AvePoint Compliance Guardian

Technical Overview

# AvePoint Perimeter

## for Microsoft SharePoint

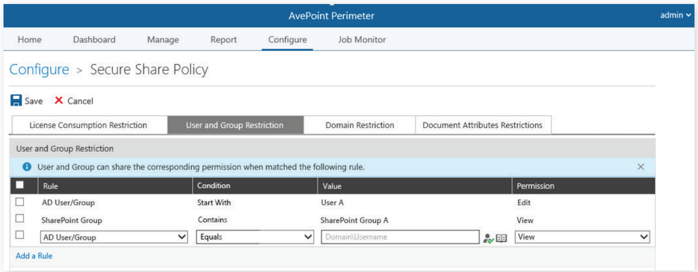
## On Point. Out-of-the Box

Make your Microsoft® SharePoint® environment like Dropbox, Google Drive, and Microsoft 365 by enabling two-way collaboration and external sharing without exiting SharePoint.

## External Sharing Features

### Controlled Sharing Options

- Share content directly from SharePoint and Microsoft 365 with internal and external users, whether the recipient is an individual or an AD group, by using an embedded 'secure share' button.
- Users can upload files directly to Perimeter's "My Drive" to share with external parties. Perfect for those seeking a secure, on-premises alternative to cloud-based file sharing solutions.
- Share recipients can view, edit, delete or download shared content based on prescribed permission rights.
- Allow remote or external collaborators to edit or comment on shared content within Microsoft 365 on mobile devices and desktop browsers, all without exposing on-premises and online SharePoint to the internet.
- Create and manage user- and group-based rules to restrict external sharing options for internal users, as well as define what permissions a user or group can grant when externally collaborating.
- Create rules that enable or disable external sharing based on document metadata such as file name, file type, and tags for all Perimeter-enabled libraries.
- Prevent external users from copying, editing, or sharing content through the AvePoint Perimeter secure document viewer with controlled sharing options.
- Users can set an expiration date for content they share.
- Secure document viewer, accessible from a mobile application or browser, is fully audited and can enforce access limitation based on user location.



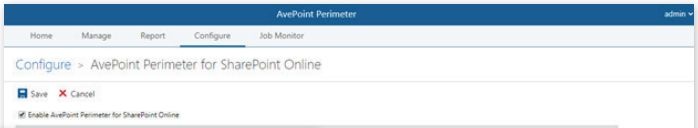
Configure > Secure Share Policy

User and Group Restriction

User and Group can share the corresponding permission when matched the following rule.

| | Rule | Condition | Value | Permission |
|---|---|---|---|---|
| □ | AD User/Group | Start With | User A | Edit |
| □ | SharePoint Group | Contains | SharePoint Group A | View |
| □ | AD User/Group | Equals | Domain\Username | View |

User/Group-based external sharing control for internal users



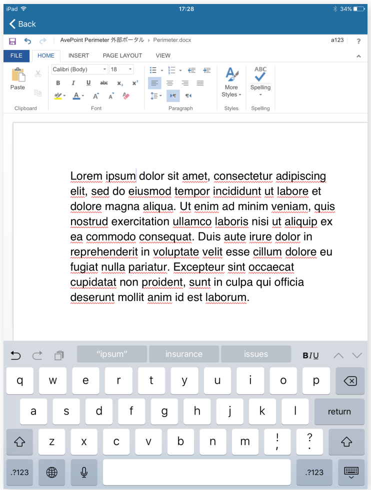
Configure > AvePoint Perimeter for SharePoint Online

☑ Enable AvePoint Perimeter for SharePoint Online

Successfully created the app.

