INTERMEDIA

eBook: SecuriSync Control and Security Features for Administrators

Now upgraded security with Bitdefender® anti-malware/antivirus solution at no additional cost.

INTRODUCTION

SecuriSync® is Intermedia's enterprise-class backup and file sharing service. This collaboration service enables file and folder backup across user devices, along with sharing features for distributing and real time backup of files both internally and externally.

SecuriSync provides not only an extremely high degree of security but also full control for administrators over users and content. This makes SecuriSync one of the file backup and sharing solutions in the market with the most extensive list of features in order to give full visibility and management capabilities for admins while being an easy to use service for end-users.

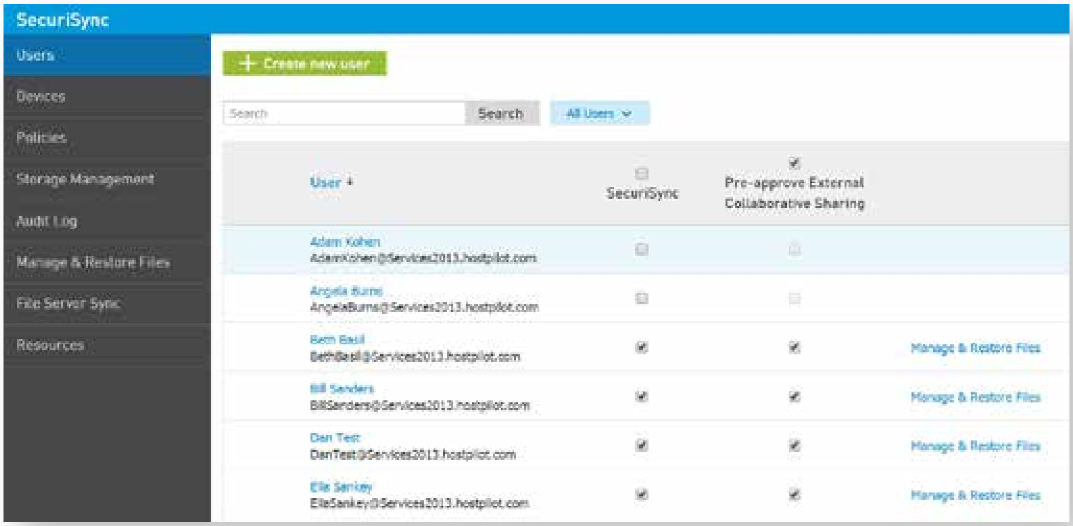
SecuriSync's protection and control features let administrators:

- Assure compliance with security best practices
- Get full visibility over end-user activity with Audit Log and Admin File Management features
- Utilize file restore and remote wipe capabilities
- Keep content safe with at-rest and in-transit encryption
- Protect files against advanced cyber threats, like ransomware and malware, with Bitdefender anti-malware and antivirus solution fully integrated within SecuriSync
- Protect content integrity with features that guard against accidental deletion or version conflict
- Recover from virtually any data loss event with advanced restore features
- Keep content in the right hands with permissions and access that are strictly controlled and easily amended
- Assure reliability with a 99.999% financially backed uptime guarantee
- Leverage enterprise-class datacenters with redundant storage clusters and connections to multiple Internet providers

CONTROL FEATURES IN SECURISYNC

User Management: Control Who Has Access to Files

User Provisioning:
SecuriSync let administrators maintain full control over who is using SecuriSync. Admins can easily add users to SecuriSync using HostPilot by selecting specific individuals or for all users at once. They can also create new users and give them access to SecuriSync.



User ↓	☐ SecuriSync	☑ Pre-approve External Collaborative Sharing	
Adam Kohen AdamKohen@Services2013.hostpilot.com	☐	☐	
Angela Burns AngelaBurns@Services2013.hostpilot.com	☐	☐	
Beth Basil BethBasil@Services2013.hostpilot.com	☑	☑	Manage & Restore Files
Bill Sanders BillSanders@Services2013.hostpilot.com	☑	☑	Manage & Restore Files
Dan Test DanTest@Services2013.hostpilot.com	☑	☑	Manage & Restore Files
Elle Sankey ElleSankey@Services2013.hostpilot.com	☑	☑	Manage & Restore Files

There is no need to adjust VPN, firewall or security policies. Like all Intermedia services, SecuriSync also comes with onboarding assistance from our Cloud Concierge as well as 24x7 support in case there is a need further assistance when deploying SecuriSync across an organization.

SecuriSync also provides a synchronization tool for environments where Active Directory is used for identity management. Admins can use this to easily enable and manage user creation and decommissioning from Active Directory.

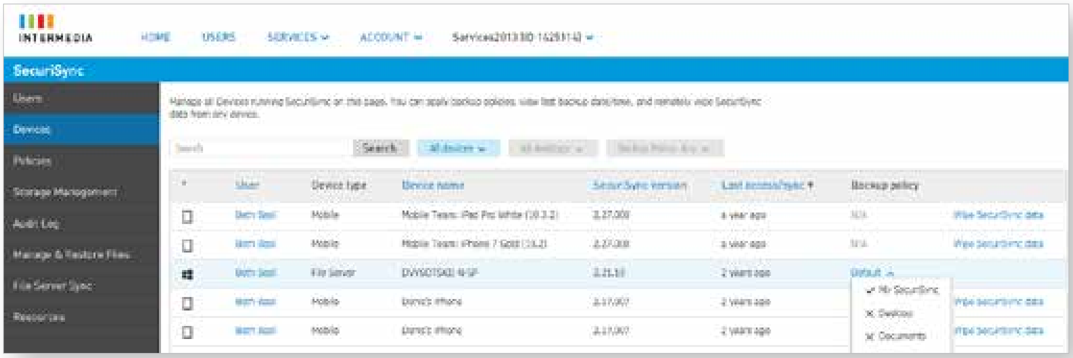
Hostpilot adds more control by providing role-based access, so individual system administrators can be assigned appropriate permissions within the control panel. All actions are tracked in the HostPilot Event log for visibility and compliance.

