Axcient

x360Sync

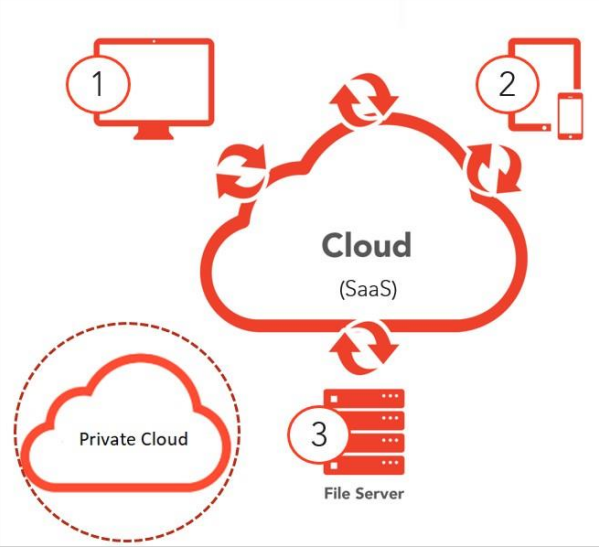
Administrator User Guide

Table of Contents

x360Sync for Administrators

x360Sync is a secure and reliable file synchronization software platform that allows end users to collaborate, synchronize content from multiple devices, and back up important files and folders. x360Sync is comprised of two services:

- The server service can be hosted within your internal infrastructure (called the private cloud model) or it can be provided by x360Sync's hosted cloud infrastructure (called the SaaS model). *System administrators* install and manage the server service, and *organization administrators* can be appointed to help manage the server service.
- The desktop client is used by *end users* and is deployed to a multitude of endpoints, including desktops, laptops, servers, and mobile devices. End users access their files, folders, and shares through the web portal, their desktop clients, and their mobile apps.



Organizations

Within the system, you create organizations and suborganizations, which represent a parent-child hierarchy of entities. An *organization* might be your internal company, a customer, a group, a department, or a location. A *suborganization* is a sub-entity that exists below the parent organization. Organizations and suborganizations can be configured to have different settings, while still maintaining a relationship within the system.

Users

Within organizations, user accounts are created for end users who work inside an organization or suborganization. Guest accounts can be created for temporary users who have been invited to collaborate on, or view, a file, folder, or share. Guest accounts might be vendors, temporary employees, or consultants.

Data

Data is stored in various *roots*, including

- A personal root, which contains data that is created when a user account is generated in the system. It holds all personal data for the user account.
- A Team Share root, which contains data that is shared with multiple user accounts.
- A backup root, which contains backed up data that can be restored in the event ofdata loss. Backup roots are not replicated to other machines.

When allocating space quota settings, you should consider that Team Share roots only count towards the storage quota of an organization. Backup roots and personal roots, however, count towards both organization and individual user account storage quota.

Maximum File Size

To promote collaboration and increase file sharing options, x360Sync does not limit the size of files a standard user or guest user can upload through the web portal or through the desktop client.

Organization administrators can use the Max File Size policy to control the size of files uploaded through the desktop client, mobile apps, and web uploads for users and guests. For more information, please reference the *How to Create a New Organization* section of the Guide. **Database Files**
x360Sync currently does not support the syncing of live database files. Examples include:

- Live Databases (.dbs)
- Microsoft Access Databases
- Quickbook Files
- .pst Files

Supported Operating Systems

Desktop clients can be installed on both Windows and OS X machines. It should be noted that x360Sync only supports 64-bit OS X machines.

TIP

Desktop clients cannot be installed under a roaming profile. You can, however, configure a terminal server environment if necessary.

x360Sync Compression

With x360Sync, your data is synchronized as efficiently as possible. When large, compressible files over 1MB are placed in the sync queue, x360Sync utilizes an rsyncbased syncing method that compares the existing revision with the updated revision, and will only transfer the changed portion. For example, if you edit one row of a large Excel spreadsheet, that change will be detected, and only that row will be synchronized. In this way, x360Sync will never unnecessarily re-upload a file or waste bandwidth, resulting in efficient, quick, and safe file syncing.

When dealing with files that are not compressible, the rsync method cannot be utilized. These file types will still be synchronized, but must be entirely re-uploaded. These file types include:

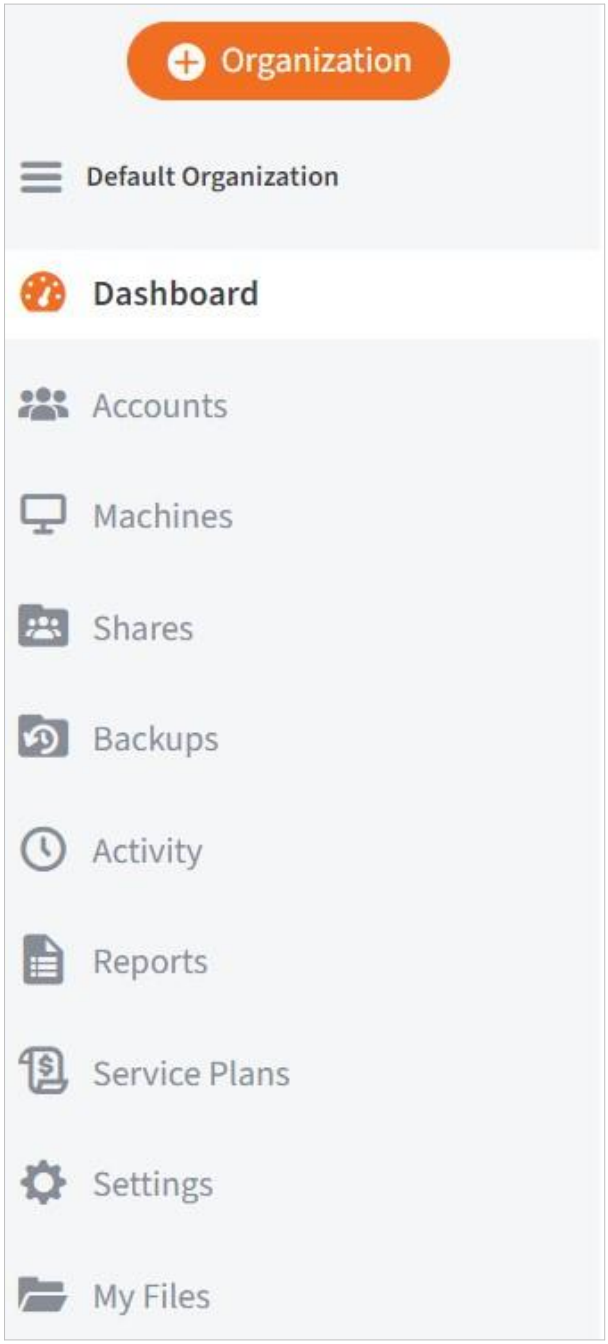
• .mis	• .rm
• .3gp	• .dts
• .avi	• .aac
• .divx	• .ac3
• .flv	• .ape
• .m4v	• .fla
• .mkv	• .flac
• .mov	• .m4a
• .mp4	• .mp1
• .mpg	• .mp2
• .mpeg	• .mp3
• .vob	• .ogg

- .wmv
- .wma
- .bik
- .mv
- .qt
- .mk

How to Navigate the Administrative Web Portal

In the administrative web portal, you can access settings and configuration tools to help you manage the system for end users. You can navigate the administrative web portal using the left navigation bar.

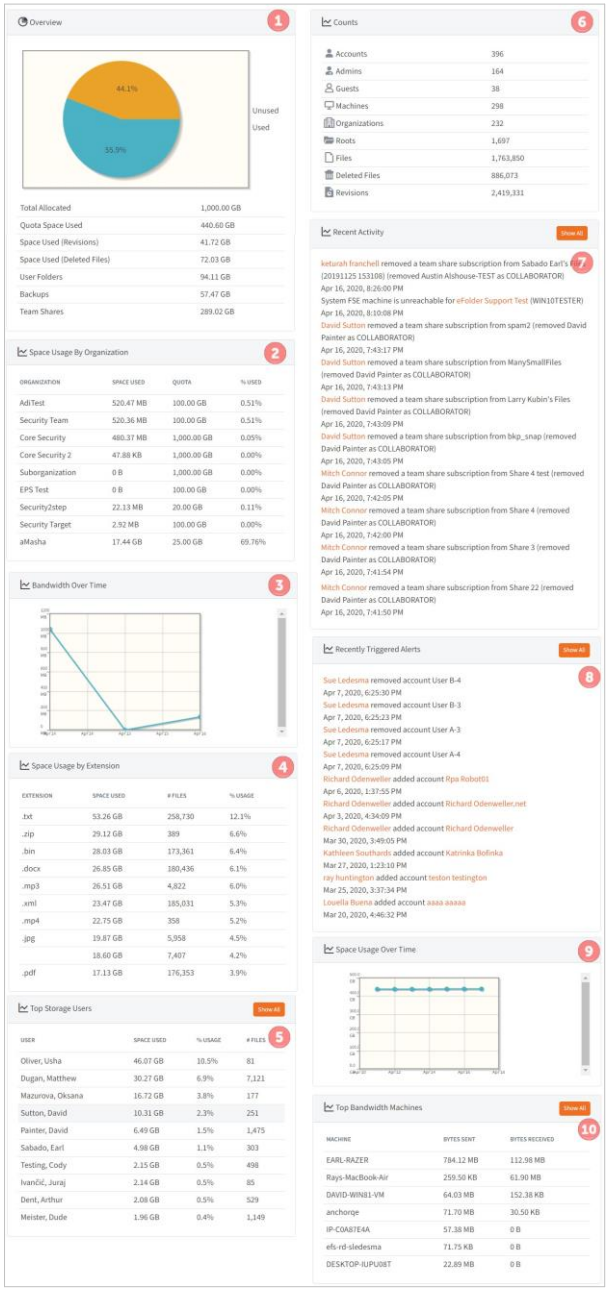
- The *Dashboard* tab provides a snapshot of activity within the selected organization.
- The *Accounts* tab lists all existing user accounts within the selected organization, and also allows you to create new accounts and manage existing accounts.
- The *Machines* tab lists all machines that are registered to user accounts, including laptops, computers, and mobile devices. The *Machines* tab also allows you to set up File Server Enablement.
- The *Shares* tab lists all Team Shares that currently exist in the selected organization. You can also create new Team Shares, view the contents of Team Shares, and manage Team Share permissions.
- The *Backups* tab lists all backups that have been configured within the selected organization and allows you to manage and restore backups if needed.
- The *Activity* tab provides access to the *Activity Log* page, where you can view activity within the selected organization. Additionally, you can create alerts so that you are notified when specific activities occur.
- The *Reports* tab lists all reports that have been created and allows you to edit and modify existing reports. You can also create a report based on specific criteria.
- The *Service Plan* tab lets you define service packages and a create a registration form for clients. When a client submits a registration form, organizations are automatically created with a trial account.
- The *Settings* tab gives you access to configuration options for your selected organization, including policy and setting options.
- The *My Files* tab launches the end user web portal where you can access your personal files, folders, and Team Shares.



How to Review the Dashboard

When you first log in to the administrative web portal, you will see the *Dashboard* page, providing overview information for all organizations. Use the *Organization* navigation menu to view specific information for individual organizations.

1. The *Overview* widget shows allotted space, and compares the percentage of used and unused space. It also displays the number of user folders, backups, and Team Shares.
2. The *Space Usage by Organization* widget shows the breakdown of space used by each individual organization.
3. The *Bandwidth Over Time* widget shows the total amount of data transferred—both uploaded and downloaded—over time.
4. The *Space Usage by Extension* widget shows how much space is used by each file type.
5. The*Top Storage Users* widget shows top storage usage for user accounts.
6. The *Counts* widget shows the number of accounts, admins, guests, machines, organizations, roots, files, deleted files, and revisions.
7. The *Recent Activity*widget shows recent events that occurred in the system.
8. The *Recently Triggered Alerts* widget shows recent events that triggered alerts.
9. The *Space Usage Over Time* widget shows the amount of space used by the system over a period of time.
10. The *Top Bandwidth Machines* widget shows a list of machines, ordered by bandwidth usage. *Bytes Sent* refers to data sent from the server to the desktop client.
    Bytes Received refers to data sent from the desktop client to the server.