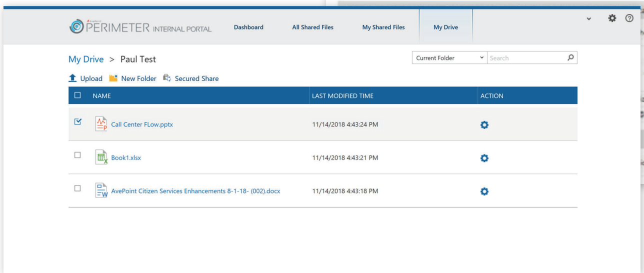
M365x582112.onmicrosoft.com

Secure External Share Settings for SharePoint Online



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Mobile editing of shared content



My Drive > Paul Test

| | NAME | LAST MODIFIED TIME | ACTION |
|---|---|---|---|
| ☑ | Call Center FLow.pptx | 11/14/2018 4:43:24 PM | ⚙ |
| □ | Book1.xlsx | 11/14/2018 4:43:21 PM | ⚙ |
| □ | AvePoint Citizen Services Enhancements 8-1-18- (002).docx | 11/14/2018 4:43:18 PM | ⚙ |

My Drive for Internal Users

- Domain restriction allows administrators to whitelist specific domains such as partners or vendors, and blacklist unauthorized domains to prevent data leakage.
- Multiple options for sharing files including anonymous access, one-time passcode or requiring registration and sign-in.

### Secure Container for Shared Document Access Portal

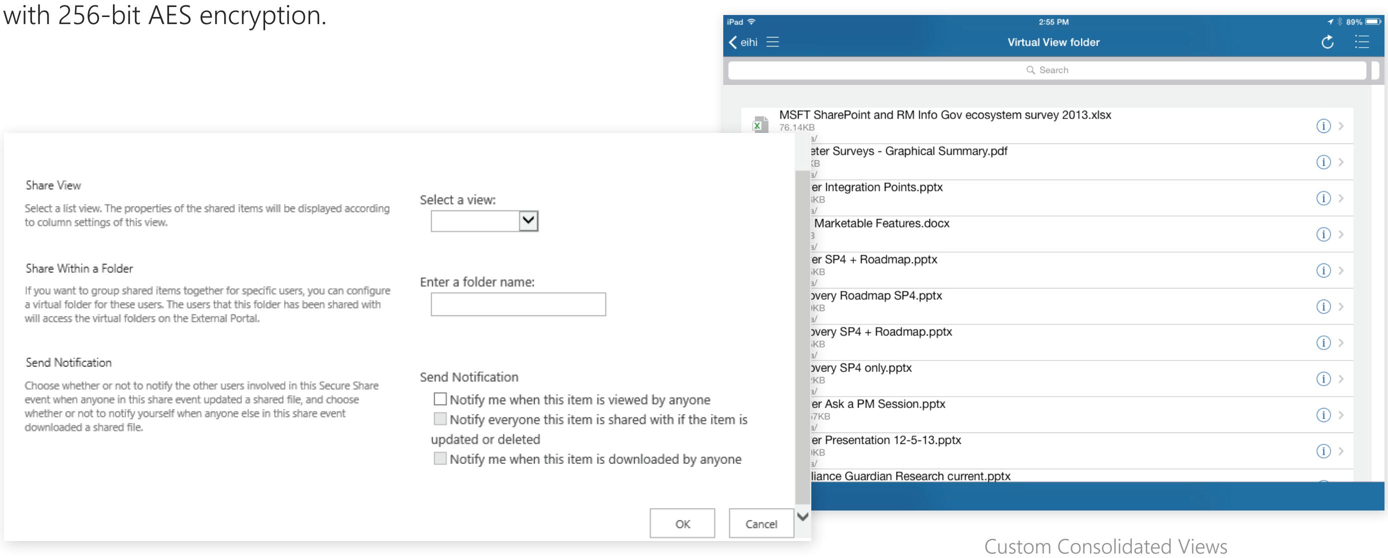
- Provide external users a secure, permission-based point of access to view, download, and edit documents shared with them.
- Protect downloaded or cached documents on iOS devices with 256-bit AES encryption.

### Custom Consolidated Views

- Present unorganized SharePoint content in a single, consolidated view that is specific to end-user needs.
- Utilize SharePoint metadata values–created and assigned–to display designated content only to external users.
- Enable internal users to  group disparate files into a virtual folder for specific external users.

### SharePoint Metadata Share

- Choose which SharePoint metadata is displayed as part of the share.



Share View

Select a list view. The properties of the shared items will be displayed according to column settings of this view.

Select a view:

Share Within a Folder

If you want to group shared items together for specific users, you can configure a virtual folder for these users. The users that this folder has been shared with will access the virtual folders on the External Portal.