Mobile Device Management (MDM) solutions can be used to provision SecuriSync mobile apps on mass.

User Decommissioning:
Admins can also easily remove SecuriSync users with just one click. User offboarding helps reduce the potential that terminated employees are still able to gain access to corporate data after they have left the company and gives admins complete control over their file management environment.

DEVICE MANAGEMENT: CONTROL DEVICES WITH SECURISYNC ENABLED

Device Visibility:
Using HostPilot, administrators can view and manage all the SecuriSync devices enabled on their account. They have visibility into mobile and desktop devices that each user has used to access SecuriSync, and the last activity related to SecuriSync across all configured devices. Each time a new device is configured by an end user, the administrator is notified.



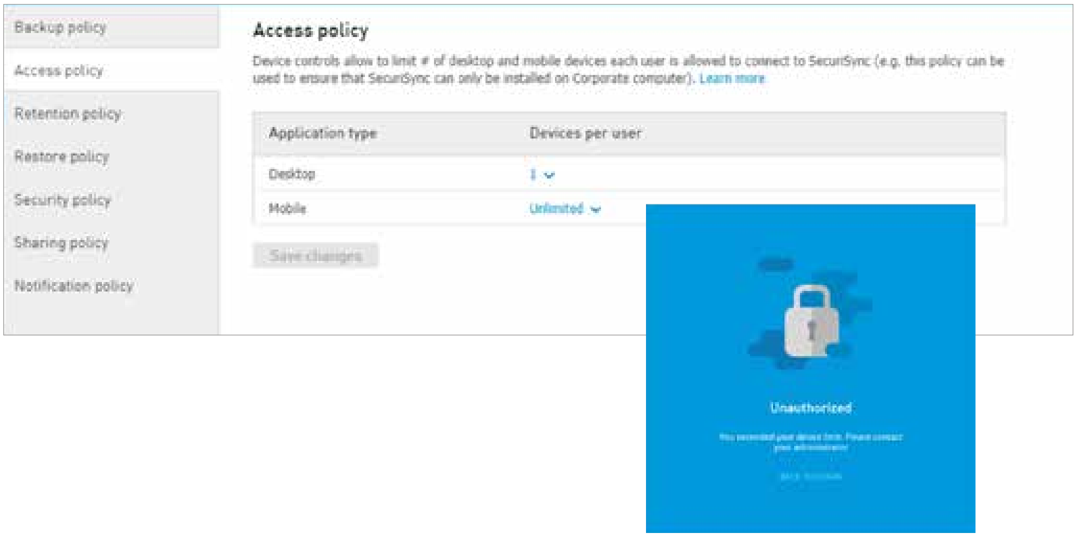
Manage all Devices running SecuriSync on this page. You can apply backup policies, view last backup date/time, and remotely wipe SecuriSync data from any device.

	User	Device type	Device name	SecuriSync version	Last access/sync	Backup policy	
□	[illegible]	Mobile	Mobile Team: iPad Pro White (10.3.2)	2.27.000	a year ago	N/A	Wipe SecuriSync data
□	[illegible]	Mobile	Mobile Team: iPhone 7 Gold (10.2)	2.27.000	a year ago	N/A	Wipe SecuriSync data
⊞	[illegible]	File Server	DVYSDTSK01 N-SP	2.21.10	2 years ago	Default	
□	[illegible]	Mobile	Dario's iPhone	2.17.007	2 years ago		Wipe SecuriSync data
□	[illegible]	Mobile	Dario's iPhone	2.17.007	2 years ago		Wipe SecuriSync data

Admins can classify devices into different categories (Personal desktop, Corporate desktop, File Server, mobile phone) and designate a different backup policy for each one and also configure which users' devices will be backed up.

Device Access Policy:

Better protect your corporate files by ensuring that SecuriSync can only be installed on corporate computers. Device Access Policy let administrators limit the number of desktop and mobile devices allowed to connect to SecuriSync. This policy is designed to control where SecuriSync apps are installed.



Access policy

Device controls allow to limit # of desktop and mobile devices each user is allowed to connect to SecuriSync (e.g. this policy can be used to ensure that SecuriSync can only be installed on Corporate computer). Learn more

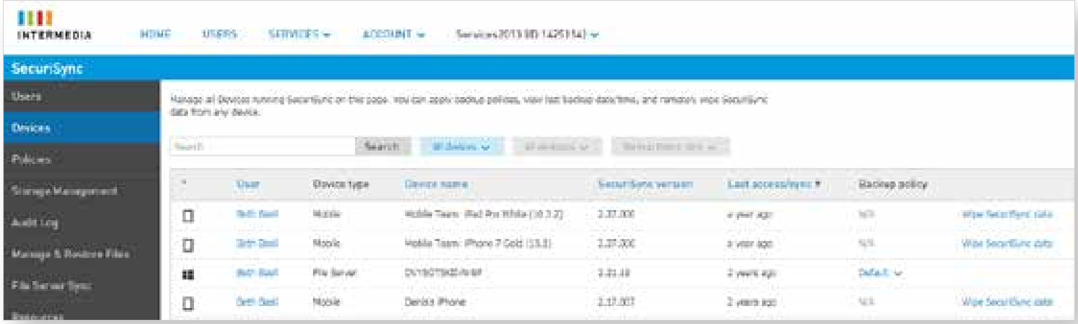
Application type	Devices per user
Desktop	1 ⌄
Mobile	Unlimited ⌄

Unauthorized

You exceeded your device limit. Please contact your administrator.

