the **Toolbar Type** to **Full Toolbar** or **Show Toolbar**.

- If your Perimeter administrator has enabled the Content Access Control for Secure Share and configured the location rules in the AvePoint Perimeter Management Console, users accessing the shared files through the Perimeter External Portal are required to provide their location information. If a user that uses Internet Explorer clicks **Continue** on the **Content Access Control** page and chooses to use a browser to provide location information, a confirmation window will appear asking for operations to allow Perimeter to track the physical location. If the user closes the confirmation window without selecting an option, the page will keep loading. This issue only exists when using Internet Explorer.
- When you access a library that has unique permissions with a user account that only has permissions to the library and does not have permissions to the site, access to the **Secure Share** window is denied.
- When opening a file with editing permissions using Office Web Apps on the AvePoint Perimeter External Portal, the controls cannot be properly rendered.
- When an XLSX file is edited in browser using the Excel Web App in the AvePoint Perimeter External Portal, the **Save a Copy** feature of the App does not work.

- When viewing document usage of the files within a shared folder using the **View Document Usage** feature in **Manage Shared Files**, the **View Document Usage** page does not display the user activities of the files residing in the sub folders under the selected folder.
- When opening a PDF file in the browser on the AvePoint Perimeter External Portal and Internal Portal, the aspect ratio of the page will automatically change.
- When you open an XLS file containing a table header in the browser in the AvePoint Perimeter External Portal and Internal Portal, the content of the file cannot be displayed completely. Root cause: This issue is caused by an issue that occurs when the PDF file converted from the XLS file is converted into a PNG image through Aspose.
- When opening a PPTX file containing SmartArt graphics in the browser on the AvePoint Perimeter Internal Portal and External Portal, the SmartArt graphics in the file cannot be displayed in the viewing page, and some text may not be displayed as well. Root cause: This issue is caused by an issue that occurs while the PPTX file is converted into a PDF file through Aspose.
- In the **Federation Policy** interface of AvePoint Perimeter Manager, the ADFS server installed on Windows 2012 R2 operating system where AvePoint Perimeter Agent resides is not displayed in the **Scope** pane.
- In AvePoint Perimeter Portal, when you open a shared file online using Internet Explorer 10 and click **Print** in the viewing page and click to print the file, the printed file contains blank pages.
- In AvePoint Perimeter 1.2, when sending a device enrollment request for enrolling a Windows Phone device with AvePoint Perimeter 1.3 Windows Phone app installed, in the enrollment page of the AvePoint Perimeter 1.3 Windows Phone app, the user enters the Device Service URL and E-mail Address provided in the enrollment request and clicks **Enroll**, a message appears displaying that **If there is an error with the security certificate of the entered Device Service URL, click here to install the certificate**. After clicking **here**, a Server Error web page appears. The Windows Phone device fails to install the certificate.

  Workaround:

  Manually export the SSL certificate of the AvePoint Perimeter Gateway's website as cert.p7b and import it into the …AvePoint/Perimeter/Manager/files/ folder on the Gateway server. Click here in the message on the enrollment page of the Windows Phone app to re-try install the certificate.

AvePoint Perimeter 1.5

Release Date: January 19, 2016

Supported Platforms

The AvePoint Perimeter mobile app is supported on Android, Apple, and Windows mobile devices.

New Features and Improvements

- Improved user experience for entering e-mail addresses when sharing files. A box is now displayed around e-mail addresses to separate multiple e-mail addresses.
- The Perimeter administrator can now configure license consumption restrictions in the Secure Share Policy to only allow users imported from Active Directory to use the Secure Share feature.
- The Perimeter administrator can configure watermark settings at Web application level in Perimeter Manager to protect shared files with watermark. The Site Collection Administrator can break watermark setting inheritance and configure unique watermark settings for the sites within the site collection to protect shared files on the Internal Portal. The files shared with external users with Read-Only or Download permissions will be protected with a watermark. The shared files will be converted to PDF with a watermark when being viewed or downloaded.
- Perimeter mobile users on Android devices can view content from SharePoint and view or download shared files to a mobile device.
- Added the **View File with Watermark** permission to the Permission Level Capabilities table. The **View File with Watermark** permission is included in the Read Only permission level and Download permission level.
- Improved user experience in the **Share With** field of the Secure Share window when sharing files, folders, or a library with others. After you enter the e-mail addresses in the Invite people text box, you can choose whether or not to send an e-mail notification to them and deliver a personal message within the invitation.
- If you have registered an AvePoint Perimeter External Portal account, the user ID will be automatically populated in the Username field when you log into the External Portal by opening the URL for the shared content in the AvePoint Perimeter Secure Share Notification e-mail.
- The link of the Login page was added into the account activation failure error message in order to help users quickly access the Login page.
- A message now displays when users choose to enable watermark settings to indicate that the files that cannot be converted to PDF will not be protected by watermark.