Enter a folder name:

Send Notification

Choose whether or not to notify the other users involved in this Secure Share event when anyone in this share event updated a shared file, and choose whether or not to notify yourself when anyone else in this share event downloaded a shared file.

Send Notification

☐ Notify me when this item is viewed by anyone
☐ Notify everyone this item is shared with if the item is updated or deleted
☐ Notify me when this item is downloaded by anyone

MSFT SharePoint and RM Info Gov ecosystem survey 2013.xlsx
76.14KB

eter Surveys - Graphical Summary.pdf

er Integration Points.pptx

Marketable Features.docx

er SP4 + Roadmap.pptx

overy Roadmap SP4.pptx

overy SP4 + Roadmap.pptx

overy SP4 only.pptx

er Ask a PM Session.pptx
7KB

er Presentation 12-5-13.pptx

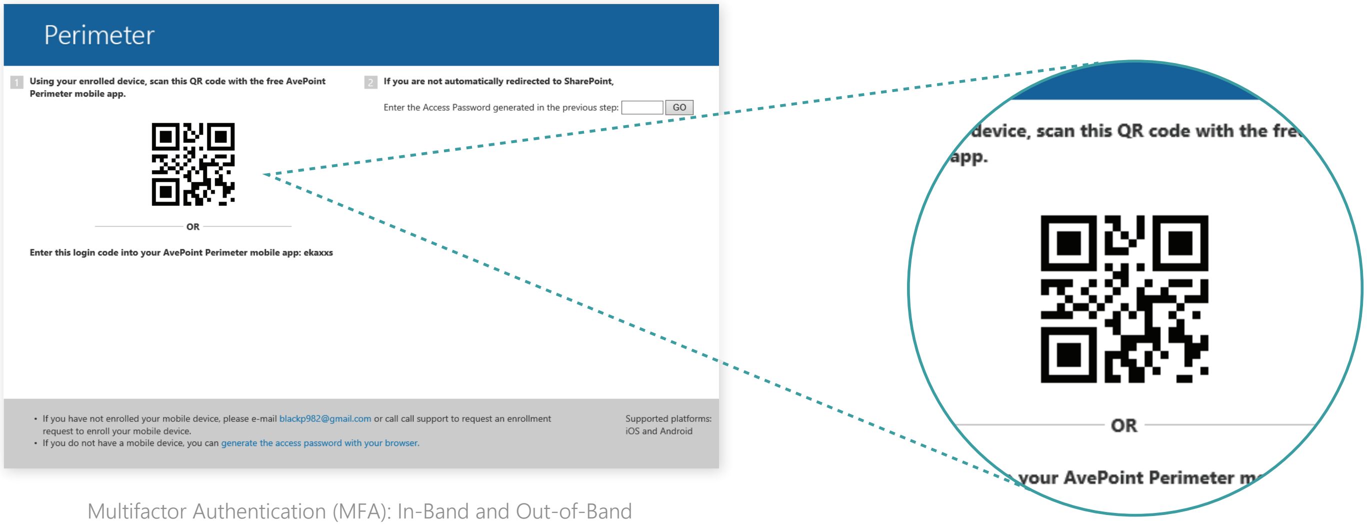
liance Guardian Research current.pptx

Custom Consolidated Views

## SharePoint Access Management Controls

### Multifactor Authentication (MFA): In-Band and Out-of-Band

- Force or block remote, in-band SharePoint access by the end user's browser, device, and operating system type.
- Add an additional in-band authentication factor by restricting access to remote SharePoint content through the AvePoint Perimeter application.
- Authenticate out-of-band users with a single use, limited time access passcode, or by scanning a QR code with the AvePoint Perimeter application.
- Enhance security by configuring two-factor authentication for external users.



Perimeter

1 Using your enrolled device, scan this QR code with the free AvePoint Perimeter mobile app.

OR

Enter this login code into your AvePoint Perimeter mobile app: ekaxxs

2 If you are not automatically redirected to SharePoint,

Enter the Access Password generated in the previous step:

- If you have not enrolled your mobile device, please e-mail blackp982@gmail.com or call call support to request an enrollment request to enroll your mobile device.
- If you do not have a mobile device, you can generate the access password with your browser.