1
Overview
44.1%
55.9%
Unused
Used
Total Allocated 1,000.00 GB
Quota Space Used 440.60 GB
Space Used (Revisions) 41.72 GB
Space Used (Deleted Files) 72.03 GB
User Folders 94.11 GB
Backups 57.47 GB
Team Shares 289.02 GB
2
Space Usage By Organization
ORGANIZATION SPACE USED QUOTA % USED
AdiTest 520.47 MB 100.00 GB 0.51%
Security Team 520.36 MB 100.00 GB 0.51%
Core Security 480.37 MB 1,000.00 GB 0.05%
Core Security 2 47.88 KB 1,000.00 GB 0.00%
Suborganization 0 B 1,000.00 GB 0.00%
EPS Test 0 B 100.00 GB 0.00%
Security2step 22.13 MB 20.00 GB 0.11%
Security Target 2.92 MB 100.00 GB 0.00%
aMasha 17.44 GB 25.00 GB 69.76%
3
Bandwidth Over Time
4
Space Usage by Extension
EXTENSION SPACE USED # FILES % USAGE
.txt 53.26 GB 258,730 12.1%
.zip 29.12 GB 389 6.6%
.bin 28.03 GB 173,361 6.4%
.docx 26.85 GB 180,436 6.1%
.mp3 26.51 GB 4,822 6.0%
.xml 23.47 GB 185,031 5.3%
.mp4 22.75 GB 358 5.2%
.jpg 19.87 GB 5,958 4.5%
18.60 GB 7,407 4.2%
.pdf 17.13 GB 176,353 3.9%
Top Storage Users
Show All
5
USER SPACE USED % USAGE # FILES
Oliver, Usha 46.07 GB 10.5% 81
Dugan, Matthew 30.27 GB 6.9% 7,121
Mazurova, Oksana 16.72 GB 3.8% 177
Sutton, David 10.31 GB 2.3% 251
Painter, David 6.49 GB 1.5% 1,475
Sabado, Earl 4.98 GB 1.1% 303
Testing, Cody 2.15 GB 0.5% 498
Ivančić, Juraj 2.14 GB 0.5% 85
Dent, Arthur 2.08 GB 0.5% 529
Meister, Dude 1.96 GB 0.4% 1,149
6
Counts
Accounts 396
Admins 164
Guests 38
Machines 298
Organizations 232
Roots 1,697
Files 1,763,850
Deleted Files 886,073
Revisions 2,419,331
Recent Activity
Show All
7
keturah franchell removed a team share subscription from Sabado Earl's
(20191125 153108) (removed Austin Alshouse-TEST as COLLABORATOR)
Apr 16, 2020, 8:26:00 PM
System FSE machine is unreachable for eFolder Support Test (WIN10TESTER)
Apr 16, 2020, 8:10:08 PM
David Sutton removed a team share subscription from spam2 (removed David
Painter as COLLABORATOR)
Apr 16, 2020, 7:43:17 PM
David Sutton removed a team share subscription from ManySmallFiles
(removed David Painter as COLLABORATOR)
Apr 16, 2020, 7:43:13 PM
David Sutton removed a team share subscription from Larry Kubin's Files
(removed David Painter as COLLABORATOR)
Apr 16, 2020, 7:43:09 PM
David Sutton removed a team share subscription from bkp_snap (removed
David Painter as COLLABORATOR)
Apr 16, 2020, 7:43:05 PM
Mitch Connor removed a team share subscription from Share 4 test (removed
David Painter as COLLABORATOR)
Apr 16, 2020, 7:42:05 PM
Mitch Connor removed a team share subscription from Share 4 (removed
David Painter as COLLABORATOR)
Apr 16, 2020, 7:42:00 PM
Mitch Connor removed a team share subscription from Share 3 (removed
David Painter as COLLABORATOR)
Apr 16, 2020, 7:41:54 PM
Mitch Connor removed a team share subscription from Share 22 (removed
David Painter as COLLABORATOR)
Apr 16, 2020, 7:41:50 PM
Recently Triggered Alerts
Show All
8
Sue Ledesma removed account User B-4
Apr 7, 2020, 6:25:30 PM
Sue Ledesma removed account User B-3
Apr 7, 2020, 6:25:23 PM
Sue Ledesma removed account User A-3
Apr 7, 2020, 6:25:17 PM
Sue Ledesma removed account User A-4
Apr 7, 2020, 6:25:09 PM
Richard Odenweller added account Rpa Robot01
Apr 6, 2020, 1:37:55 PM
Richard Odenweller added account Richard Odenweller.net
Apr 3, 2020, 4:34:09 PM
Richard Odenweller added account Richard Odenweller
Mar 30, 2020, 3:49:05 PM
Kathleen Southards added account Katrinka Bofinka
Mar 27, 2020, 1:23:10 PM
ray huntington added account teston testington
Mar 25, 2020, 3:37:34 PM
Louella Ruona added account aaaa aaaaa
Mar 20, 2020, 4:46:32 PM
Space Usage Over Time
9
Top Bandwidth Machines
Show All
10
MACHINE BYTES SENT BYTES RECEIVED
EARL-RAZER 784.12 MB 112.98 MB
Rays-MacBook-Air 259.50 KB 61.90 MB
DAVID-WIN81-VM 64.03 MB 152.38 KB
anchorqe 71.70 MB 30.50 KB
IP-C0A87E4A 57.38 MB 0 B
efs-rd-sledesma 71.75 KB 0 B
DESKTOP-IUPU08T 22.89 MB 0 B

Installing and Configuring the x360Sync Server (Private Cloud)

When you host x360Sync on your own server, it is recommended that you configure x360Sync and its components according to best practices.

The system requirements for the server are as follows:

Requirement	Minimum	Recommended
Hard Disk	80GB minimum hard disk, with 350mb required for installation	1TB+ direct-attached hard disk 6gb/s transfer speed 32mb cache 7200+RPM or SSD
Ram	2gb	6gb
CPU	2Ghz single core	3Ghz quad-core
OS	Windows 2008 R2, Windows 2012, Windows 2012 R2, and Windows Server 2016	Same

You should install the most current revision of x360Sync and its components using the *Setup Wizard*. By default, the *Setup Wizard* installs the following services on one machine:

- x360Sync Server
- Apache Server
- PostgreSQL Database

NOTE

You must contact the x360Sync Support Team to schedule a consultation before configuring a high availability environment.

TCP Ports

Before installing x360Sync and its components, please be aware that the following TCP ports must be open on the firewall:

- 510—HTTPS connections
- 443—Secure agent-server connections
- 80—HTTP connections

Backing Up and Restoring the x360Sync Server

It is recommended that you perform a file-level backup on the drive where your file store exists, and a bare-metal backup of your x360Sync server. These can be scheduled at the same time for consistency.

There are three components that we recommend you back up in order to ensure rapid restoration and prevent data loss:

- File store—stores raw binary data, and is configured during the system setup process. This can be configured as a file-level backup.
- DB store—stores file and folder metadata. By default, this is located at c:\x360SyncServer\store_#. Because these databases typically reside on the same drive as your server, we recommend that you perform a bare-metal snapshot of this drive for quick restoration.
- PostgreSQL—stores business object information, including accounts, usernames,and passwords. It is located at c:\PostgreSQL9.1\. This also resides on the same drive as the x360Sync Server and should be included in the bare-metal backup.

This section will provide detailed instructions for installing x360Sync, configuring x360Sync, and setting up SSL certificates. When setting up SSL certificates, please note that you can use an existing SSL certificate, convert an existing IIS *.pfx* file, or configure a new SSL certificate (or wildcard certificate) for use.

How to Install the x360Sync Server (Private Cloud)

After you are registered and you receive your license key, you can download and install the latest server installer. The server installer includes each required component, including the x360Sync server, Apache server, and PostgreSQL database.

NOTE

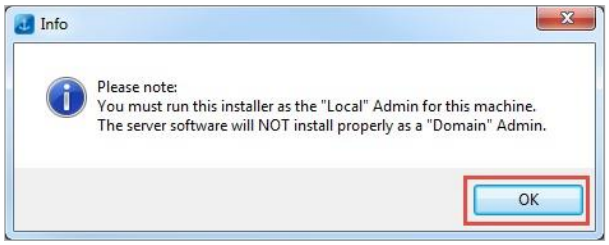
Please run the server installer as a local administrator (not as a domain administrator) on a stand-alone Windows Server. PostgreSQL cannot install properly if the server is a member of a domain. You can optionally elevate the server to a domain after installation.

NOTE

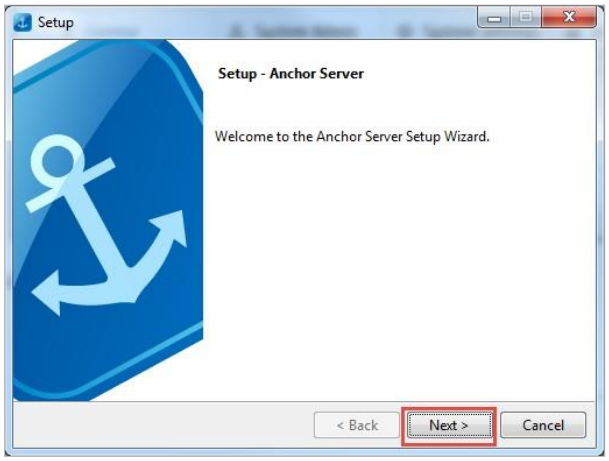
If you would like to configure a high-availability environment, please contact the x360Sync Support Team.

To install the x360Sync server:

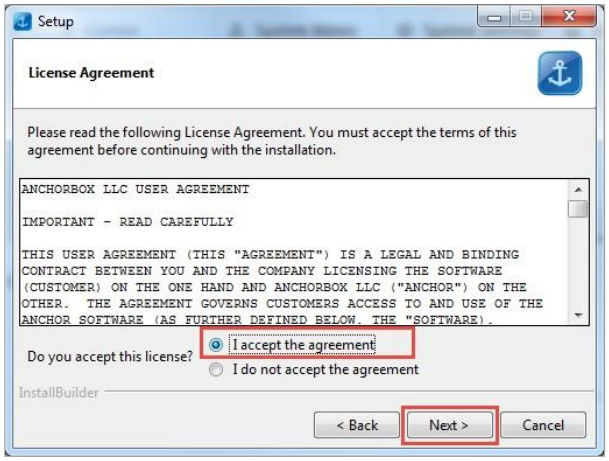
1. Double-click the installation file to launch the *Setup Wizard*. A pop-up message displays, warning you that you must be signed in as a local administrator, and not as a domain administrator.
2. In the pop-up message, click the **OK** button to confirm that you are signed in as a local administrator.



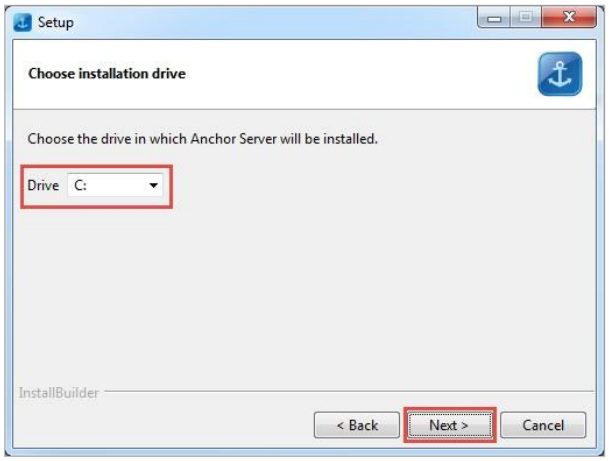
   The *Setup Wizard* displays with a welcome message.
3. In the *Setup Wizard*, click the **Next** button to continue.



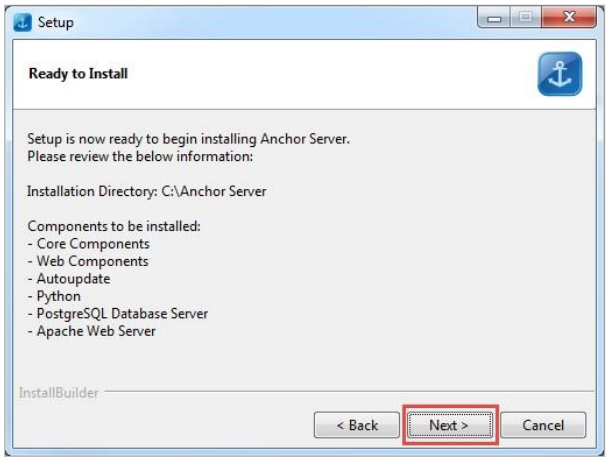
4. In the *License Agreement* screen, click the **I accept the agreement** radio button if you accept the license agreement. Click the **Next** button to continue.



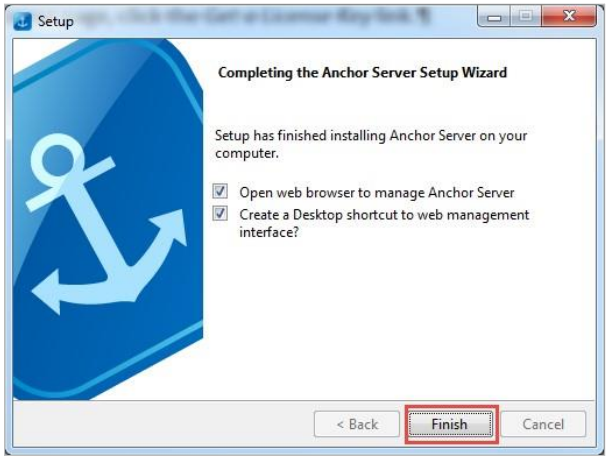
5. In the *Choose Installation Drive* screen, use the *Drive* drop-down menu to select the **drive** on which x360Sync Server will be installed. Click the **Next** button to continue.