Reduce Corporate Data Leakage with Remote Wipe:

SecuriSync is one of just a few file management solutions to allow administrators to wipe data remotely from any device. In case of a lost or stolen laptop, tablet, or mobile phone, or when facing a personnel issue, corporate data can be quickly removed, minimizing potential data leakage.



Manage all Devices running SecuriSync on this page. You can apply backup policies, view last backup date/time, and remotely wipe SecuriSync data from any device.

*	User	Device type	Device name	SecuriSync version	Last access/sync ▾	Backup policy	
▯	Seth Bell	Mobile	Mobile Team: iPad Pro White (10.3.2)	2.37.300	a year ago	N/A	Wipe SecuriSync data
▯	Seth Bell	Mobile	Mobile Team: iPhone 7 Gold (13.3)	2.37.300	a year ago	N/A	Wipe SecuriSync data
■	Seth Bell	File Server	[illegible]	2.31.18	2 years ago	Default ⌄	
▯	Seth Bell	Mobile	Derick iPhone	2.17.303	2 years ago	N/A	Wipe SecuriSync data

The remote wipe functionality is even available for SecuriSync data stored in external user's devices. Admins can use it when the engagement or project with the external user has been completed.

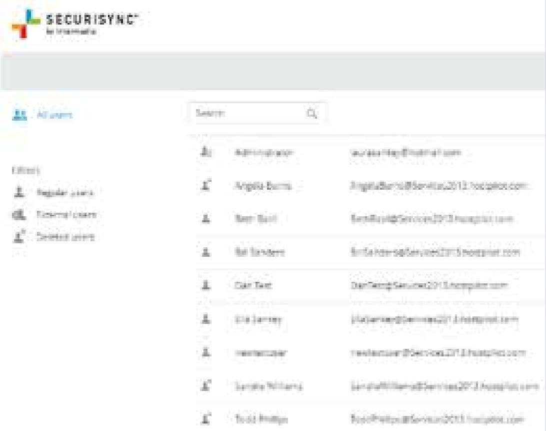
Remote wipe is another control feature of SecuriSync that helps ensure the success of offboarding processes making easy to remove corporate data when an employee leaves the company. Remote wipe is available to all Account Owners as well as Technical Administrators that have been assigned the special remote wipe permission.

CONTENT MANAGEMENT

Admin File Management:
SecuriSync let administrators have full visibility over all end-user files and folders so they can easily monitor and manage the content.

Administrators can add and delete files and folders across SecuriSync, share them with internal and external users, and use the search bar to look for a specific file in end-user accounts. This feature needs to be explicitly enabled for each admin. All admin actions are tracked in the audit log.

The management of disabled user content is enabled by default and included in all plans while the management of active user content has to be manually enabled.

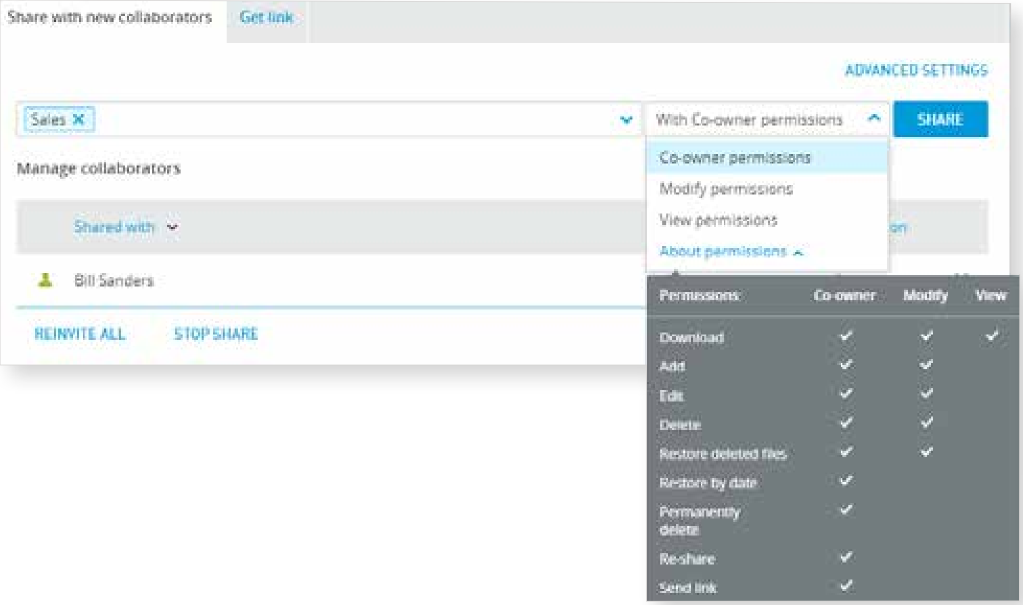


Administrator	[illegible]
Angela Burns	[illegible]
Beth Bush	[illegible]
Bill Sanders	[illegible]
Dan Test	[illegible]
Ella Jamsey	[illegible]
newtestuser	[illegible]
Sandra Williams	[illegible]
Todd Phillips	[illegible]

CONTENT PERMISSIONS & ACCESS MANAGEMENT

When a user shares a SecuriSync folder, he or she can set permissions for each collaborator independently. The configurable sharing permissions are “Co-Owner,” (full control to modify, delete or share content), “Modify” (allow other to view, modify and delate but not share), or “View-only” permissions (only enable others to download files).