- Site collection administrators can now configure the watermark settings for each site within a site collection.
- In the Action menu of the External Portal, exchange the positions of the **Upload a New Version** option and the **Download & Lock for Editing** option.
- Internal users can now use their e-mail address as their user ID to log into the External Portal.
- Screenshot capturing using an Android device is no longer possible.

Bug Fixes

- When opening an XLSX file using the Microsoft Excel Web App in Internet Explorer 11, the **EDIT IN BROWSER** button will now function properly.

Known Issues

- When opening an XLS file containing a table header in the browser from the AvePoint Perimeter External Portal and Internal Portal, the content of the file cannot be displayed completely. This issue occurs when the PDF file converted from XLS file is converted into a PNG image through Aspose.
- When opening a PPTX file containing SmartArt graphics in the browser on the AvePoint Perimeter Internal Portal and External Portal, the SmartArt graphics in the file cannot be displayed in the viewing page, and some text may not be displayed. This issue is caused by an issue that occurs while the PPTX file is converted into a PDF file through Aspose.
- In AvePoint Perimeter 1.2, when sending a device enrollment request for enrolling a Windows Phone device with AvePoint Perimeter 1.3 Windows Phone app installed, in the enrollment page of the AvePoint Perimeter 1.3 Windows Phone app, the user enters the Device Service URL and E-mail Address provided in the enrollment request and clicks **Enroll**, a message appears displaying that **If there is an error with the security certificate of the entered Device Service URL, click here to install the certificate**. After clicking **here**, a Server Error web page appears. The Windows Phone device fails to install the certificate.

  Workaround:

  Manually export the SSL certificate of the AvePoint Perimeter Gateway's website as cert.p7b and import it into the …AvePoint/Perimeter/Manager/files/ folder on the Gateway server. Click here in the message on the enrollment page of the Windows Phone app to re-try install the certificate.
- In a SharePoint site where the AvePoint Perimeter Secured Share feature is active, if a document that is displayed in a Web part is selected and the toolbar type of the Web part is **Summary Toolbar** or **No Toolbar**, the Secure Share and Manage Shared Files buttons may not display or may be disabled on the ribbon.

Workaround:
Edit the Web part and set the **Toolbar Type** to **Full Toolbar** or **Show Toolbar**.

- On the **Federation Policy** interface of the AvePoint Perimeter Manager, AD FS servers that are on the Windows 2012 R2 operating system and that contain AvePoint Perimeter Agents are not displayed in the **Scope** pane.
- When opening a file with editing permissions using Office Web Apps on the AvePoint Perimeter External Portal, the controls cannot be properly rendered.
- When an XLSX file is edited in a browser using the Excel Web App on the AvePoint Perimeter External Portal, the **Save a Copy** feature of the App will not work.
- When using the **View Document Usage** feature in **Manage Shared Files** to view usage of files within a shared folder, the **View Document Usage** page does not display user activity on files in sub folders.
- When opening a PDF file in the browser on the AvePoint Perimeter External Portal and Internal Portal, the aspect ratio of the page will automatically change.

AvePoint Perimeter 1.4.2

Release Date: September 2, 2015

Supported Platforms

The AvePoint Perimeter mobile app is supported on Android, Apple and Windows mobile devices.

New Features and Improvements

- Added Japanese language support.

Known Issues

- In a SharePoint site where the AvePoint Perimeter Secured Share feature is active, if a document that is displayed in a Web part is selected and the toolbar type of the Web part is **Summary Toolbar** or **No Toolbar**, the Secure Share and Manage Shared Files buttons may not display or may be disabled on the ribbon.

  Workaround: Edit the Web part and set the Toolbar Type to Full Toolbar or Show Toolbar.

- On the **Federation Policy** interface of the AvePoint Perimeter Manager, AD FS servers that are on the Windows 2012 R2 operating system and that contain AvePoint Perimeter Agents are not displayed in the **Scope** pane.
- When opening a file with editing permissions using Office Web Apps on the AvePoint Perimeter External Portal, the controls cannot be properly rendered.
- When an XLSX file is edited in a browser using the Excel Web App on the AvePoint Perimeter External Portal, the **Save a Copy** feature of the App will not work.
- When using the **View Document Usage** feature in **Manage Shared Files** to view usage of files within a shared folder, the **View Document Usage** page does not display user activity on files in sub folders.
- When opening a PDF file in the browser on the AvePoint Perimeter External Portal and Internal Portal, the aspect ratio of the page will automatically change.
- When opening an XLS file containing a table header in the browser from the AvePoint Perimeter External Portal and Internal Portal, the content of the file cannot be displayed completely. This issue occurs when the PDF file converted from XLS file is converted into a PNG image through Aspose.
- When opening an XLSX file using the Microsoft Excel Web App in Internet Explorer 11, the **EDIT IN BROWSER** button may not work. This issue is caused by an Internet Explorer 11 compatibility issue with Microsoft Excel Web App.