Supported platforms: iOS and Android

device, scan this QR code with the fre
app.
OR
your AvePoint Perimeter m

Multifactor Authentication (MFA): In-Band and Out-of-Band

### Location-Based Access Controls

- Centralize control for AvePoint Perimeter administrators in order to define where and how sensitive documents are viewed or accessed.
- Control access based on a user's geographic location, allowing corporate content to be viewed in predefined locations.
- Group multiple locations based on political boundaries or a fixed radius around specific points in order to apply rules and policies governing user access.

### Active Directory Federation Services (ADFS) & Forms-Based Authentication

- Add additional access controls and enhance security to any ADFS-capable application–including Microsoft® Office 365™, Microsoft® Dynamics CRM Online, Microsoft® Dynamics ERP Online, Microsoft® Project Server Online as well as the Windows Azure management console–by deploying AvePoint Perimeter as part of an ADFS installation.

### Web Services Access Controls

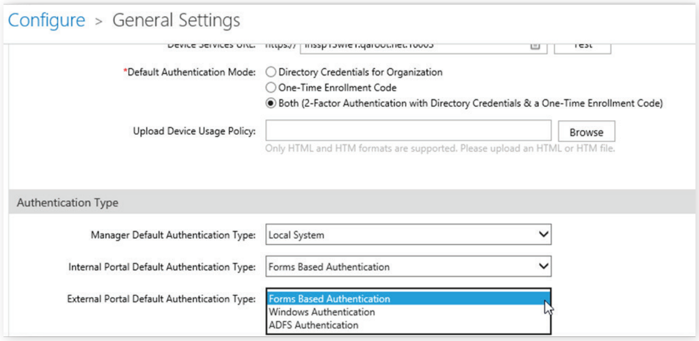
- Manage and control mobile content on a service-by-service basis by blocking or allowing web services access to Microsoft® SharePoint® based on user agent.

### Cached Document Storage on Mobile Devices

- Remotely access file storage from mobile devices to view documents, online and offline.

### Password Policy Management for External Users

- Manage external user accounts and define password requirements for external users accessing the external portal within AvePoint Perimeter Manager.



Configure > General Settings

Device Services URL: https:// [illegible] Test

*Default Authentication Mode: ○ Directory Credentials for Organization
○ One-Time Enrollment Code
● Both (2-Factor Authentication with Directory Credentials & a One-Time Enrollment Code)

Upload Device Usage Policy: Browse
Only HTML and HTM formats are supported. Please upload an HTML or HTM file.

Authentication Type

Manager Default Authentication Type: Local System

Internal Portal Default Authentication Type: Forms Based Authentication

External Portal Default Authentication Type: Forms Based Authentication
Windows Authentication
ADFS Authentication