6. In the *Ready to Install* screen, click the **Next** button to begin the installation process.



7. When the installation process is complete, the *Setup Wizard* will display a confirmation screen. it is recommended that you select the **Open Web Browser to Manage x360Sync Server** checkbox, as well as the **Create a Desktop Shortcut to Web Management Interface** checkbox, to easily access the administrative web portal. Click the **Finish** button to close the *Setup Wizard*.



x360Sync is now installed, and you will be presented with the administrative web portal in your default browser.

How to Configure the x360Sync Server (Private Cloud)

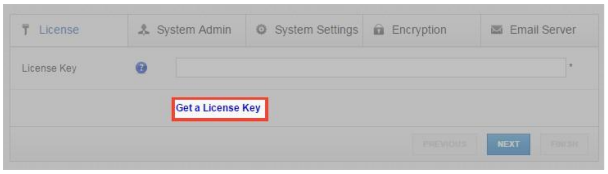
After x360Sync server is installed, you will need to enter a license key and configure general system settings in the administrative web portal.

NOTE

Your Private Cloud license key can only be used once during registration. The original license key cannot be detached and re-provisioned. A new key must be requested for each registration.

To configure the x360Sync server:

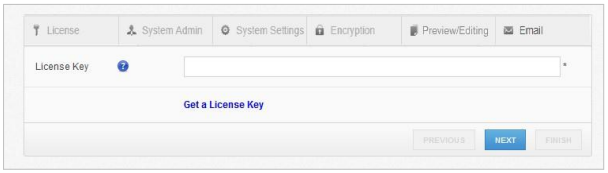
1. Open the administrative web portal. The administrative web portal will display, showing the *License* tab.
2. In the *Licensee* tab, click the **Get a License Key** link.



   Your web browser will redirect you to the *Home* page in your x360Sync account.
3. In the *Home* page of your x360Sync account, click the **Licenses** navigation item.

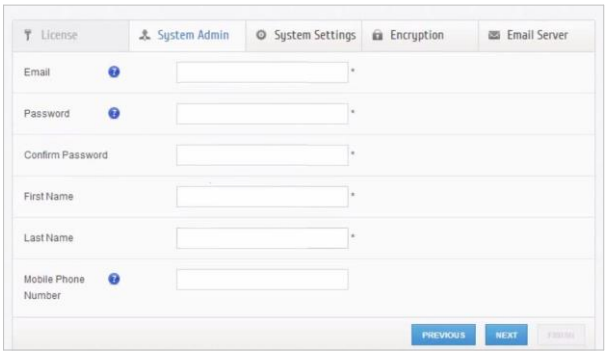
   The *Licenses* page displays.
4. In the *Licenses* page, record the license number. Please note that your Private Cloud license key can only be used once during registration. The original license key cannot be detached and re-provisioned. A new key must be requested for each registration.

5. Return to the administrative web portal, and enter the **license key** into the *License Key* field, and click the **Next** button.



The license key will be validated by the system, and you will be redirected to the *System Admin* tab.

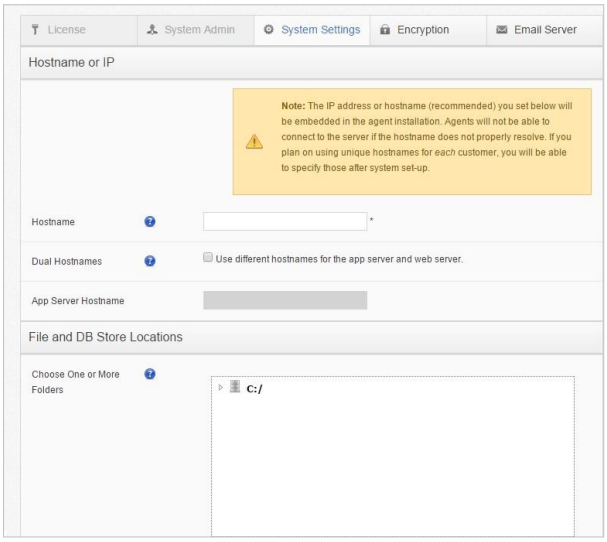
6. In the *System Admin* tab, enter information about the system administrator account.
   a. In the *Email* field, enter the **email address** of the system administrator account.
   b. In the *Password* field, enter a **password** for the system administrator account.
   c. In the *Confirm* Password filed, **confirm the password** for the system administrator account.
   d. In the *First Name* field, enter the **first name** of the system administrator.
   e. In the *Last Name* field, enter the **last name** of the system administrator.
   f. In the *Mobile Phone Number* field, enter a **phone number**, so that the system administrator can optionally receive text message alerts.
   g. Click the **Next** button when you are finished.



7. In the *System Settings* page, enter server information for x360Sync.
   a. In the *Hostname* field, enter the publicly available **hostname or IP address** that will be used by your desktop clients to connect with the x360Sync server.
   b. Use the **Dual Hostnames** checkbox to specify separate hostnames for the application server and the web server. We recommend that you set up dual hostnames *after* you complete the initial configuration process. You will be required to set some network translation rules on the firewall and server to use dual hostname settings; you will also need two unique public IP addresses.
   For more information, please contact the x360Sync Support Team.
   c. In the *Choose Folders* area, select the **folder** where the raw binary data will be stored (at least 1TB of direct-attached hard disk space is recommended).

Please note that you must use a permanently mounted drive during the initial setup process. After you complete the setup process, you can migrate the store path to a network drive (for example, SAN or NAS). For more information, please contact the x360Sync Support Team. If you need to add additional disk space in the future, you can configure new store locations in the *Stores* tab, which is located under the *Settings* tab in the administrative web portal.

d. In the *File and DB Store Locations* area, select the **folder** where file metadata will be stored. By default, this location is set to the x360Sync directory; optionally, you can also select a separate drive.



8. Also in the *System Settings* page, you can optionally enter information about the master organization; or, you can configure this information later. Click the **Next** button when you are finished.
9. In the **Encryption** tab, determine how your database encryption key will be stored.
   a. Click the **Persistent** radio button to permanently store the encryption key to the database.
   b. Alternatively, click the **Transient** radio button to protect the key with a key password, which must be entered each time the service is restarted. You only need to select this option if you do not trust the server on which x360Sync resides. Please note that if you forget this key password, it cannot be reset.

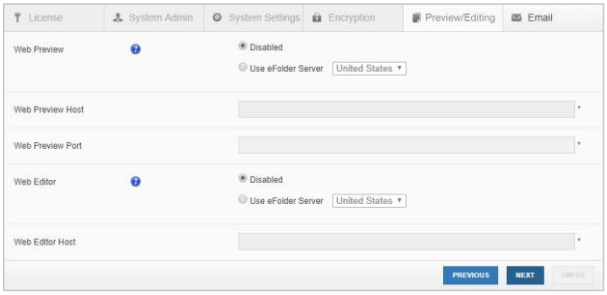
c. If you select the *Transient* radio button, enter a **password** in the *Key Password* field. You must also confirm the password in the *Conform Password* field.

d. Click the **Next** button when you are finished.

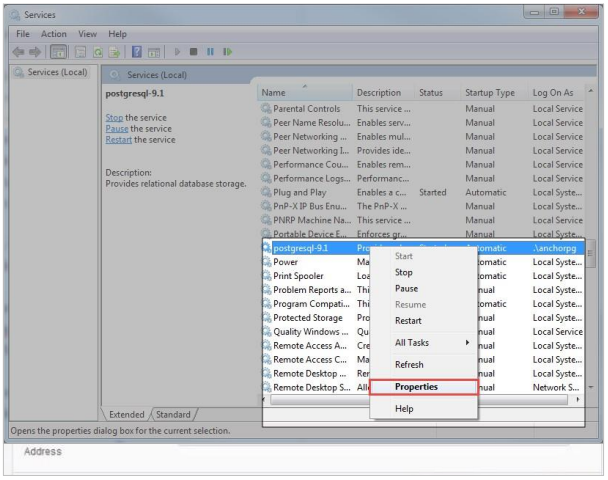
10. In the *Preview/Editing* tab, you can optionally configure settings for the Web Preview server and the Web Editor server.

    a. In the *Web Preview Settings* section, click the **Use Server** radio button, and then use the drop-down menu to select the server most closely matching your environment's geographic location. The *Web Preview Host* field and the *Web Preview Port* field will populate based on your selection.

    b. In the *Web Editor Settings* section, click the **Use Server** radio button, and then use the drop-down menu to select the server most closely matching your environment's geographic location. The *Web Editor Host* field will populate based on your selection.



11. In the *Email Server* tab, configure your email server settings; or, you can configure this information later. For information about configuring an email server, please reference the *How to Specify an Email Server* section of the Guide.



You are now ready to begin using x360Sync.

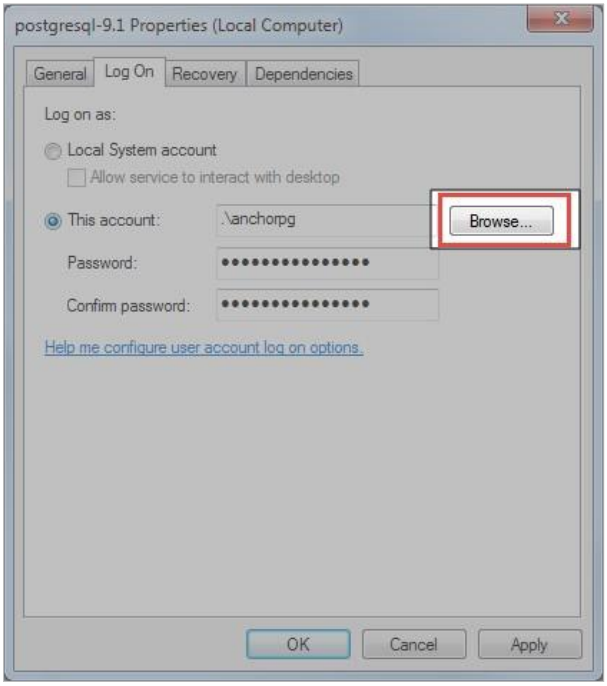
How to Add x360Sync to a Windows Domain (Private Cloud)

You must install the x360Sync Server software onto a standalone server as a local admin; PostgreSQL cannot install properly if the server is a member of a domain. After x360Sync has successfully been installed, you can join the x360Sync server to your Windows Domain.

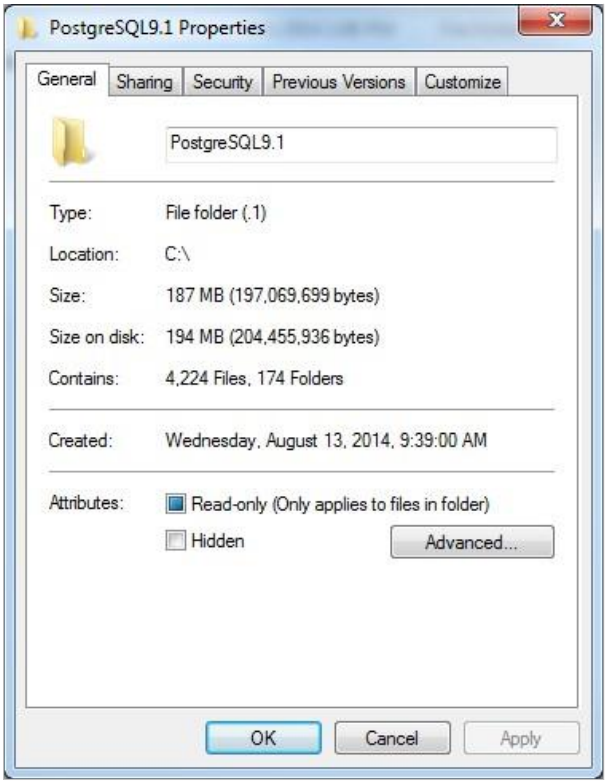
To add x360Sync to a Windows Domain:

1. In Active Directory, create a user named, *anchorpg*, which is the same user that was created when PostgreSQL was installed.
2. On your x360Sync server, click the **Start** menu, enter **services.msc** into the search box, and press the **Enter** key. The *Services* window displays.
3. In the *Services* window, right-click the *PostgreSQL* service, and select **Properties**.

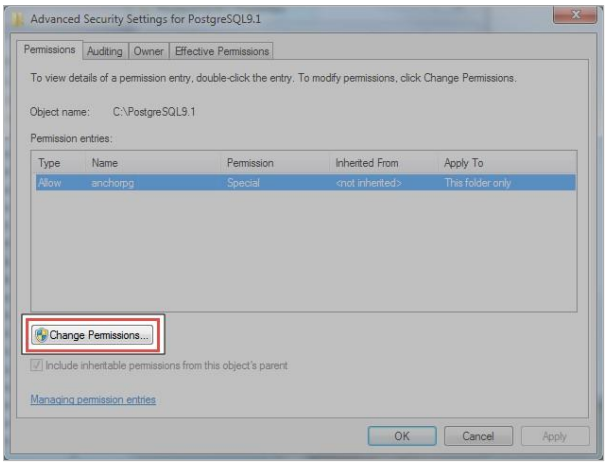
   The *Properties* dialog box displays.
4. In the *Properties* dialog box, click the **Log On** tab. The *Log On* tab displays.
5. In the *Log On* tab, click the **This account** radio button, and browse to select the *anchorpg* user you created in Active Directory, making sure that you enter the same password (the password can be found in the *[target drive]:\anchorserver \conf\config.ini* file).