Workaround:

1. Go to the installation directory of the Office Web Apps: …*Microsoft Office Web Apps\ExcelServicesWfe_layouts*
2. Copy and paste the **XLViewerInternal.aspx** to another location as a backup
3. Open the **XLViewerInternal.aspx** file using Notepad under the …*Microsoft Office Web Apps\ExcelServicesWfe_layouts* directory
4. Within the **<head>** node, locate the **<meta>** sub node that containing the **http-equiv** and **content** attributes
5. Change the value of the **content** attribute to **IE=10**
6. Save the change and close the file.

AvePoint Perimeter 1.4.1

Release Date: June 9, 2015

Supported Platforms

The AvePoint Perimeter mobile app is supported on Android, Apple and Windows mobile devices.

New Features and Improvements

AvePoint Perimeter Manager

- Internal users can submit an enrollment request on the AvePoint Perimeter External Portal by clicking the **Enroll New Device** link on the External Portal. To disable the **Enroll New Device** feature for internal users on the External Portal, locate the AppSettings.config file in the ...\AvePoint\Perimeter\Manager directory, and set the value of the **internalUserSelfEnrollEnabled** attribute to false.

Known Issues

- In a SharePoint site where the AvePoint Perimeter Secured Share feature is active, if a document that is displayed in a Web part is selected and the toolbar type of the Web part is **Summary Toolbar** or **No Toolbar**, the Secure Share and Manage Shared Files buttons may not display or may be disabled on the ribbon.

  Workaround: Edit the Web part and set the Toolbar Type to Full Toolbar or Show Toolbar.

- On the **Federation Policy** interface of the AvePoint Perimeter Manager, AD FS servers that are on the Windows 2012 R2 operating system and that contain AvePoint Perimeter Agents are not displayed in the **Scope** pane.
- When opening a file with editing permissions using Office Web Apps on the AvePoint Perimeter External Portal, the controls cannot be properly rendered.
- When an XLSX file is edited in a browser using the Excel Web App on the AvePoint Perimeter External Portal, the **Save a Copy** feature of the App will not work.
- When using the **View Document Usage** feature in **Manage Shared Files** to view usage of files within a shared folder, the **View Document Usage** page does not display user activity on files in sub folders.
- When opening a PDF file in the browser on the AvePoint Perimeter External Portal and Internal Portal, the aspect ratio of the page will automatically change.
- When opening an XLS file containing a table header in the browser from the AvePoint Perimeter External Portal and Internal Portal, the content of the file cannot be displayed

completely. This issue occurs when the PDF file converted from XLS file is converted into a PNG image through Aspose.

- When opening an XLSX file using the Microsoft Excel Web App in Internet Explorer 11, the **EDIT IN BROWSER** button may not work. This issue is caused by an Internet Explorer 11 compatibility issue with Microsoft Excel Web App.

  Workaround:

  1. Go to the installation directory of the Office Web Apps: ...*Microsoft Office Web Apps\ExcelServicesWfe_layouts*
  2. Copy and paste the **XLViewerInternal.aspx** to another location as a backup
  3. Open the **XLViewerInternal.aspx** file using Notepad under the ...*Microsoft Office Web Apps\ExcelServicesWfe_layouts* directory
  4. Within the **<head>** node, locate the **<meta>** sub node that containing the **http-equiv** and **content** attributes
  5. Change the value of the **content** attribute to **IE=10**
  6. Save the change and close the file

AvePoint Perimeter 1.4

Release Date: April 28, 2015

Supported Platforms

The AvePoint Perimeter mobile app is supported on Android, Apple and Windows mobile devices.