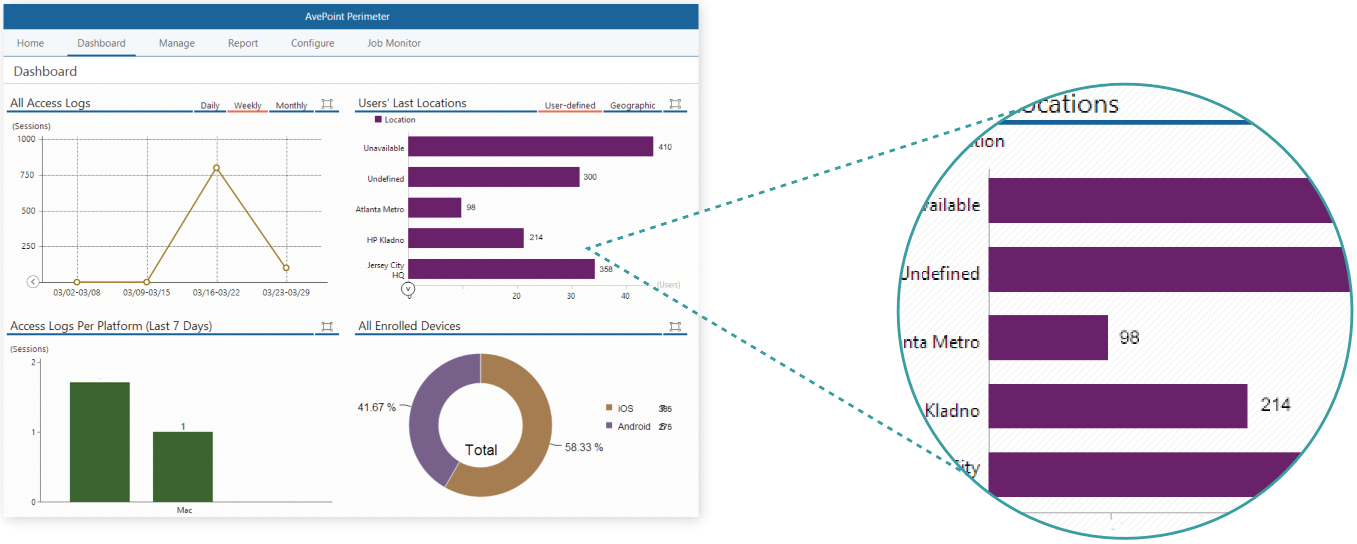
## Administrative Features

### Detailed Dashboards and Reporting Over Content Access

- Track, monitor, report, and audit all remote SharePoint content access, user activity, enrolled devices, and geographic locations.

### Burglar Alarm

- Monitor, record, and proactively react to users engaging in suspicious activities with configurable Burglar Alarm tracking and alerts focused on core Perimeter activities, including authentication, file sharing, unauthorized location log-ins, and content downloads.



Detailed Dashboards and Reporting Over Content Access

### Share Expiration Policy Management

- Enforce mandatory expiration and the maximum duration of a share.

### Daily User Audit Tracking

- Access an exportable, unified view of the activity across devices of a single user within both Perimeter portals and your greater SharePoint environment, reporting on all behaviors during a specified duration.

### Permissions Management

- Manage configurations, permissions, and access settings for users, devices, and locations in one central administrator portal with AvePoint Perimeter's user-friendly wizard.

### Enterprise Wipe Capabilities

- Remotely wipe all stored or cached documents and data – as well as all user activity performed within the application – in the event of a breach, loss of device, or employee turnover.

### Bulk Enrollment of Users and Devices

- Enroll multiple users and devices simultaneously by uploading a formatted CSV file.

## Supported Technologies

### Platforms & Applications

- Supports on-premises and online platforms including
  - Microsoft SharePoint 2019
  - Microsoft SharePoint 2016
  - Microsoft SharePoint 2013
  - Microsoft SharePoint 2010
  - Microsoft Project 2013
  - Microsoft Project 2010
  - Microsoft SharePoint Online
  - OneDrive for Business
- Supports all Active Directory Federation Services (ADFS) enabled applications including:
  - Microsoft 365
  - Microsoft Dynamics CRM Online
  - Microsoft Dynamics ERP Online
  - Microsoft Project Server Online
  - Windows Azure management console.
- Remotely access SharePoint® through the following supported browsers: Internet Explorer® , Edge, Chrome™ , Firefox®, and Safari.
- Remotely access SharePoint® through the following supported mobile devices: iPad, iPhone, and iPod Touch (iOS 5 and newer versions) .
- Remote access to shared documents through mobile devices on Android™ platform  (Gingerbread 2.3 and newer versions).
- Two-factor authentication supported on Windows Phone, iOS, and Android devices. .

## How to Buy AvePoint Products

Contact: 201.793.1111 | Sales@AvePoint.com
AvePoint Global Headquarters | 525 Washington Blvd, Suite 1400 | Jersey City, NJ 07310

Start your free trial today:
www.avepointonlineservices.com

© AvePoint, Inc. All rights reserved. AvePoint and the AvePoint logo are trademarks of AvePoint, Inc. All other marks are trademarks of their respective owners.

*Accessible content available upon request*

Internet Explorer® is a registered trademark of Microsoft Corporation in the United States and other countries.

© 2012 Google Inc. All rights reserved. Chrome™ browser is a trademark of Google Inc.

Apple, the Apple logo, iPhone, iPad and iPod touch are trademarks of Apple Inc., registered in the U.S. and other countries. App Store is a service mark of Apple Inc.

© 2012 Google Inc. All rights reserved. Android™ platform is a trademark of Google Inc.