Permissions can be set differently for each collaborator. Sub-folders can be shared with different permissions and collaborators than parent folders. Permission levels can be changed or revoked at any time.

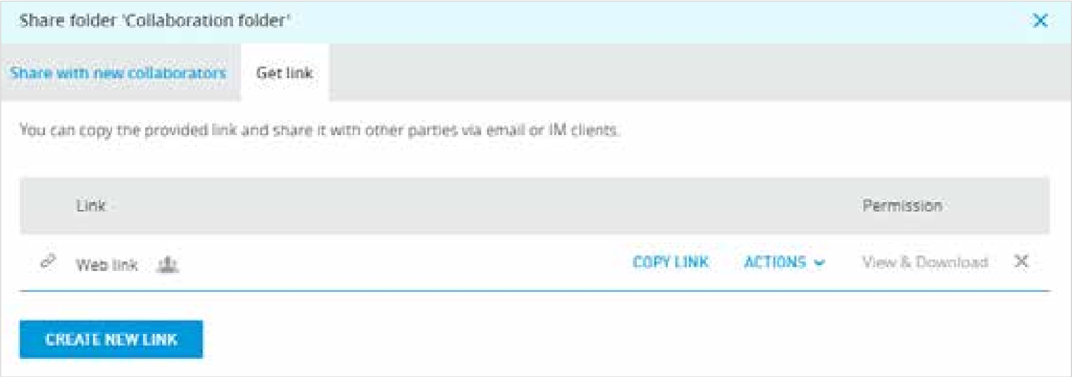


Permissions	Co-owner	Modify	View
Download	✓	✓	✓
Add	✓	✓	
Edit	✓	✓	
Delete	✓	✓	
Restore deleted files	✓	✓	
Restore by date	✓		
Permanently delete	✓		
Re-share	✓		
Send link	✓		

User can generate secure links to any files or folder to share content. Sharing content via web links helps insure that the most up-todate content is always being referenced.

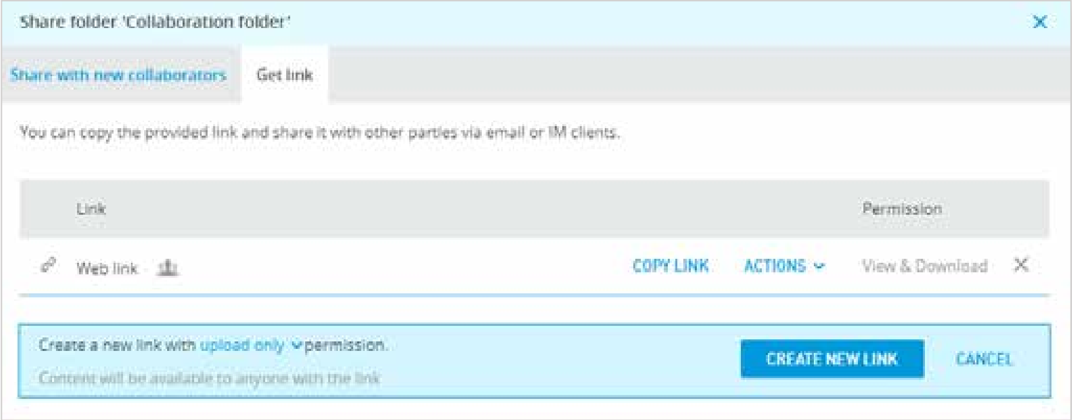
Based on Admin preference, users may have access up to 4 different web link permissions:

- **View and Download links:** These web links allow recipients to both preview and download the content
- **View-only permission:** These web links allow recipients to preview the content, but not download it
- **Upload-only permission:** These web links allow users to request/collect files from various parties without having to set up external shares. These web links allow recipients to upload content into a folder without being able to see what's in the folder already
- **Download & Upload permission:** These web links allow users to request/collect files from various parties without having to set up external shares. These web links allow recipients to upload content into a folder while also being able to view and download existing folder content


Share folder 'Collaboration folder'

You can copy the provided link and share it with other parties via email or IM clients.

Link			Permission
Web link	COPY LINK	ACTIONS	View & Download


Share folder 'Collaboration folder'

You can copy the provided link and share it with other parties via email or IM clients.

Link			Permission
Web link	COPY LINK	ACTIONS	View & Download

Create a new link with upload only permission.