New Features and Improvements

AvePoint Perimeter Manager

- Redesign of the Perimeter Manager user interface.
- The **Install Gateway** and **Install Portal** options have been removed from the AvePoint Perimeter Manager Installation Wizard – in Perimeter 1.4, the Gateway and External Portal must be installed together on the same server.
- Examples are now provided on how to configure the **OWA Server URL** and **WOPI Host Server URL** fields in the **Office Web Apps Server Settings** interface.
- Added the Office Web Apps Server Settings feature to Perimeter Manager for configuring an Office Web Apps (OWA) server for AvePoint Perimeter Internal Portal and External Portal to enable users to open and edit shared files in a browser using Office Web Apps.
- The Perimeter 1.4 license now includes the **total user quantity** field to display the total number of internal end-users that can be registered into the Perimeter management system per license.
- E-mail notifications are now sent under the following conditions:
    - When a folder or library is shared by an internal user from SharePoint using the AvePoint Perimeter Pro Secured Share feature, an e-mail notification will be sent to each user with whom the folder/library is shared.
    - When a shared file/folder/library is updated from the AvePoint Perimeter External Portal, an e-mail notification will be sent to the user who shared this object with the modifier.
    - When a shared file/folder/library is updated from the SharePoint side, an e-mail notification will be sent to each user with whom the object is shared.
    - When a file has been locked for editing by a user for more than a specified period, an e-mail notification will be sent to request the user unlock the file.

    - When an internal user's secure sharing permission settings for a file/folder/library has been overwritten by another user, an e-mail notification will be sent to the user.

- E-mail notifications sent by Perimeter now display the time in the following format: **MM/DD/YYYY HH:MM(time zone)**.
- The template for e-mail notifications sent for **Enterprise Wipe** has been standardized.
- In the **Agent** tab of Log Manager, the checkboxes for the Agents whose services are down are now able to be unselected.
- In the **Configure** interface for an Agent in **Agent Monitor**, the name of the Agent that is being configured is displayed on the ribbon.

AvePoint Perimeter Internal/External Portal

- AvePoint Perimeter External Portal users who are granted Edit permission to shared folders/libraries can now share files back to SharePoint by uploading files to shared folders/libraries in the External Portal.
- Users can now download a copy of the file that is opened in FlexPaper on the AvePoint Perimeter External Portal and Internal Portal.
- With an Office Web Apps (OWA) Server configured for the AvePoint Perimeter External Portal, the External Portal now supports opening and editing shared files with .docx, .xlsx, and .pptx formats in a browser via Office Web Apps.
- The **Annotation** function has been removed from the FlexPaper page where shared files are opened from the External Portal.
- The text in the body of the **AvePoint Perimeter External Portal Account Activation** e-mail notification is updated.
- The **Country/Region** and **State/Province** fields are now optional for the **Account Registration** page on the AvePoint Perimeter External Portal.
- After a user clicks the **SIGN UP** link on the **AvePoint Perimeter Secure Share Notification** e-mail and opens the **Account Registration** page for the AvePoint Perimeter External Portal, the user's e-mail address is automatically filled into the **User ID** field.
- Users can now view document usage of files within shared folders and libraries in the AvePoint Perimeter Internal Portal.
- A default domain name for internal users can now be configured on the **Login** page of the AvePoint Perimeter Internal Portal.
- If a user clicks on the file name of a shared file whose file format is not supported for online viewing on the AvePoint Perimeter External Portal and Internal Portal and the user

has the download permission for this file, the download bar or pop-up window for this file will appear and the user can download a copy of this file.

- When a user clicks on a shared file name to open it online on the AvePoint Perimeter External Portal, but the file type is unsupported for online viewing and the user does not have the download permission for this file, the following message appears: **This file cannot be opened online. The file format is not supported. To download a copy, please contact the user who shared the file with you to update permission settings.**
- The action menu for a shared object on the AvePoint Perimeter External Portal now includes an **Unlock** option for users to unlock files they have locked for editing.
- Additional file types can now be opened on the AvePoint Perimeter External Portal and Internal Portal – the following file types are supported for online viewing: **doc**, **.docx**, **.txt**, **.vsd**, **.vsdx**, **.ppt**, **.pptx**, **.xls**, **.xlsx**, **.mpp**, **.html**, **.htm**, **.jpg**, **.png**, **.gif**, **.pdf**, **.pcl**, **.xps**, **.svg**, and **.dwg**.

AvePoint Perimeter Secured Share Feature

- Users can now share folders and libraries using the AvePoint Perimeter Pro Secured Share feature in SharePoint.
- In the **AvePoint Perimeter: Secured Sharing Permissions Overwritten** e-mail notification, the e-mail address of the user whose permission for the shared file has been overwritten is now displayed.
- There is now a tooltip for the **Edit in Browser Only** permission level to inform users that online editing is only supported for PPTX, DOCX, and XLSX files where internal users can configure secured share permission settings for shared objects on the **Secured Share** window and the **Permission Level Capacities** window in the SharePoint sites where the Secured Share feature is deployed and on the **Manage Permissions** interface on the Internal Portal.
- Support using the AvePoint Perimeter Pro **Secured Share** feature to share files stored in **SkyDrive Pro.**
- The salutation has been removed from **AvePoint Perimeter Secure Share Notification** e-mails.