6. Click the **OK** button when you are finished.
7. While still in the x360Sync server, right-click the PosgreSQL directory (for example, C:\PostgreSQL9.1), and select **Properties**. The *Properties* dialog box displays.

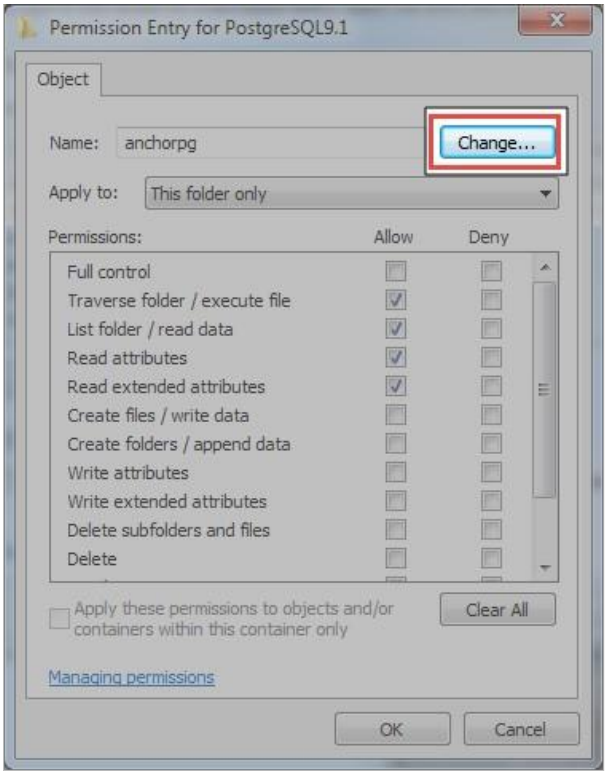


8. In the *Properties* dialog box, click the**Security** tab. The *Security* tab displays.
9. In the *Security* tab, click the **Advanced** button. The *Advanced Security Settings* dialog box displays.
10. In the *Advanced* dialog box, click the **Change Permission** button.



The *Permission* tab displays.

11. In the *Permission entries* box, highlight the *anchorpg* user and click the Edit button. The *Object* tab displays.
12. In the *Object* tab, click the **Change** button.



The **Select User or Group** dialog box displays.

13. In the *Select User or Group* dialog box, change the user to the *anchorpg* Active Directory user.
14. Click the **OK** button when you are finished.
15. Navigate to the PostgreSQL data folder (for example, C:\PostgreSQL9.1\data),and give the *anchorpg Active Directory user* full permissions to the folder.
16. Return to the *Services* window and restart the *PostgreSQL* service, the *x360Sync* service, and the *Apache* service. x360Sync has now been added to your Windows domain.

Installing and Configuring SSL Certificates (Private Cloud)

A valid CA signed SSL certificate must be installed on both the Apache server and the x360Sync application server. Specifically:

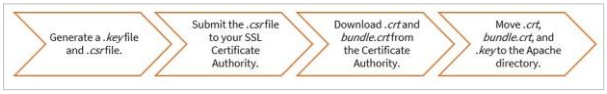
- A valid CA signed SSL certificate must be installed on your Apache server to allowmobile devices to connect.
- A valid CA signed SSL certificate must be installed on your x360Sync applicationserver to allow desktop clients to connect, and to support WebDAV.

When configuring SSL certificates, you might decide to convert an IIS certificate, use an existing SSL certificate, or configure a new SSL certificate. This section will cover each of these options.

How to Convert an Existing IIS .pfx File (Private Cloud)

After x360Sync is installed and configured, you can set up SSL certificates to allow for secure connections to your Apache server. Specifically, you will need to add a *.crt* file (certificate file) and a *bundle.crt* file in your Apache SSL directory. Unsigned certificates are not supported.

When you create a *new* SSL certificate or wildcard certificate, you generate a *.key* file (private key), as well as a *.csr* file (certificate signing request file), using your OpenSSL application. You then submit the *.csr* file to the SSL Certificate Authority of your choice (for example, GoDaddy, Thawte, Verisign, and so forth) in order to receive the appropriate *.crt* (certificate file)and *bundle .crt* files, which are then installed on your Apache web server.



If you already have an existing IIS *.pfx* file (Personal Information Exchange file), you can use it to extract both a *.key* file and a*.crt* file using your OpenSSL application.

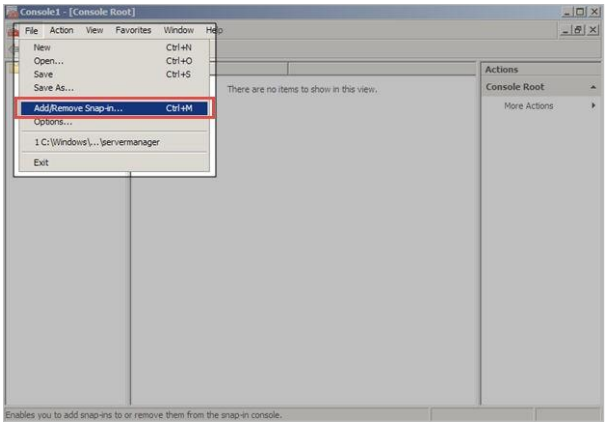
This article will review the following steps in detail:

- Export an IIS certificate to a *.pfx* file

- Use the OpenSSL application to extract the *.key* file and the *.crt* file
- Update the *.crt* file

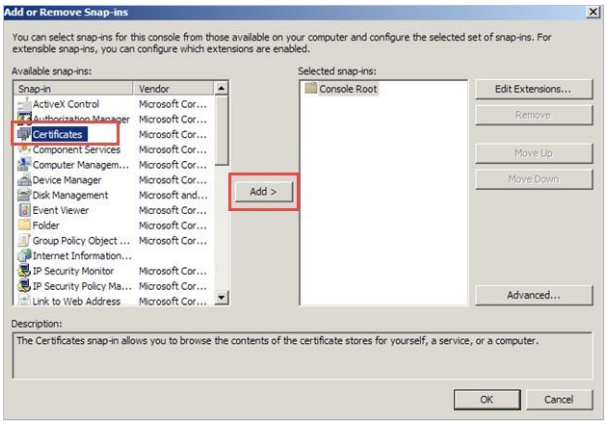
To Export an IIS certificate:

1. From the *Start* menu, enter **mmc.exe** into the search box and press the **Enter** key. The *Microsoft Management Console* window displays.
2. In the *Microsoft Management Console* window, click the **File** menu, and select **Add/Remove Snap in**.



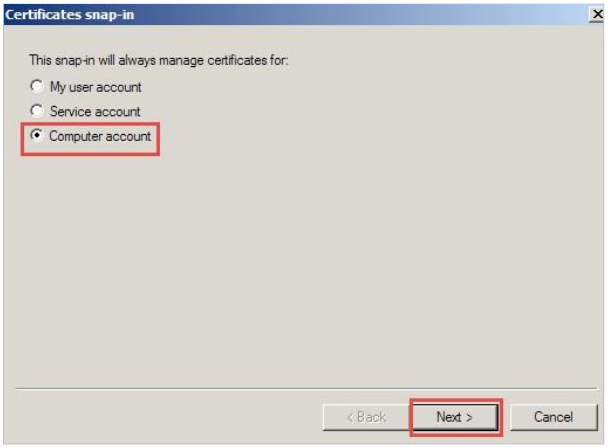
The *Add or Remove Snap-ins* dialog box displays.

3. In the *Add or Remove Snap-ins* dialog box, select **Certificates**, and then click the **Add** button.

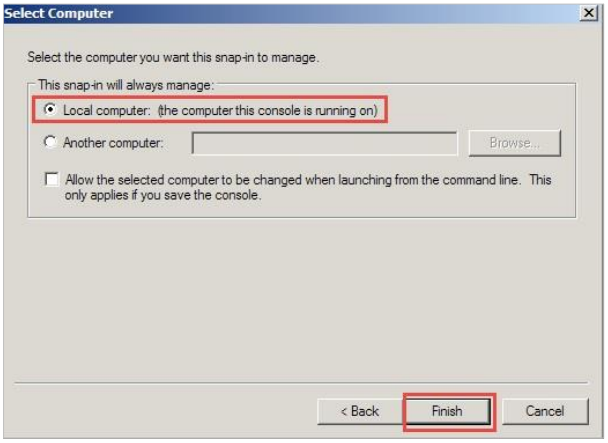


The *Certificates Snap-in* dialog box displays.

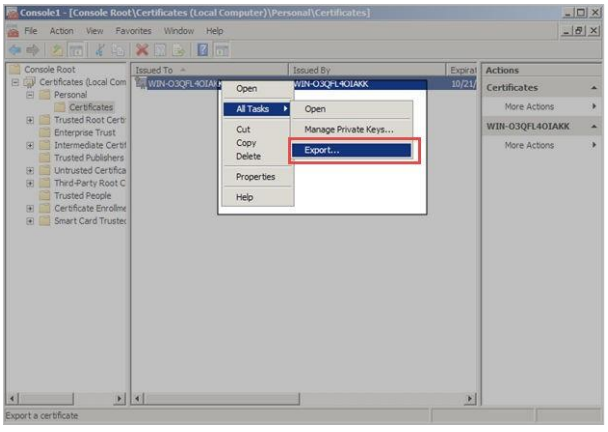
4. In the *Certificates Snap-in* dialog box, select the **Computer account**radio button, and then click the **Next** button.



5. In the *Select Computer* dialog box, select the **Local computer** radio button, and then click the **Finish** button.



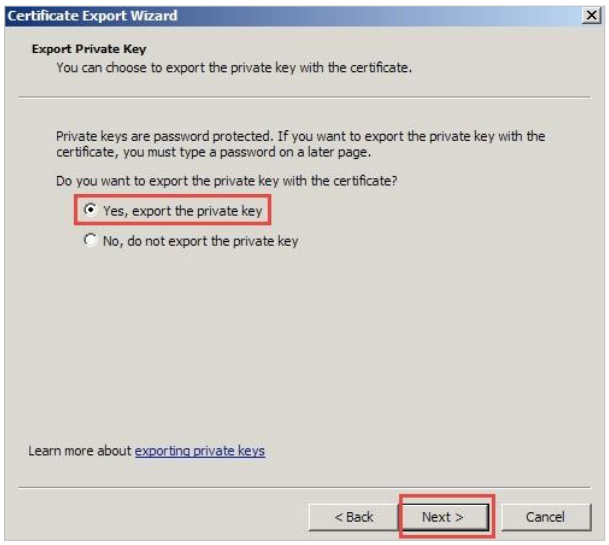
6. Click the **OK** button to close the *Add or Remove Snap-ins* dialog box.
7. Back in the *Microsoft Management Console* window, click to expand the **Certificate** folder, then click to expand the **Personal** folder, and then select the **Certificates** folder. A list of certificates will display.
8. Right-click the certificate you want to export; point to *All Tasks*, and then select **Export**.



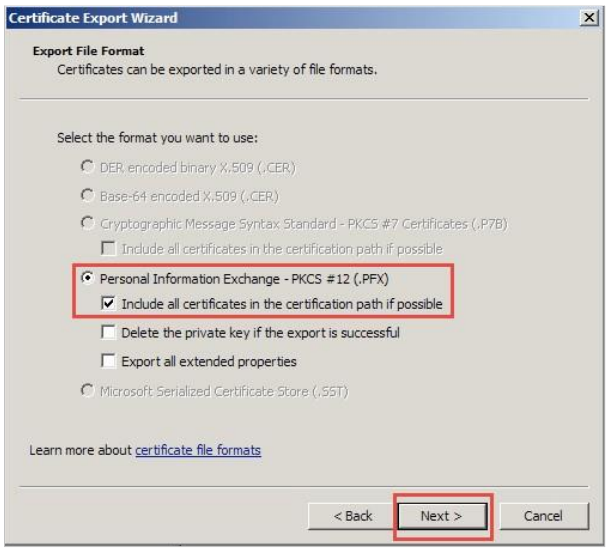
The *Certificate Export Wizard* displays.

9. In the *Certificate Export Wizard*, click the **Next** button to begin.

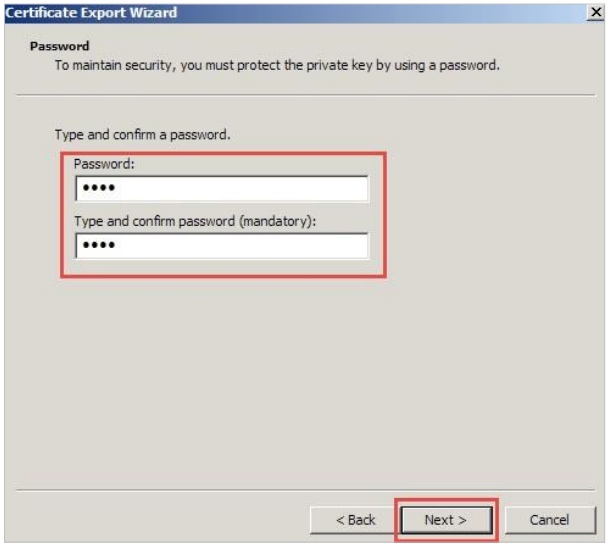
10. In the *Export Private Key screen*, select the **Yes, export the private key** radio button. Click **Next** to continue.