Content will be available to anyone with the link

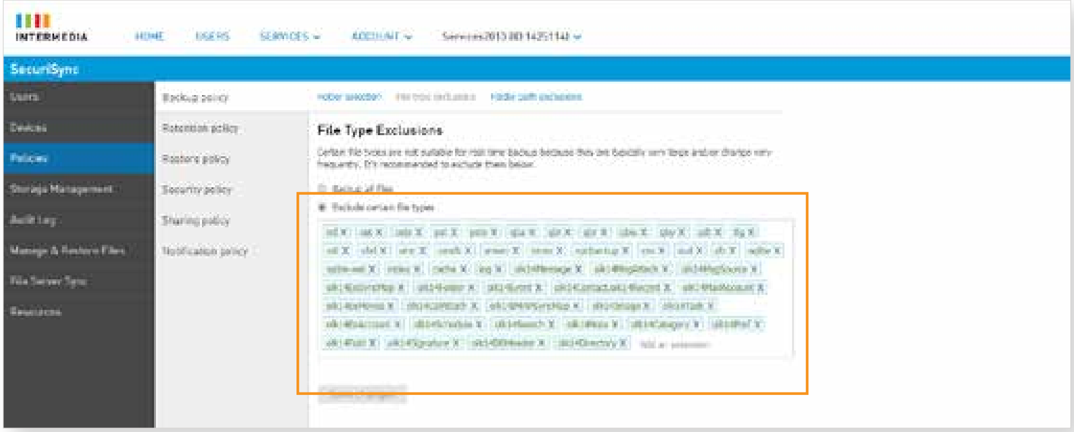
Users can choose to password-protect a link and/or to set an automatic expiry date, before sending it. If a link is password-protected, the recipient will be asked to enter a password before being able to view and download the content. Admins can optionally enforce password-protection and automatic expiry.

BACKUP & RESTORE

Backup Policies:
SecuriSync backs up not just the files in the SecuriSync folder but also the files and folders on Desktop, My Documents, Music, Video, Downloads folder, and photos and videos from iOS and Android devices.

Unlike traditional solutions that set their backup to run every 24 hours, which create gaps because they back-up on a set schedule, SecuriSync backs up files in real time, every time a change is made, and will keep an unlimited numbers of versions.

If administrators consider that certain file types are not suitable for real-time backup because they are very large, frequently changed, and typically do not need to be backed up, SecuriSync let them configure some exclusions like Outlook files, virtual machines (vmdk, vhd, etc.), QuickBooks/Sage, Logs, Databases, and temporary files.



File Type Exclusions

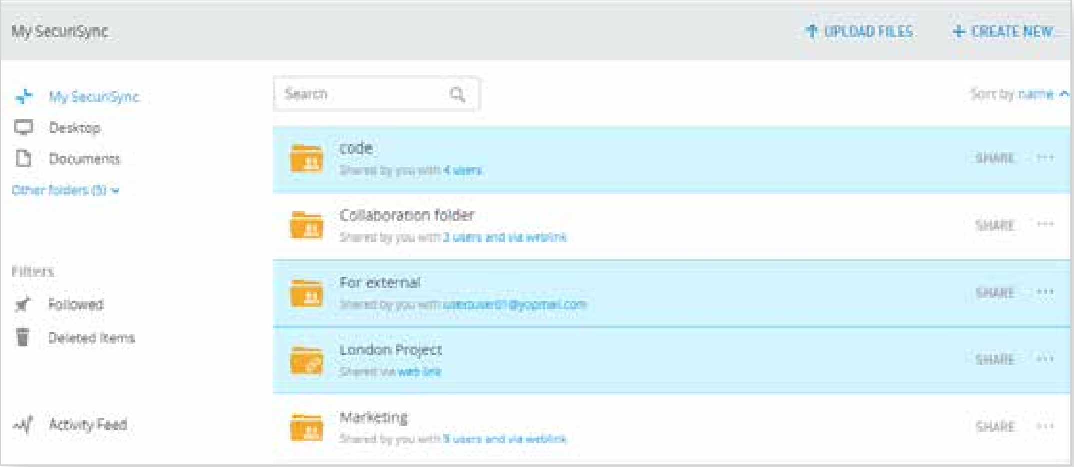
Certain file types are not suitable for real time backup because they are typically very large and/or change very frequently. It's recommended to exclude them below.

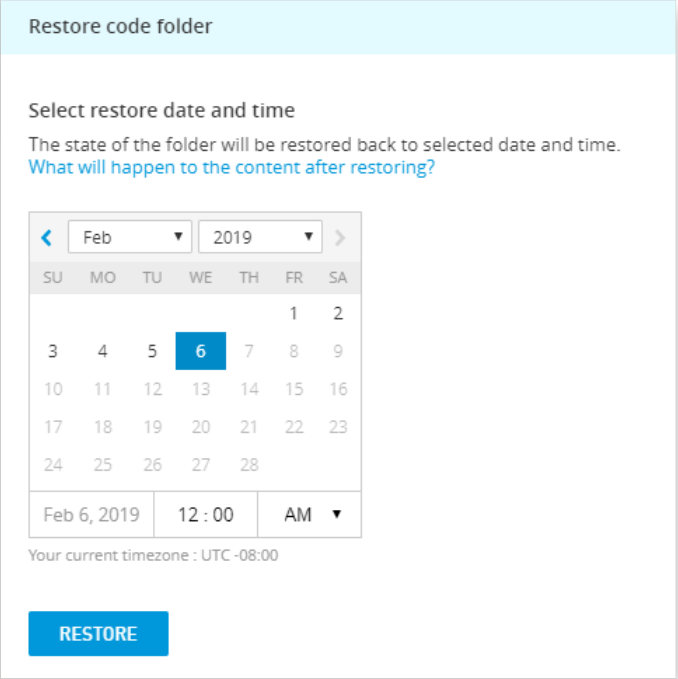
○ Backup all files

● Exclude certain file types

Protect Data from Loss Events with Roll Back and File Versioning:

Intermedia designed SecuriSync with a high level of data protection, to help reduce the chances of files being accidentally deleted, and to help simplify the process to restore and recover files in the case of a data loss event.