AvePoint Perimeter iOS App

- Users can now view files within folders and libraries shared via the AvePoint Perimeter Pro Secured Share feature using the AvePoint Perimeter app on enrolled iOS devices.
- The version number for the AvePoint Perimeter app for iPad, iPhone, and iPod Touch is updated to **1.4** and the copyright message is updated to **© 2013-2015 AvePoint, Inc. All Rights Reserved.**

Known Issues

- In a SharePoint site where the AvePoint Perimeter Secured Share feature is active, if a document that is displayed in a Web part is selected and the toolbar type of the Web part is **Summary Toolbar** or **No Toolbar**, the Secure Share and Manage Shared Files buttons may not display or may be disabled on the ribbon.

  Workaround: Edit the Web part and set the **Toolbar Type** to **Full Toolbar** or **Show Toolbar**.
- On the **Federation Policy** interface of the AvePoint Perimeter Manager, AD FS servers that are on the Windows 2012 R2 operating system and that contain AvePoint Perimeter Agents are not displayed in the **Scope** pane.
- When opening a file with editing permissions using Office Web Apps on the AvePoint Perimeter External Portal, the controls cannot be properly rendered.

- When an XLSX file is edited in a browser using the Excel Web App on the AvePoint Perimeter External Portal, the **Save a Copy** feature of the App will not work.
- When using the **View Document Usage** feature in **Manage Shared Files** to view usage of files within a shared folder, the **View Document Usage** page does not display user activity on files in sub folders.
- When opening a PDF file in the browser on the AvePoint Perimeter External Portal and Internal Portal, the aspect ratio of the page will automatically change.
- When opening an XLS file containing a table header in the browser from the AvePoint Perimeter External Portal and Internal Portal, the content of the file cannot be displayed completely. This issue occurs when the PDF file converted from XLS file is converted into a PNG image through Aspose.
- When opening an XLSX file using the Microsoft Excel Web App in Internet Explorer 11, the **EDIT IN BROWSER** button may not work. This issue is caused by an Internet Explorer 11 compatibility issue with Microsoft Excel Web App.

  Workaround:

  1. Go to the installation directory of the Office Web Apps: ...*Microsoft Office Web Apps\ExcelServicesWfe_layouts*
  2. Copy and paste the **XLViewerInternal.aspx** to another location as a backup
  3. Open the **XLViewerInternal.aspx** file using Notepad under the ...*Microsoft Office Web Apps\ExcelServicesWfe_layouts* directory
  4. Within the **<head>** node, locate the **<meta>** sub node that containing the **http-equiv** and **content** attributes
  5. Change the value of the **content** attribute to **IE=10**
  6. Save the change and close the file

AvePoint Perimeter 1.3.1

Release Date: October 7, 2014

Supported Platforms

The AvePoint Perimeter mobile app is supported on Android and Apple mobile devices.

Bug Fixes

- Fixed an issue with incorrect license version information being displayed in License Manager.
- Users will no longer receive duplicate Burglar Alarm Suspicious Activity Alert e-mails.
- The Retrieve Audit Data feature automatically excludes system accounts while retrieving audit data from a SharePoint farm.

Known Issues

- In the Federation Policy interface of AvePoint Perimeter Manager, an ADFS server installed on Windows 2012 R2 Operating System with a Perimeter Agent does not display in the **Scope** panel.
- In AvePoint Perimeter Portal, opening a shared file online using Internet Explorer 10 and printing may produce some blank pages.
- In the Burglar Alarm Report interface, viewing the details a Document Activity Burglar Alarm rule may display more events than the **Number of Events** value displayed in the Burglar Alarm Report interface.
- In a SharePoint site where the AvePoint Perimeter Secured Share feature is active and a document is displayed in a Web part, **Summary Toolbar** or **No Toolbar** types cause the Secure Share and Manage Shared Files buttons to not display correctly on the ribbon. **Workaround:** Edit the Web part and set the **Toolbar Type** to **Full Toolbar** or **Show Toolbar**.
- Enabling the 2-factor authentication feature on an Active Directory Federation Services (ADFS) server and then attempting to authenticate into a site within a replying party of this ADFS server may result in the user not being able to access the page.

  Workaround: Export the relying party server's token-decrypting certificate, including the private key, and then import it to the corresponding claims provider server.