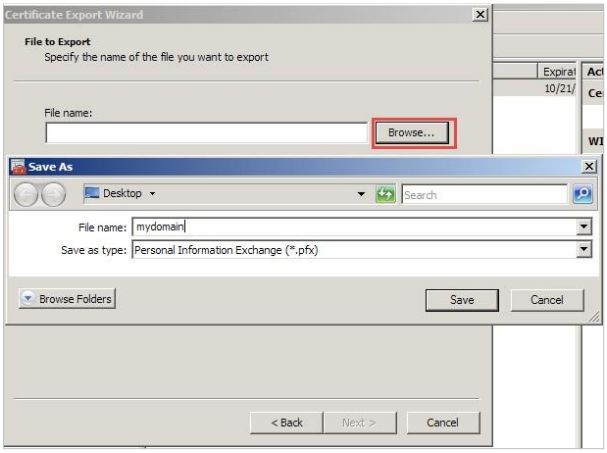
11. In the *Export File Format* screen, click the **Personal Information Exchange** radio button, and then select the **Include all certificates in the certification path if possible** checkbox. Click the **Next** button to continue.



12. In the *Password* screen, type and confirm a **password**. Click the **Next** button to continue.

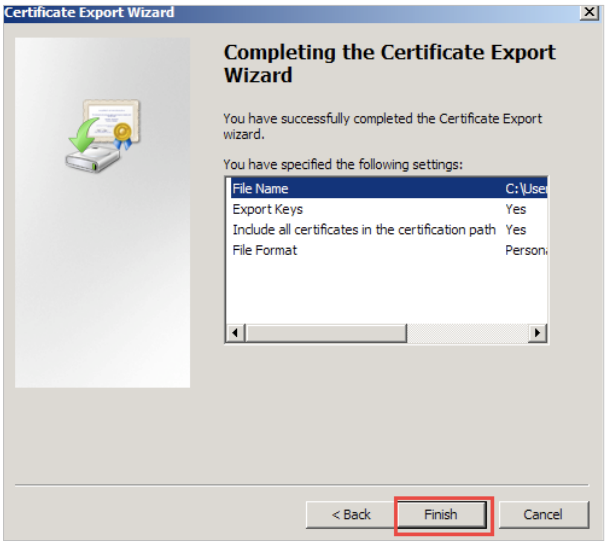


13. In the *File to Export* screen, click the **Browse** button to find a location to save the *.pfx* file.



Click the **Next** button to continue.

14. When the *Certificate Export Wizard* is complete, click the **Finish** button.

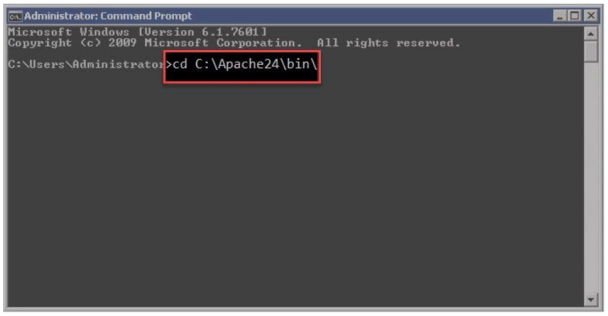


The *.pfx* file, which contains the *.crt* file and the *.key* file, is now saved.

Next, use the OpenSSL application to extract the *.key* file and the *crt* file.

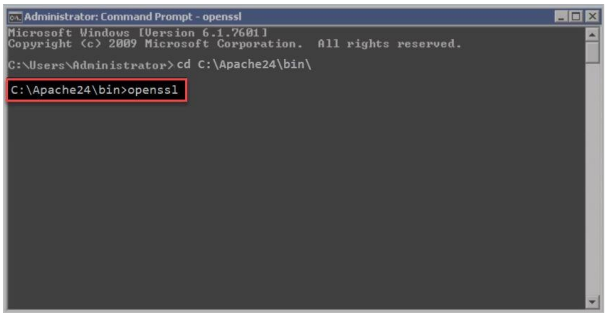
1. From the *Start* menu, enter **cmd** into the search box and press the **Enter** key. A new *Command Prompt* window displays.
2. In the *Command Prompt* window, navigate to the Apache bin directory using the *cd* command, and press the Enter key:

   cd C:\Apache24\bin



3. While still in the *Command Prompt* window, launch the openssl application using the *openssl* command:

   openssl



4. Within the OpenSSL application, export the *crt* file from the *.pfx* file using the following command:

   pkcs12 -in filename.pfx -nocerts -out key.pem

5. After the pfx file is exported, export the *crt* file from the *.pfx* file using the following command:

   pkcs12 -in filename.pfx -clcerts -nokeys -out yourdomainname.crt

6. Remove the password from the *.key* file so Apache will not prompt you for your password when it starts.

   -in key.pem –out yourdomainname.key

Finally, you can update your *crt* file.

1. Open the *.crt* file.
2. Delete all content that is listed before the -----BEGIN CERTIFICATE----- section.

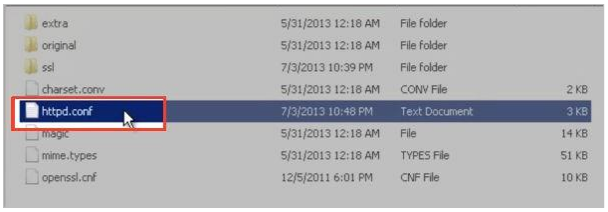
3. Save the *crt* file. You can now configure Apache to use these files. For more information, please reference the *How to Use an Existing SSL Certificate with Apache* section of the Guide.

How to Use an Existing SSL Certificate (Private Cloud)

Alternatively, if you already have the required *.key* file, *.crt* file, and *bundle.crt* file, you can simply move these files into your Apache directory. You must also update the Apache *httpd.conf* file to reflect this change.

To use an existing SSL certificate with Apache:

1. In your server, copy the following files:
   - *.key* file
   - *.crt* file
   - *bundle.crt* file
2. Paste the three files into your Apache SSL directory (for example, C:*Apache24**conf**ssl*).
3. Navigate to Apache's *conf* directory (for example, *C:\Apache24**conf*\) and open the *httpd.conf* file.



4. In the *VirtualHost* section, update the following lines:
   - SSLCertificateFile "C:\Apache24\conf\ssl\yourdomainname.crt"
   - SSLCertificateKeyFile "C:\Apache24\conf\ssl\yourdomainname.key"
   - SSLCertificateChainFile "C:\Apache24\conf\ssl\yourbundle.crt"For example:

     < VirtualHost_default_:510>

     SSLEngine on

     SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDI-UM:+LOW:+SSLv2:+EXP:+eNULL

     SSLCertificateFile "C:\Apache24\conf\ssl\anchor.crt"

     SSLCertificateKeyFile "C:\Apache24\conf\ssl\anchor.key"

```
SSLCertificateChainFile "C:\Apache24\conf\ssl\anchorbundle.crt"
```

AllowEncodedSlashes On
</VirtualHost>

Your SSL certificate is now ready for use with Apache.

How to Configure a New SSL Certificate (Private Cloud)

You can also create a *new* SSL certificate or wildcard certificate. When you do this, you generate a *.key* file (private key), as well as a *.csr* file (certificate signing request file), using your OpenSSL application. You then submit the *.csr* file to the SSL Certificate Authority of your choice (for example, GoDaddy, Thawte, Verisign, and so forth) in order to receive the appropriate *.crt* (certificate file) and *bundle .crt* files, which are then installed on your Apache web server.

NOTE

This process is for *new* SSL certificates or wildcard certificates. If you already have an existing SSL certificate, please reference the *How to Use an Existing SSL Certificate with Apache* section of the Guide.

NOTE

If you already have an existing IIS *.pfx* file, you must convert it to a *.key file* using the OpenSSL application. For more information, please reference the *How to Convert an Existing IIS .pfx File to a Private Key File* section of the Guide.

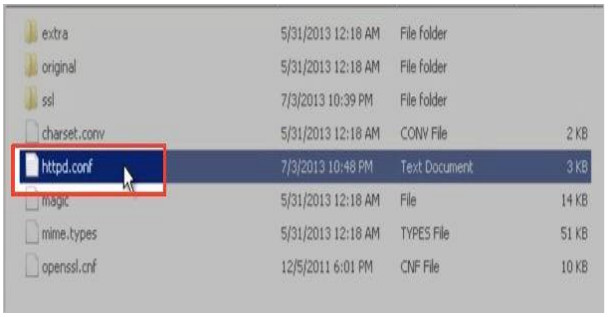
This article will review the following steps in detail:

- Use the OpenSSL application to generate a *.key* file
- Use the OpenSSL application to generate a *.csr* file
- Purchase a certificate from an SSL Certificate Authority using the newly gener-ated *.csr* file
- Update the SSLCertificateChainFile path in the *http.conf* file To generate a *.key* file

  using the OpenSSL application:

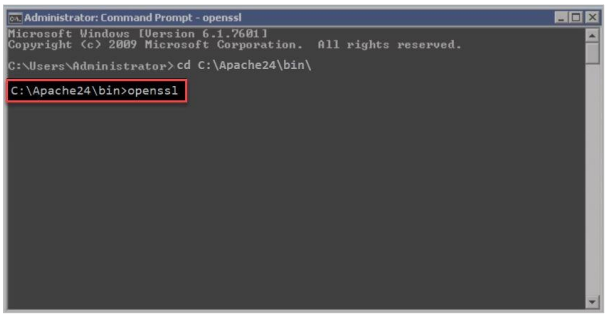
1. From the *Start* menu, enter **cmd** into the search box and press the **Enter** key. A new *Command Prompt* window displays.
2. In the *Command Prompt* window, navigate to the Apache bin directory using the *cd* command, and press the Enter key:

   cd C:\Apache24\bin



3. While still in the *Command Prompt* window, launch the openssl application using the *openssl* command:

   openssl

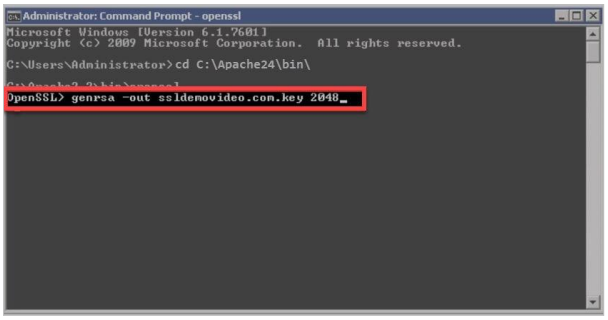


4. Within the OpenSSL application, generate a *.key* file using the *genrsa* command:

   genrsa –out yourdomainname.key 2048

   For example:

   genrsa -out yourdomainname.key 2048

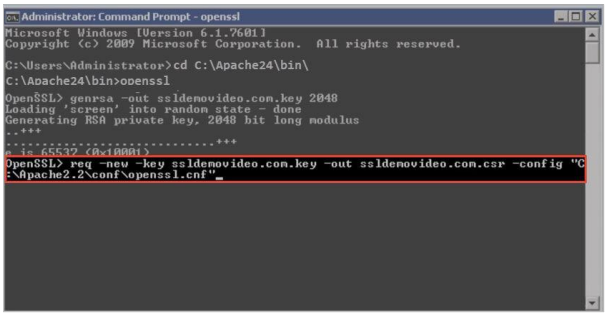


To generate a *.csr* file using the OpenSSL application:

1. While still in the OpenSSL application, generate a *.csr* file using the following command:

   req -new –key yourdomainname.key –outyourdomainname.csr-config "C:\Apache24\conf\openssl.cnf" For example:

   OpenSSL> req -new -key yourdomainname.key -out yourdomainname.csr -config "C:\Apache24\conf\openssl.cnf"



2. You will be prompted to enter information into the *Command Prompt* window:
   a. When prompted to enter a *Country Name*, enter your country's two letter code (for example, US).
   b. When prompted to enter a *State or Providence Name*, enter the full name of your state or providence (for example, California).
   c. When prompted to enter a *Locality Name*, enter the full name of your city (for example, San Francisco).
   d. When prompted to enter an *Organization Name*, enter the name of your organization.
   e. When prompted to enter an *Organizational Unit Name*, enter your organizational unit, or leave this field blank.
   f. When prompted to enter a *Common Name*, enter your server FQDN (for example, *hostname.yourdomainname.com*, or **.yourdomainname.com* for a wildcard certificate).