Restore code folder

Select restore date and time

The state of the folder will be restored back to selected date and time.
What will happen to the content after restoring?

Feb ▾ 2019 ▾

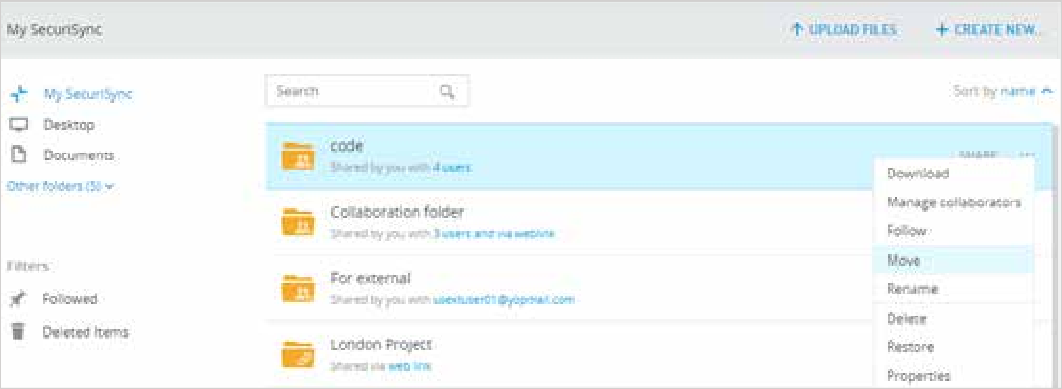
SU	MO	TU	WE	TH	FR	SA
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28		

Feb 6, 2019 12 : 00 AM ▾

Your current timezone : UTC -08:00

Files can be rolled back to specific earlier versions or to a specific point in time. Files can be rolled back individually or multiple files and folders can be rolled back in a mass restore capability. Files can be restored by either end users or by administrators through the Admin File Management functionality.

From a service architecture perspective, every SecuriSync file is replicated to redundant storage clusters to help minimize the risk of data loss. Additionally, each user's data is fully isolated from every other user's data. In the unlikely event of a service outage, users can still access all their locally backed up data.



code
Shared by you with 4 users

Collaboration folder
Shared by you with 3 users and via weblink

For external
Shared by you with userxtuser01@yopmail.com

London Project
Shared via web link

SecuriSync co-editing features helps to prevent file overwrites and conflicts.
File versioning allows users to easily restore previous versions of files stored in SecuriSync. If a file is deleted, it is moved to a recycle bin, where it can be restored. Administrators can restore deleted files and prevent permanent deletions.

CENTRALIZED FILE MANAGEMENT WITH HOSTPILOT CONTROL PANEL

SecuriSync is managed through HostPilot™, a simple, powerful and intuitive control panel that integrates all Intermedia cloud services, all users and devices -including mobile device management- for centralized management and increased administrator productivity.

Most IT administrators, when they're selecting a cloud file collaboration and backup services, don't think about the control panel. That's a mistake: nothing is more important to both administrator and user productivity than a simple and secure control panel.

HostPilot is a command post for deploying file sharing and backup, plus other cloud services, to your workforce. It keeps the management of files in the cloud simple so you stay focused on business.

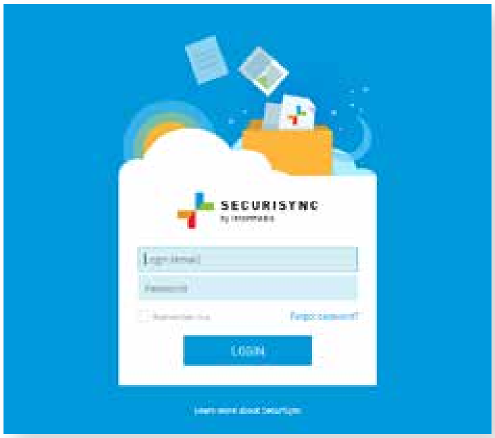
- Accessible using a web browser
- Advanced security with two-factor authentication (extra layer of security when logging into the control panel)
- Simple to add users, new services, manage app settings, respond to user service requests, get reports, and much more.
- Integrate with on-premise Active Directory
- 24/7 admin phone support
- 99.999% uptime Service Level Agreement (SLA)

SECURITY & COMPLIANCE IN SECURISYNC

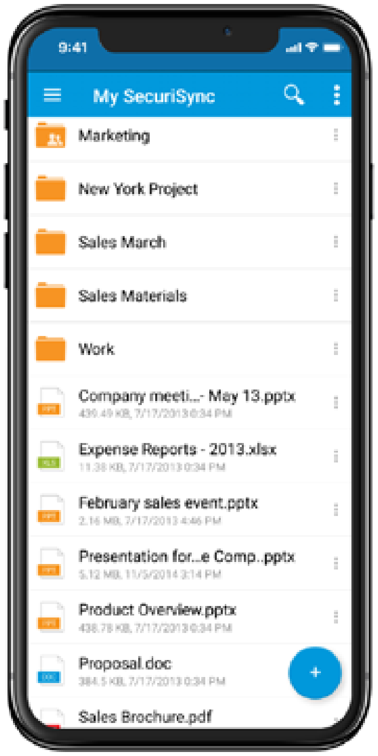
Active Directory Integration:

Each time a user activates a new SecuriSync device or accesses SecuriSync from the web, they must login using their username and password.