AvePoint Perimeter 1.3

Release Date: September 16, 2014

Supported Platforms

The AvePoint Perimeter mobile app is supported on Android and Apple mobile devices.

New Features and Improvements

- Added the **Windows Phone Logs** feature to the **Configure** menu of AvePoint Perimeter Manager.
- Perimeter now sends alert e-mails to administrators and direct managers for suspicious user activities identified by **Burglar Alarm Rules**.
- Added the **Burglar Alarm Report** feature into the **Report** menu, which displays suspicious user activity identified by **Burglar Alarm Rules**.
- Added the **Daily Audit Tracking** report to allow users to view all end-user activities within a specific day or date range.
- Added the **Retrieve Audit Data** feature, which retrieves SharePoint audit data and stores it in the Manager Configuration database.
- Windows Phone devices can now be enrolled into the AvePoint Perimeter management system.
- Integrated 2-Factor Authentication with the Authentication feature of the Windows Phone app.
- Added support for data synchronization between the AvePoint Perimeter Manager server and the Windows Phone app.
- Renamed the **Content Access Logs** feature to **Event Logs**.
- Added a tooltip for the **Apply Now** button in the **Configure** interface of the SharePoint Audit Settings feature, informing the user that the current SharePoint audit settings will be overwritten.
- Standardized various e-mail templates.
- Added support for viewing 2D AutoCAD 2004 DWG files online.
- Improved the interaction styles for the **Add Locations to Groups** drop-down lists in the pages for adding/editing location groups, and using the **Manage Location Groups** feature.
- Renamed the **Updates** interface to **Notification** in iOS.

- In the **Documents/SharePoint** interface, added support for viewing all available actions for a document/item by clicking the information icon next to the document name or the right arrow button next to the item name.
- Perimeter now automatically performs a heartbeat to synchronize the data of managed SharePoint site settings and Secured Share permission settings from the AvePoint Perimeter Manager server every 2 hours with WIFI connection or 6 hours with GPS connection.

Known Issues

- In the Federation Policy interface of AvePoint Perimeter Manager, an ADFS server installed on Windows 2012 R2 Operating System with a Perimeter Agent does not display in the **Scope** panel.
- In AvePoint Perimeter Portal, opening a shared file online using Internet Explorer 10 and printing may produce some blank pages.
- In the Burglar Alarm Report interface, viewing the details a Document Activity Burglar Alarm rule may display more events than the **Number of Events** value displayed in the Burglar Alarm Report interface.
- In a SharePoint site where the AvePoint Perimeter Secured Share feature is active and a document is displayed in a Web part, **Summary Toolbar** or **No Toolbar** types cause the Secure Share and Manage Shared Files buttons to not display correctly on the ribbon. **Workaround:** Edit the Web part and set the **Toolbar Type** to **Full Toolbar** or **Show Toolbar**.
- Enabling the 2-factor authentication feature on an Active Directory Federation Services (ADFS) server and then attempting to authenticate into a site within a replying party of this ADFS server may result in the user not being able to access the page.

  Workaround: Export the relying party server's token-decrypting certificate, including the private key, and then import it to the corresponding claims provider server.

AvePoint Perimeter 1.2

Release Date: May 1, 2014

Supported Platforms

The AvePoint Perimeter mobile app is supported on Android and Apple mobile devices.

New Features and Improvements

- Added the **User Access Group** feature in Perimeter Manager. In **User Access Group**, Perimeter administrators can create and manage user access groups, which contain both internal users and external users based on predefined parameters. User access groups can be dynamic or static, and are primarily used to assign permissions to the shared documents contained within virtual views.
- Added the **Virtual Views** feature in Perimeter Manager. In **Virtual Views**, Perimeter administrators can create and manage the virtual views used to share a group of SharePoint files based on configured rules and user access groups.
- After the AvePoint Perimeter Secured Share feature is activated in the SharePoint site, the **Manage Share Files** button will appear next to the **Secure Share** button on the ribbon. Internal users can go to the AvePoint Perimeter Internal Portal to manage shared files by clicking **Manage Share Files**.
- Added the **Manage External Users** feature to enable Perimeter administrators to view and manage all external users registered within the AvePoint Perimeter Portal.
- Added instructions in e-mail notifications and the AvePoint Perimeter Portal to tell users how to sign up to the AvePoint Perimeter Portal, activate an account, and reset a password.
- Added the **Shared File Location** feature for configuring the UNC path of a location used to store shared files that were downloaded from SharePoint.
- Added the **System Credentials** feature for configuring system credentials used to download shared files from SharePoint.
- Support for viewing shared files' document usage details in the **Manage Shared Files** interface of Perimeter Manager or the **All Shared Files** and **My Shared Files** interfaces of the AvePoint Perimeter Internal Portal.
- Support for adding annotations to copies of shared files in AvePoint Perimeter Portal.
- External users can now reset their AvePoint Perimeter Portal account passwords by clicking **Forgot password?** on the login page.
- Admins can now add custom properties into external user profiles by configuring the **SecureShareConfig.xml** file in the *bin\Config* folder located under the AvePoint Perimeter Manager installation path.