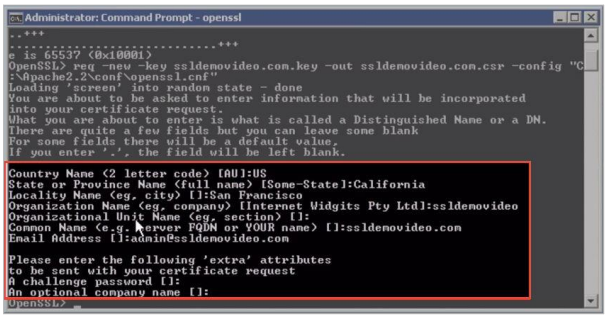
NOTE

Make sure you have access to the email account that you provide. Depending upon the SSL Certificate Authority you select, you might need to validate ownership of your domain.

NOTE

You must include a * symbol in front of your yourdomainname.com if you are registering a wildcard certificate.

   g. When prompted to enter your email address, enter a valid email address.
   h. When prompted to enter *extra* attributes (a challenging password and an optional company name), leave these fields blank.



To Purchase a certificate from an SSL Certificate Authority:

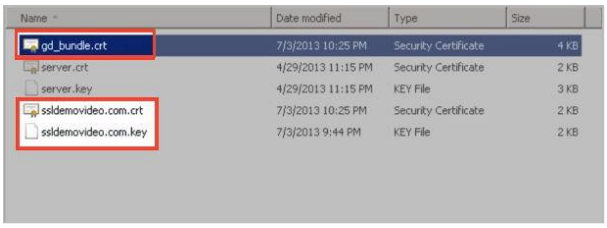
1. Purchase a certificate from an SSL Certificate Authority of your choice using your newly generated *.csr* file. For example, you may wish to purchase from GoDaddy, Thawte, Verisign, and so forth.
2. Each of these Certificate Authorities will require a specific set of steps for submitting the content of your newly generated *.csr* file. Follow the specific set of instructions provided by your selected Certificate Authority.

> **NOTE**
>
> Depending upon the SSL Certificate Authority you selected, you might need to validate ownership of your domain.

3. When prompted to submit your *.csr* file, you can access the file in the Apache directory (for example, *C:\Apache24\bin_.yourdomainname.com.csr*).

   Your SSL Certificate Authority will provide you with two files: a *.crt* file and a *yourbundle.crt* file. Make sure that you specify Apache server type when you download the files.

4. After your SSL Certificate Authority provides you with the *.crt* file and the *yourbundle.crt* file, move the files into the *C:\Apache24\conf\ssl* directory. Specifically:
   a. Move the *.crt* file into Apache's *ssl* directory (for example, *C:\Apache24\conf\ssl*).
   b. Move the *yourbundle.crt* file into Apache's *ssl* directory (for example, *C:\Apache24\conf\ssl*).
   c. Move the *.key* file from Apache's *bin* directory to Apache's *ssl* directory (for example, from *C:\Apache24\bin* to *C:\Apache24\conf\ssl*).



To update the SSLCertificateChainFile path in the *http.conf* file:

1. Navigate to Apache's *conf* directory (for example, *C:\Apache24\conf*) and open the *httpd.conf* file.

2. For single certificates, in the *VirtualHost* section, update the following lines:
   - SSLCertificateFile "C:\Apache24\conf\ssl\yourdomainname.crt"
   - SSLCertificateKeyFile "C:\Apache24\conf\ssl\yourdomainname.key"
   - SSLCertificateChainFile "C:\Apache24\conf\ssl\yourbundle.crt"*<VirtualHost_default_:510>SSLEngine onSSLCipherSuite ALL:!*

     ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDI-UM:+LOW:+SSLv2:+EXP:+eNULLSSLCertificateFile "C:\Apache24\conf\ssl\yourdomainname.crt"SSLCertificateKeyFile "C:\Apache24\conf\ssl\yourdomainname.key"SSLCertificateChain-File "C:\Apache24\conf\ssl\yourbundle.crt"AllowEncodedSlashes On</VirtualHost>
3. Alternatively, for wildcard certificates, update the following lines:

- <VirtualHost *:510>
- ServerName yourdomainname.com
- ServerAlias *.yourdomainname.com
- SSLCertificateFile "C:\Apache24\conf\ssl\yourdomainname.crt"
- SSLCertificateKeyFile "C:\Apache24\conf\ssl\yourdomainname.key"
- SSLCertificateChainFile "C:\Apache24\conf\ssl\yourbundle.crt"For example:

*<VirtualHost *:510>*

ServerName anchor.com

*ServerAlias *.anchor.com*

SSLEngine on

SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM

SSLCertificateFile "C:\Apache24\conf\ssl\yourdomainname.crt"

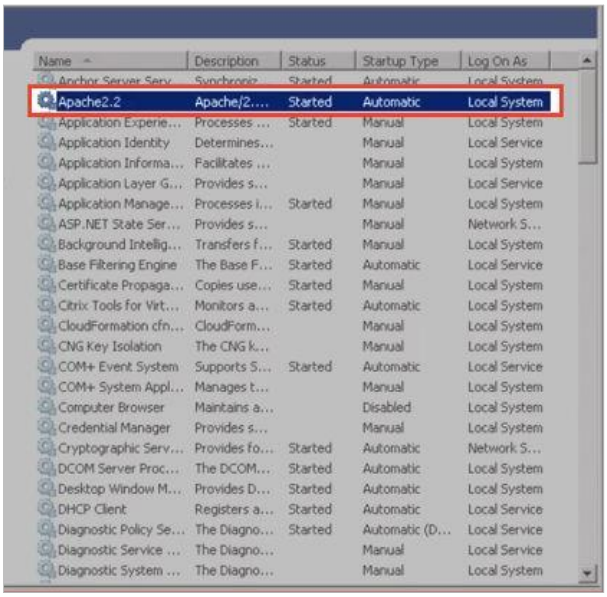
SSLCertificateKeyFile "C:\Apache24\conf\ssl\yourdomainname.key"

SSLCertificateChainFile "C:\Apache24\conf\ssl\yourbundle.crt"

AllowEncodedSlashes On

</VirtualHost>

4. Save and close the file.
5. In the *Start* menu, enter **Services** into the search box and press the **Enter** key. The *Services* window displays.
6. Right-click *Apache Service* and select **Restart**. The Apache Service will restart.



Integrating x360Sync with Microsoft 365 (Private Cloud)

If your organization has access to a commercial Microsoft 365 subscription, you can integrate x360Sync with Microsoft 365 apps, allowing users to edit files from within the web portal.

To configure this feature, SaaS partners can simply turn on the Microsoft 365 policy in the administrative web portal; however, if you are a Private Cloud partner, you must also request access to the Office Cloud Storage Partner Program so that you can deploy your own Microsoft 365 integration.

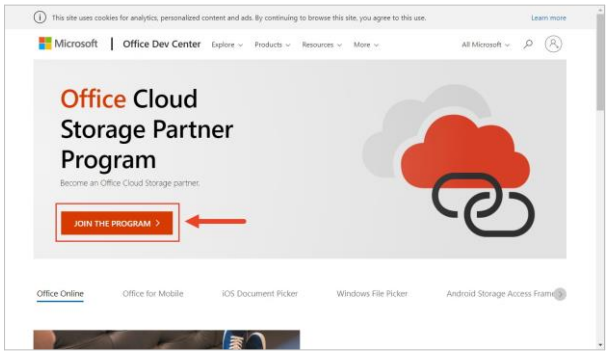
NOTE

This process can take a month or more to complete. Please plan accordingly.

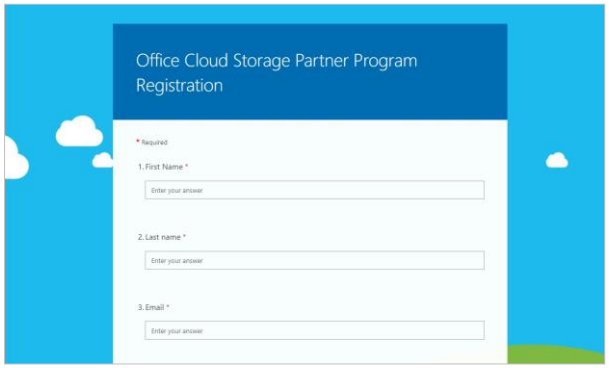
Step 1: Request Access to the Microsoft Cloud Storage Partner Program

As a first step, you need to request access to the Microsoft Cloud Storage Partner Program.

1. Navigate to the Office Cloud Storage Partner Program site and click the **Join the Program** button.



2. Complete the registration form and click the **Submit** button when you are finished.This form will initiate the approval process. The approval process can take a week or more to complete.



3. When you are approved for the program, Microsoft will contact you and provide access to the following resources:
   a. WOPI Yammer group—the WOPI Yammer group is the best way to submit requests, questions, or problems related to your Office Cloud Storage Partner Program membership.
   b. Web Integration Documentation—this WebHelp file outlines integration information and instructions.
   c. Shipping Information—this section of the WebHelp file provides instructions for validating and launching your completed web integration.

Step 2: Use the WOPI Protocol to Integrate Microsoft 365 with your Private Cloud Environment

After you are approved as an Office Cloud Storage Partner, you can use the WOPI protocol to integrate Microsoft 365 with your Private Cloud environment. This integration is already available in the x360Sync installation folder. You simply need to enable this feature through the configuration file (config.py):

1. Open the config.py file.
2. Update the following settings: *WOPI_ENABLED = True WOPI_TESTING = True*

Step 3: Validate your Integration

Before deploying to production, Microsoft must validate your integration package.

NOTE

Note: This process can take two weeks or longer. Before starting the launch process, please ensure that you have reviewed all requirements, and that you are ready to provide test accounts and videos.

To validate your integration:

1. Before you begin the validation process, you must set up a test domain for Microsoft validation through Yammer. You can view an example Yammer request in the Yammer group.
2. To prepare for the validation process, you have access to a WOPI Validation application that executes a test suite against a host's WOPI implementation. The test suite verifies semantics for all the WOPI operations.
3. Create test accounts and videos that will be used by Microsoft for validation during the release process. For a complete list of requirements, please reference Microsoft's Web Integration Documentation.
4. When you are ready, request Trello access through Yammer. You can view an example Yammer request for reference.
5. When your request has been received, Microsoft will provide a private Trello board to track issues and promote communication between your team and Microsoft. Follow the provided Trello release guide (this will include setting up and providing an M365-specific subdomain for use by the WOPI protocol).

Step 4: Deploy to Production

When Microsoft has signed off on your integration, you can begin to roll out to your users.

NOTE

Microsoft might request that you roll out over a period of several days to ensure you do not overload Office for the web or your WOPI servers.

How to Configure an SSL Certificate (Private Cloud)

Before desktop clients can connect and sync data, the x360Sync application server must be configured with a valid SSL certificate. This SSL certificate is also required to support WebDAV connections.

This article will review the following SSL configuration steps in detail:

- Chain together your *yourbundle.crt* file and your *yourdomainname.crt* file.
- Modify your *config.ini* file to point to the new *combinedbundle.crt* file and the copied *yourdomainname.key* file.

To chain together your *yourbundle.crt* file and your *yourdomainname.crt* file:

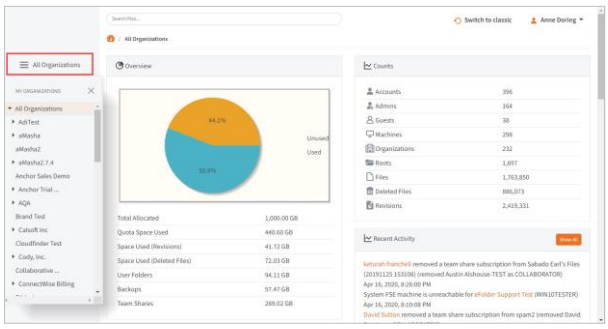
1. *Copy* (do not move) the following three files from your Apache folder (for example, C:\Apache24\conf\ssl) and *paste* them into the x360Sync *conf* directory (for example, *C:\x360Sync Server\conf*).
   - *yourdomainname.crt* file
   - *yourbundle.crt*
   - *yourdomainname.key* file
2. Open the newly copied *yourname.crt* file, highlight the entire contents of the file, and copy the selected content.
3. Open the newly copied *yourbundle.crt* file and place your mouse cursor at the beginning of the file (before the first character). Paste the contents of the copied *yourdomainname.crt* file into this location. You will now have a single file that combines the content of the *yourdomainname.crt* file and the *yourbundle.crt* file.
4. Save the modified *yourbundle.crt* file as *combinedbundle.crt*, or another similar name.

To modify your config.ini file:

1. Open the *config.ini* file, which resides in the x360Sync *conf* director (for example, C:\x360Sync Server\conf\config.ini).
2. Under the *[server]* section, change the following values to point to your modified *combinedbundle.crt* file and the copied *yourdomainname.key* file. For example:
   - *ssl_crt = "C:/x360Sync Server/conf/combinedbundle.crt"*
   - *ssl_key = "C:/x360Sync Server/conf/yourdomainname.key"*
3. Save the *config.ini* file and restart your x360Sync Server Service.

Creating and Configuring Organizations

In the administrative web portal, you can use the *Organization* navigation menu to create and manage organizations and suborganizations.