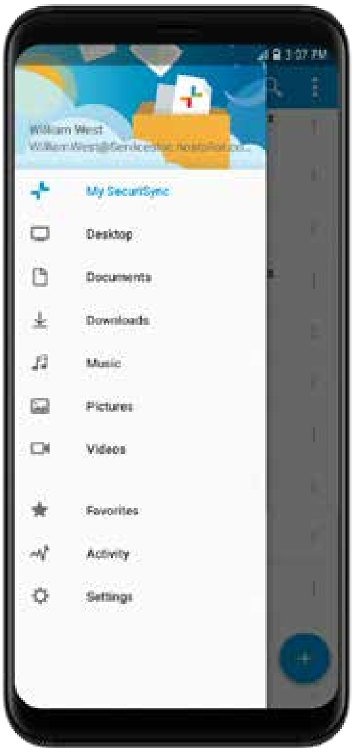
SecuriSync password policies are imported from Active Directory and utilize “strong” parameters, helping to eliminate the possibility that external parties will guess passwords. This Active Directory integration requires users to use the same password for SecuriSync that they use for all their Intermedia-powered services. Because there are no additional passwords to remember, it reduces the possibility that they will write their password down where others might see it.



For mobile devices, an additional layer of security can be added by configuring a passcode that must be entered each time the app is launched.



iPhone



Android

ENCRYPTION

SecuriSync data is encrypted both when it's at rest as well as when it's in transit. At-rest data is encrypted with 256-bit AES encryption, while in-transit data is encrypted using 256-bit SSL/HTTPS encryption. Additionally, SecuriSync generates a unique encryption key for every account, creating an even greater degree of protection through data isolation.

Storing data on platforms without unique account-level encryption keys dramatically increases the risk of data leaks.

CONTINUOUSLY PROTECT CORPORATE FILES

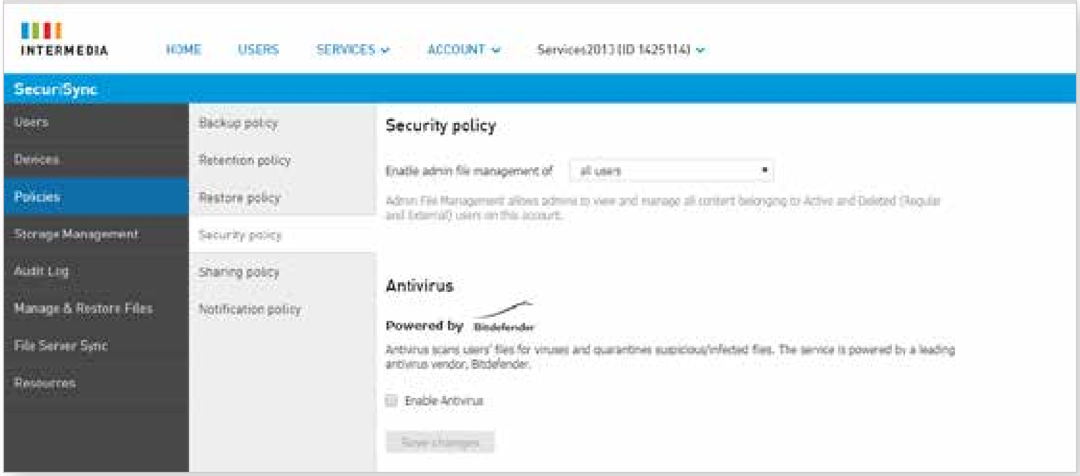
Bitdefender® Advanced Anti-Malware Integrated with SecuriSync

Bitdefender advanced anti-malware and antivirus protection is integrated with SecuriSync to provide an extra layer of protection to keep files and content safe and secure.

This new layer of security provided by Bitdefender continuously protects files and documents from advanced cyber threats by quarantining infected files and will be available for free to all SecuriSync customers.

SecuriSync files are now automatically scanned to spot and detect cyber threats - including viruses, ransomware, and malware - that are developed by attackers to gain access to documents and systems.

Administrators can choose to activate Bitdefender, and end-users don't need to configure anything to enable this vital functionality.



Security policy

Enable admin file management of: all users

Admin File Management allows admins to view and manage all content belonging to Active and Deleted (Regular and External) users on this account.

Antivirus

Antivirus scans users' files for viruses and quarantines suspicious/infected files. The service is powered by a leading antivirus vendor, Bitdefender.