- Support for viewing logs that details every time a shared file was viewed via the AvePoint Perimeter mobile app and AvePoint Perimeter Portal.
- Support for changing shared files' permissions settings in the **All Shared Files** and **My Shared Files** interfaces of the AvePoint Perimeter Internal Portal.
- Added the **Managed Site Collections** feature to enable site collection administrators to add managed site collections. They can view all of the shared files within the managed site collections on the **All Shared Files** tab and Dashboard.
- In the Dashboard of the AvePoint Perimeter Internal Portal, site collection users can view the number of shared files and recently shared files within each managed site collection.
- Added license control over the **AvePoint Perimeter Secured Share** feature in SharePoint and the **Virtual Views** feature in Perimeter Manager.
- If the **External** option is selected as the user type in the **Enroll New Device** interface, the external user's organization e-mail address can be the username by selecting **Use e-mail address as username** checkbox.
- Support for viewing offline copies of shared files downloaded from SharePoint on mobile devices.
- Support for changing the expiration time of shared files in **My Shared Files** and **All Shared Files** interfaces of AvePoint Perimeter Internal Portal.
- Support for searching shared files by file name in the **Documents** interface of the AvePoint Perimeter app.

Known Issues

- In a SharePoint site where the AvePoint Perimeter Secured Share feature is active and a document is displayed in a Web part, **Summary Toolbar** or **No Toolbar** types cause the Secure Share and Manage Shared Files buttons to not display correctly on the ribbon. **Workaround:** Edit the Web part and set the **Toolbar Type** to **Full Toolbar** or **Show Toolbar**.
- Enabling the 2-factor authentication feature on an Active Directory Federation Services (ADFS) server and then attempting to authenticate into a site within a replying party of this ADFS server may result in the user not being able to access the page.

  Workaround: Export the relying party server's token-decrypting certificate, including the private key, and then import it to the corresponding claims provider server.

AvePoint Perimeter 1.1.1

Release Date: February 7, 2014

Supported Platforms

The AvePoint Perimeter mobile app is supported on Android and Apple mobile devices.

New Features and Improvements

- Added **1 GB or greater** as the recommended **Available Disk Space** into the **Manager Installation Scan Rules for Windows Server Editions** webpage.
- Renamed **API Controller to AvePoint Perimeter Gateway**.
- Renamed the **Manager Installation Scan Rules for Windows Server 2012/Windows Server 2008 R2** webpage to **Manager Installation Scan Rules for Windows Server Editions**.
- Added **Windows Server 2008** to the **Support Condition for Operating System Edition**.
- Improved the installation process for the Perimeter Gateway and Geolocation database:
    - Separated the process of installing the Manager GUI from installing the Gateway. Users can install them on the same machine or different machines using the installer, and then publish the Gateway to the Internet.
    - Users can now remotely install the Geolocation database using the installer. Users can choose whether to install the Geolocation database immediately after the Manager installation or install it later.
    - To define location groups based on geographic and boundary data stored in the Geolocation Database in Perimeter Manager, users must connect the Perimeter Manager to an available Geolocation database using the Geolocation Database feature.

Bug Fixes

- Fixed a bug that occurred in the **Access Warning Logs** report interface. This section allows administrators to view the corresponding access warning records within the current selected time range. Previously, on occasion no data would display in the report displaying pane.

Known Issues

- Enabling the 2-factor authentication feature on an Active Directory Federation Services (ADFS) server and then attempting to authenticate into a site within a replying party of this ADFS server may result in the user not being able to access the page.

Workaround: Export the relying party server's token-decrypting certificate, including the private key, and then import it to the corresponding claims provider server.

AvePoint Perimeter 1.1

Release Date: December 27, 2013

Supported Platforms

The AvePoint Perimeter mobile app is supported on Android and Apple mobile devices.

New Features

Additional Support

- Added support for the Android platform.
- AvePoint Perimeter Manager and Agents are FIPS 140-2 compliant.