Organizations

All of your organizations and suborganizations will be organized in a hierarchy within the *Organization* navigation menu, allowing for a scalable environment that can grow and change according to your needs.

Master Organization

The master organization—which is system generated—will display at the top-level of the hierarchy, and all other organizations and suborganizations will sit below the master organization. The name of the master organization will be the company name that you used when first registering as a partner. For private cloud partners, the master organization will be titled, *All Organizations*.

TIP
This master organization should remain empty; except for a few trusted administrators, users should not be given access to the master organization, and it should never be configured for internal or customer use.

Master organizations should remain unpopulated for the following two reasons:

- Organization administrators have the ability to view content and user account information within the organization to which they have been assigned. Additionally, unless Privacy Mode has been enabled, they also have the ability to view this information in lower-level organizations. To mitigate the chance of exposing

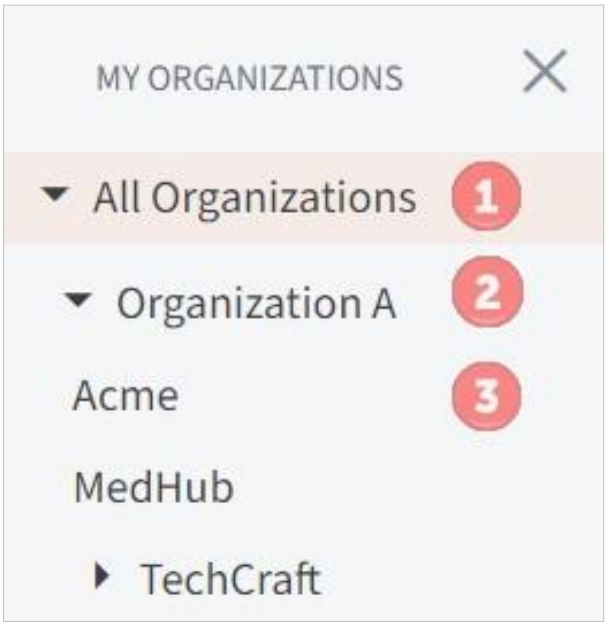
sensitive customer data to unauthorized individuals, you should only create organization administrator users within the organization to which they need access.

- The master organization's Dashboard provides a totaled overview of all organizationdata usage, activity, and so forth. If the master organization is actively used as an organization, there is no way to view the actual usage for this organization apart from suborganizations' usage.

Structuring Organizations

Instead of populating the master organization with user accounts and data, you should instead create organizations and suborganizations under the Master Organization.

1. Master Organization—each new system is populated with a master organization, which displays at the top-level of the hierarchy. The name of your master organization is based on your registration settings. The master organization should remain empty, and can be used to see an overall view of all of your organizations. Additionally, it is important to only add a minimal number of administrator accounts to this top level, as accounts added to this level will have access rights to every organization in the system.
2. A Parent Organization—you can create organizations for each of your customers, or for your own internal use. Optionally, you can assign organization administrators to these specific organizations. These organization administrators only have privileges to administer the organization to which they have been assigned.
3. A Suborganization—you can optionally create lower-level organizations that sit under the parent organization.



Suborganizations

By default, suborganizations inherit many features and settings from parent organizations, but also allow you to configure different settings if needed.

For example, if you want to turn on Privacy Mode for one or two users (for example, a CEO), create a suborganization, add this user, and then turn on Privacy Mode at the suborganization level.

Or, if you want to restrict storage quota for a Team Share, create a suborganization for this Team Share, and configure storage quota policies accordingly.

Organization Policies and Settings

When a new organization is created, you will use the *Settings* tab to configure settings for the organization, including:

- General information for an organization, including the name, URL, and so forth
- Policies, which control the way in which an organization manages data, users, filesand folders, API tokens, bandwidth, and other features
- Email settings, which allow you to specify an email server used for distributingemails

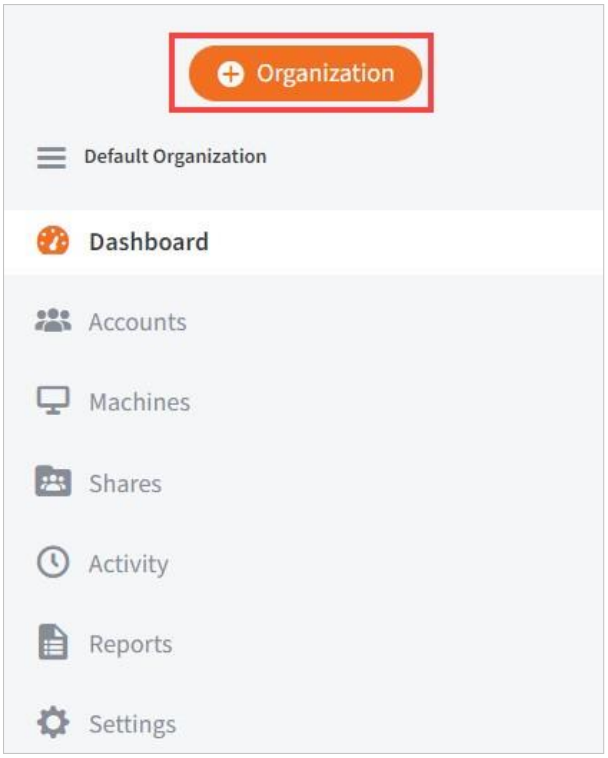
- Authentication source, which allows you to import users from Active Directory orother related systems
- Integration with a PSA system (if your organization uses a PSA system), to help youbetter manage alerts and notifications for individual organizations
- Custom branding, to allow you to define logos and colors used within the system
- Privacy Mode option, which allows you to limit your view of lower-level organization-al data

How to Create a New Organization

You can create organizations and suborganizations for each of your customers. You can also create an organization for internal use.

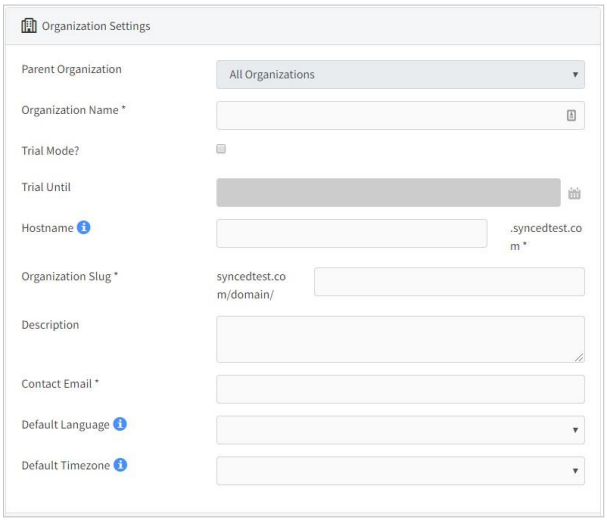
To create an organization:

1. In the *Organization* navigation menu, select the organization under which you want to create the new organization. For example, if you want to create a new organization under the master organization, select the master organization. The selected organization displays.
2. Click the **Organization** button in the *Organization* navigation menu.



The *Organization Settings* page displays.

3. In the *Organization Settings* page, enter information into the *Create an Organization* section, including:
    a. In the read-only *Parent Organization* field, view the **name of the higher-level organization**. If you want to change where your new organization will be created within your organization hierarchy, use the *Organization* navigation menu to select the parent organization. For example, if you want to create an organization under the master organization, select the name of your master organization.
    b. In the *Organization Name* field, enter a descriptive **title** for the organization.
    c. Select the **Trial Mode** checkbox if the organization should be created as a trial for a customer. Trials expire after a specified number of days.
    d. In the *Trial Until* field, select the **date** on which the trial should expire for the customer, if applicable. If you select a date in the past, the trial to expire immediately, and lock out users.
    e. In the *Hostname* field, enter a unique **URL** that will be used when linking to the organization. Links to resources and shares will be prepended with this hostname (for example, *customer*.syncedtool.com). The *Hostname* field value can be edited after you create an organization.
    f. In the *Organization Slug* field, enter a **unique identifier**, which will be used to link to your organization (for example, customer.syncedtool.com/*customerorganization*). The *Organization Slug* field value *cannot* be edited after you create an organization.
    g. In the *Description* field, provide a **description** of the organization that can be used to organize and identify the organization.
    h. In the *Contact Email* field, enter the **email address** that will be used as the main contact for the organization.
    i. In the *Default Language* field, select the preferred **site language** for the organization, which controls the language settings displayed in the web portal and mobile apps, as well as number formatting. Leave this field blank to use the default language set for the system.
    j. In the *Default Timezone* field, select the preferred **timezone** for the organization, which affects dates and times displayed across the system. Leave this field blank to use the default timezone for the system.



4. In the *Organization Policies* section of the page, configure policies for this new organization, including:
   a. In the *Space Quota* field, set the **space limit** for the organization. Space quota values must be greater than 0 and less than 10000000. As a best practice, ensure that this limit is enough to account for personal files and folders, Team Shares, backups, deleted files and folders, revisions, and so forth. The sync process will stop if this limit is reached. Additionally, you might consider configuring an alert so that you are notified when the organization is reaching its set limit. For more information, please reference the How to Create Activity Alerts section of this guide.
   b. In the *Parent is Using* area, view the amount of space used by the parent organization, if applicable. This number will help you understand how much data is available for this new organization.
   c. In the *Max File Size* field, set the **maximum size of individual files** that can be uploaded into the system through desktop clients, mobile apps, and the web portal. By default, this is set to 300MB.
   d. In the *Excluded Extensions* field, enter **fileextensions** that you want added to the list of default excluded extensions, making sure that each extension is separated by a comma. Files with excluded extensions cannot be synced by the system. If an excluded extension is upload through the web portal, end users will receive an error messaging notifying them that their file is on the exclusion list.
   e. In the *Max Number of Users* field, enter a **user limit** that will be allowed for the organization. Alternatively, enter **0**, which represents an unlimited

number of users. Suborganizations cannot exceed the maximum number of users set for the parent organization.

f. Select the **Allow Creation of Suborganizations** checkbox to allow child organizations to be created under the organization. A suborganization will inherit this policy from its parent.

g. In the *Max Number of Suborganizations* field, set the **maximum number of child organizations** allowed under the higher-level organization. Alternatively, leave the field blank to allow an unlimited number of suborganizations. A suborganization will inherit this policy from its parent.

h. Select the **Enable Service Plans** checkbox to allow the creation of service plans. A suborganization will inherit this policy from its parent.

i. Select the **Enable Branding** checkbox to allow custom styles and logos for the organization. A suborganization will inherit this policy from its parent.

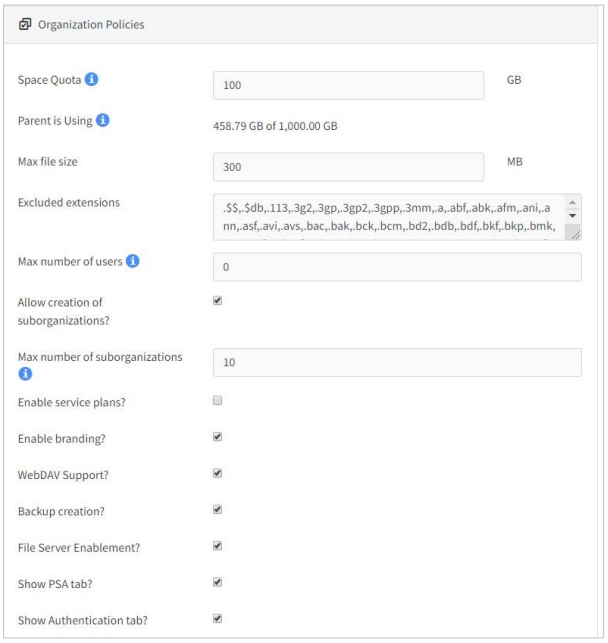
j. Select the **WebDAV Support** checkbox to support WebDAV connections, which is another way for end users to view and edit files—both personal and through Team Shares—located in the cloud. WebDAV is useful when you do not want local copies of large files being stored on external machines. For more information, please reference the End User Guide. A suborganization will inherit this policy from its parent.

k. Select the **Backup Creation** checkbox to allow administrators to create backups from the administrative web portal. A suborganization will inherit this policy from its parent.

l. Select the **File Server Enablement** checkbox to allow machines to be cloudenabled. With File Server Enablement, you can keep the existing file structure on the server while allowing remote access to files and folders.

m. Select the **Show PSA Tab** checkbox to give access to the *PSA* tab in the administrative web portal, which is located under the *Settings* tab. In the *PSA* tab, professional services automated systems—such as ConnectWise and Autotask—can be integrated with x360Sync. A suborganization will inherit this policy from its parent.

n. Select the **Show Authentication Tab** checkbox to give access to the *Authentication* tab in the administrative web portal, which is located under the *Settings* tab. In the *Authentication* tab, authentication sources can be configured for the organization. A suborganization will inherit this policy from its parent.