□ Enable Antivirus

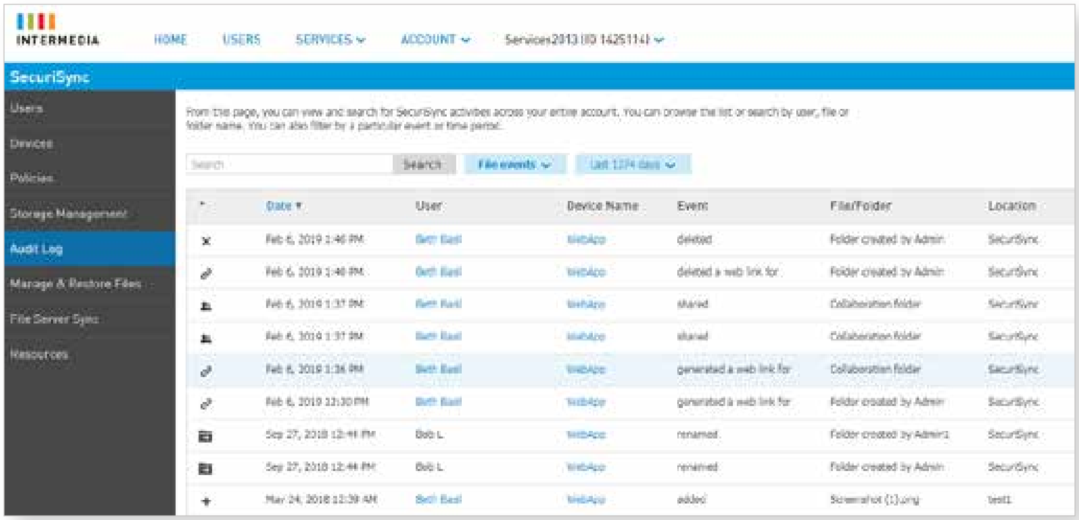
Bitdefender is a market leader in the Endpoint Security market according to Forrester Research (Forrester Wave™: Endpoint Security Suites, Q2 2018).

GREATER LEVEL OF CONTROL WITH AUDIT LOG

The Audit Log is a HostPilot feature and allows administrators to view all the SecuriSync activities on their account. Whenever files or folders are added, updated, shared, or deleted, the event is logged and available for tracking and auditing purposes, providing a greater level of administrative control over SecuriSync.

There are multiple ways to use the Audit Log:

- Browse by event type
- Search by user, file name, or folder name
- Filter by event type or date range



From this page, you can view and search for SecuriSync activities across your entire account. You can browse the list or search by user, file or folder name. You can also filter by a particular event or time period.

•	Date ▾	User	Device Name	Event	File/Folder	Location
✕	Feb 6, 2019 1:46 PM	Beth Basl	WebApp	deleted	Folder created by Admin	SecuriSync
🔗	Feb 6, 2019 1:40 PM	Beth Basl	WebApp	deleted a web link for	Folder created by Admin	SecuriSync
👥	Feb 6, 2019 1:37 PM	Beth Basl	WebApp	shared	Collaboration folder	SecuriSync
👥	Feb 6, 2019 1:37 PM	Beth Basl	WebApp	shared	Collaboration folder	SecuriSync
🔗	Feb 6, 2019 1:36 PM	Beth Basl	WebApp	generated a web link for	Collaboration folder	SecuriSync
🔗	Feb 6, 2019 12:30 PM	Beth Basl	WebApp	generated a web link for	Folder created by Admin	SecuriSync
🗀	Sep 27, 2018 12:44 PM	Bob L	WebApp	renamed	Folder created by Admin1	SecuriSync
🗀	Sep 27, 2018 12:44 PM	Bob L	WebApp	renamed	Folder created by Admin	SecuriSync
+	May 24, 2018 12:39 AM	Beth Basl	WebApp	added	Screenshot (1).png	test1

SECURE INFRASTRUCTURE WITH 99.999% SLA

SecuriSync is backed by a 99.999% uptime guarantee. This is the same industry-leading Service Level Agreement (SLA) that Intermedia extends to all its cloud services. No other file collaboration service offers a comparable uptime guarantee.

SecuriSync is delivered through Intermedia's world-class data infrastructure.
This infrastructure is comprised of:

- Multi-tenant platforms secured with redundant firewalls and multiple intrusion prevention systems
- Facilities with dedicated, full-time certified security personnel and rigorous physical security measures

COMPLIANCE

SecuriSync takes strict security measures to reach regulatory compliance across industry and vertical-specific standards.

Data Privacy, Integrity and Security Standards

SOC 2 Type II, SOC 3 - Intermedia has a SOC 2 Type II and SOC 3 audit report from an independent auditor who has validated that, in their opinion, our controls and processes were effective in assuring security during the evaluation period. Intermedia is audited company-wide, not just at the datacenter level. Additionally, while some service providers may only choose to be audited against one or two of the five trust service principles (security, availability, processing integrity, confidentiality and privacy), Intermedia has been audited against all five.

SSAE 16 Type II-audited datacenters - Intermedia datacenters are audited to the SSAE 16.

Type II standard, which validates the provider's commitment to the trust principles of security, availability, processing integrity, confidentiality, and privacy.

US-EU & US-Swiss Safe Harbour - Intermedia is registered and certified with the US. Department of Commerce as compliant with US-EU and US-Swiss Safe Harbor frameworks, which were created to bridge the gap between US and EU/Swiss data protection and privacy standards. All our EU and US customers benefit from this level of protection.

PCI Data Security Standards (PCI DSS) - The payment processing system utilized by Intermedia has passed the strict testing procedures necessary to be compliant with the PCI Data Security Standards (PCI DSS). This helps ensure that your payment information will not be accessed by unauthorized parties or shared with unscrupulous vendors.

Vertical-Specific Compliance

HIPAA - The Health Insurance Portability and Accountability Act mandates a set of regulations protecting the privacy and security of patients' confidential health information, including when and with whom that information can be shared.