Security Enhancements

- When the AvePoint Perimeter service is not available, the SharePoint environment protected by AvePoint Perimeter is inaccessible, and a fail close page is displayed.
- Added 2-Factor Authentication Logs, which display logs of all attempts to access sites with 2-factor authentication.
- Added support for 2-factor authentication for sites using ADFS authentication.
- Perimeter now checks whether the device is a rooted Android device or a jailbroken iOS device each time the AvePoint Perimeter app is started. The AvePoint Perimeter app cannot run on a rooted or jailbroken device.
- Added functionality to prevent the Android device from reporting fake locations to the Perimeter Manager, ensuring that the Perimeter Manager can get actual location information from each Android device.
- Added a section in the interface for configuring a time-out period for 2-factor authentication for SharePoint on-premises sites.
- Added support for accessing Forms-based authentication SharePoint sites and Claims-based authentication sites.

Perimeter Management Enhancements

- Added functionality to quickly and easily update the following three components of AvePoint Perimeter:
    - Update the AvePoint Perimeter app for iPhone, iPad, and iPod touch.
    - Update the AvePoint Perimeter Manager.
    - Update the AvePoint Perimeter Agent.

- Added the **Manage Login Account** function to achieve **User** and **Login Account** separation.
- Added the Log Manager for managing logs of all jobs.
- Added the **Manage Location Groups** feature to combine multiple locations into a single group. This can help define boundaries by taking into account various smaller locations, and creating custom shapes with multiple locations.
- Added support to perform an action on multiple devices at one time in **Manage Enrolled Devices**.
- Added the **Bulk Device Enrollment** feature to support enrolling multiple devices simultaneously.
- Added support for searching users using the **Advanced Search** in the **Manage Users** interface.
- Added the **Remove** button into the Agent Monitor to enable users to remove Agents.
- Added the **Delete Cache** feature to the page for configuring a SharePoint site's settings. This feature allows users to delete the local cache files for the SharePoint contents they have viewed in that particular site.

Usability Enhancements

- Added support for customization of Web pages and e-mail templates for AvePoint Perimeter.
- Added an optional Geolocation database to support defining locations based on geographic and political boundaries.
- Added the **Export Report** feature, which supports selecting **Export Scope** and **Report Format** of the exported report file.

Improvements and Bug Fixes

- Performing the Enterprise Wipe action to a specific enrolled device in the **Manage Enrolled Devices** interface no longer results in the page perpetually loading.
- Added icons for the statuses displayed in the **Status** column in the **Device Enrollment** interface.
- In the interface for assigning or editing permission of managed SharePoint sites to device groups, added a link to access the **New Device Group** page.
- In the **SharePoint Policy** interface, added checkmarks on the site collections icons to show that you have configured **Content Access Control** rules for those site collections.
- Added support for configuring an expiration time of each device enrollment request in the **Enroll New Device** page.

- Changed the actions for managing enrolled devices. **Disable Authentication** in 1.0 is changed to **Disable** in 1.1, which is used to disable the AvePoint Perimeter app in the enrolled device. **Deactivate** in 1.0 is removed in 1.1.
- Added options for removing the Manager Configuration database and the Geolocation database in the **Welcome** page of **Manager Uninstallation Wizard**.
- Imported "location" attributes from Active Directory can be used as filter conditions while creating device groups.
- Added a message bar to inform the user where to view job details when a Log Collection job begins.
- Enhancements to the Geolocation boundaries of certain countries and districts.
- In the page for creating a new geographic location group, moved the **Select All** option above the line to separate it from the list of districts in the **District** column.
- Added display of what lists/libraries are selected for each site in the diagnostic logs of AvePoint Perimeter app.
- Added support for viewing Calendar lists using the app on iPhone and iPad.
- Added support to allow end users to select which lists/libraries they want to display when viewing SharePoint sites on the app.
- Added buttons to the **UIWebView** for browsing Wiki pages within the app.
- The button for switching between **Online** reading mode and **Offline** reading mode lights up in **Online** mode and greys out in **Offline** mode.
- Enhanced the pop-up error message that appears when there is no available network for accessing SharePoint sites.

Known Issues

- Enabling the 2-factor authentication feature on an Active Directory Federation Services (ADFS) server and then attempting to authenticate into a site within a replying party of this ADFS server may result in the user not being able to access the page.

  Workaround: Export the relying party server's token-decrypting certificate, including the private key, and then import it to the corresponding claims provider server.

AvePoint Perimeter 1.0

Release Date: October 15, 2013

Known Issues

- When performing the Enterprise Wipe action to a specific enrolled device in the **Manage Enrolled Devices** interface, the page keeps loading after the action is initiated.

  Root cause: This issue is caused by an undefined value that occurs in the front-end JavaScript code after the Enterprise Wipe action is initiated.

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

Trademarks

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, NJ 07310
USA