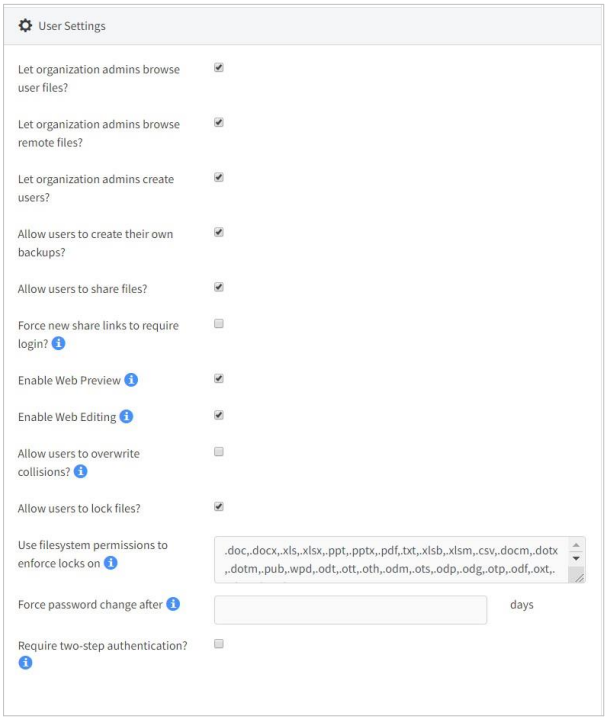
5. In the *User Settings* section of the page, you can define the user rights granted to administrators and standard accounts, including:
   a. Select the **Let Organization Admins Browse User Files** checkbox to allow organization administrators to view data in files, folders, shares, and backups, which is required to restore end user files. A suborganization will inherit this policy from its parent.
   b. Select the **Let Organization Admins Browse Remote Files** checkbox to allow organization administrators to browse machines. Browsing machines is required when setting up backups or File Server Enablement. A suborganization will inherit this policy from its parent.
   c. Select the **Let Organization Admins Create Users** checkbox to allow organization administrators to generate new user accounts in the system. A suborganization will inherit this policy from its parent.
   d. Select the **Allow Users to Create Their Own Backups** checkbox to allow end users to configure backups from the web portal or from their local machine. A suborganization will inherit this policy from its parent.
   e. Select the **Allow Users to Share Files** checkbox to allow end users to send shares. A suborganization will inherit this policy from its parent.
   f. Select the **Force New Share Links to Require Login** checkbox to disable public shares, and require the use of secure shares for all members of the organization on all devices. This policy also applies to shared items sent through the Outlook add-in. Secure shares require a username and a

password before the content can be accessed. If a secure share is sent to some-
one outside of the user's organization, a guest account will automatically be created for the recipient. This policy is only available if the *Allow Users to Share Files* policy is enabled. A suborganization will inherit this policy from its parent.

g. Select the **Enable Web Preview** checkbox to enable the Web Preview tool for end users. This feature allows users to preview content in the web portal and on mobile devices.
h. Select the **Enable Web Editing** checkbox to enable the Collaborative Web Editor feature for end users. This feature allows users to edit content collaboratively, in real time, from the web portal.
i. If the organization has access to a commercial Microsoft 365 subscription, use the *Microsoft 365 Integration* section to configure integration preferences. Click the **Enabled for Editing** radio button to allow authenticated users to read and edit files using their Microsoft apps. Click the **Enabled for Readonly** radio button to allow authenticated users to read (but not edit) files using their Microsoft apps.
j. Select the **Allow Users to Overwrite Collisions** checkbox to allow end users to resolve collisions by syncing their own local copy as the latest server revision.
k. Select the **Allow Users to Lock Files** checkbox to allow users to lock and unlock files. If this policy is enabled at the master organization level, the policy will appear for each organization. Otherwise, this policy is set per organization.
l. The *Use Filesystem Permissions to Enforce Locks On* field allows you to specify extensions on which you would like the desktop client to enforce locks through filesystem permissions (also called hard locks). This field is important for File Server Enablement environments where mapped drive users must be notified by the filesystem when a file is in use. When a lock is placed, the desktop client will change the NTFS permissions on Windows, or HFS Plus permissions on Mac, in order to prevent changes by other users. These permissions still allow administrators to modify files, but they prevent standard end users from doing so, and makes for a much stronger lock. This field can only be edited if you previously selected the *Allow Users to Lock Files* checkbox.

m. In the **Force Password Change After** field, enter the number of days that end users can keep their passwords. End users with expired passwords will be required to change their passwords when logging into the web portal.

n. Select the **Require Two-Step Authentication** checkbox to add an extra layer of security to user accounts. With Two-Step Authentication, end users will be sent an authentication code through a mobile authenticator app, text message, or email; they must then enter their authentication code, along with their username and password, before they can access the web portal or register a desktop client, the Outlook add-in, or a mobile device. They will also be required to set up a passcode for any of their registered mobile devices. End users must configure their own authentication settings. If you turn *off* this setting for an organization, end users must individually disable their own configuration settings. For more information, please reference the End User Guide.



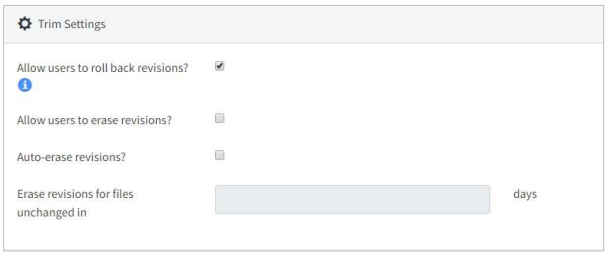
6. In the *File Trim Settings* section of the page, you can define how the organization retains file revisions (file versions), including:

a. Select the **Allow Users to Roll Back Revisions** checkbox to give end users access to the Revision Rollback feature. If this policy is turned off, administrators will still retain the ability to utilize this feature for end user support.

b. Select the **Allow Users to Erase Revisions** checkbox to allow end users to delete previous revisions of files within the system.

c. Select the **Auto-Erase Revisions** checkbox to automatically delete previous revisions of files within the system. If this option is selected, you will need to enter the number of days that revisions should be stored. By default, the system retains all revisions.

d. In the *Erase Revisions for Files Unchanged In* field, enter the **number of days** that revisions should be stored for unchanged files, if you previously selected the option to auto-erase revisions. By default, the system retains all revisions.

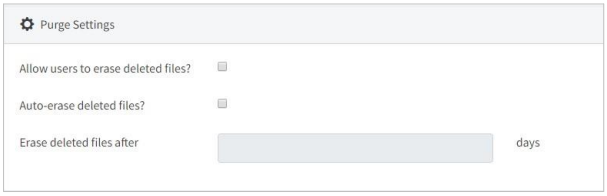


7. In the *File Purge Settings* section of the page, you can define how the organization retains deleted files, including:

a. Select the **Allow Users to Erase Deleted Files** checkbox to allow end users to permanently remove files that have been deleted from the system.

b. Select the **Auto-Erase Deleted Files** checkbox to automatically remove deleted files from the system after a specified number of days. If you select this option, you will need to specify the number of days that deleted files should be stored before being erased. By default, the system retains all deleted files.

c. In the *Erase Deleted Files After* field, enter the **number of days** the deleted files should be stored before being removed, if you previously selected the option to auto-erase deleted files. By default, the system retains all deleted files.



8. In the *Backup Settings* section of the page, you can define how the organization retains files and revisions in backups, including:

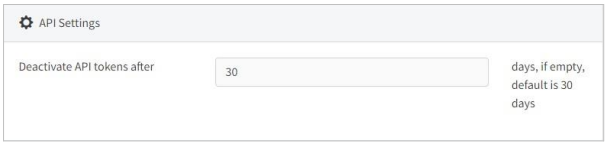
a. Select the **Auto-Erase Revisions** checkbox to automatically delete previous versions of files within backups. If this option is selected, you will need to enter the number of days that revisions should be stored.
b. In the *Erase Revisions for Files Unchanged In* field, enter the **number of days** the that revisions should be stored for unchanged files in backups, if you previously selected the option to auto-erase revisions.
c. Select the **Auto-Erase Deleted Files** checkbox to automatically remove deleted files from backups after a specified number of days. If you select this option, you will need to specify the number of days that deleted files should be stored before being erased.
d. In the *Erase Deleted Files After* field, enter the **number of days** the deleted files should be stored before being removed from a backup, if you previously selected the option to auto-erase deleted files.

9. In the *API Token Settings* section, use the *Deactivate API Tokens After* field to enter the **number of hours** that an API token should be set as active. By default, API tokens expire after 30 days.

Note: API tokens expire immediately after initial use for certain sessions initiated from the desktop client, including:

- Launching the web portal
- Viewing an item in the web portal
- Backing up a folder
- Sharing a link
- Viewing revision

In these instances, API tokens will expire immediately after they are used, allowing desktop clients to *securely* connect to the web portal without requiring a username and password. API tokens for other sessions, including mobile and Outlook connections, will expire according to your API policy settings.



10. In the *Bandwidth Settings* section of the page, configure bandwidth settings. For example:
    a. Select the **Throttle Bandwidth** checkbox to help regulate traffic and minimize bandwidth congestion. Restricting bandwidth will mitigate the impact that large files and shares might have on business-critical applications. You can also restrict bandwidth on individual machines.
    b. Select the **Enable Throttle Exception** checkbox to configure times when bandwidth throttling is not enabled. If you select this option, you will be prompted to specify a time period during which exceptions will be scheduled.

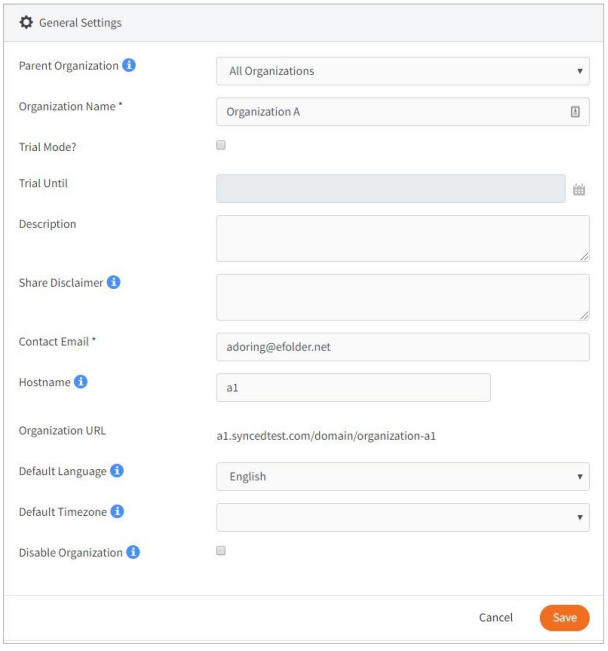
11. Click the **Save** button when you are finished. Your organization is now created.

How to Update Settings and Policies for an Organization

After an organization is created, you have the option of editing general settings and policies for the organization.

To edit general settings for an organization:

1. While in the appropriate organization, click the **Settings** tab. The *Organization Settings* page displays, showing the *General* tab.



2. In the *General Settings* section of the page, you will see general organization settings that were configured when the organization was created. Optionally, you can edit these settings. Click the **Save** button if you make any changes.
3. Next, click the **Policies** tab to edit the same policies that were configured when you first created your organization. Click the **Save** button if you make any changes.

How to Manage Inherited Policies in Suborganizations

When you create a suborganization, certain policies will be inherited from its parent. Inherited policies can only be managed by higher-level organization administrators. If you assign an organization administrator to a specific suborganization, he or she will *not* see inherited policies in the *Policies* page, regardless of whether this policy is turned on or off. The purpose of inherited policies is to allow higher-level organization administrators to appropriately manage organizations while still enabling lower-level organization administrators to support their assigned suborganizations.

For example, when you create a *new* suborganization under a parent organization:

- If an inherited policy is turned *on* in the parent organization, you will be given the option of turning on or off this inherited policy when creating a new suborganization.
- If an inherited policy is turned *off* in the parent organization, you will *not* be given the option of configuring this policy when creating a new suborganization. This policy must first be turned on in the parent organization.

For *existing* suborganizations:

- If you turn *off* an inherited policy in a parent organization, this policy will also be turned off in any existing suborganizations. Only you or another higher-level organization administrator can turn on this policy in the suborganization.
- If you turn *on* an inherited policy in a parent organization, any existing suborganizations will not be affected. The policy will remain turned off in any of these suborganizations, unless specifically changed within the suborganization.

NOTE

Policies that are marked as inherited can only be managed by higherlevel organization administrators. If you assign an organization administrator to a specific suborganization, he or she will not see inherited policies in the *Policies* page, regardless of whether these policies are turned on or off.

How to Specify an Email Server

After you create an organization and configure general settings and policy settings, you can configure email server settings for outbound emails. The email server is used to send account invitation emails, reset password emails, alerts, and share emails. By default, the x360Sync email service is configured for use immediately after an organization is created.

The system currently supports a multitude of email servers that you can configure for use with the system, including Gmail, Yahoo, and Outlook.

NOTE

The default email server is offered as a failover server. it is recommended that you implement your own email server to improve email bounce rates.

NOTE

After you set up an email server, you might consider creating an alert so that you are aware of changes to these email settings. For information on how to create alerts, please reference the *How to Create Activity Alerts* section of the Guide.

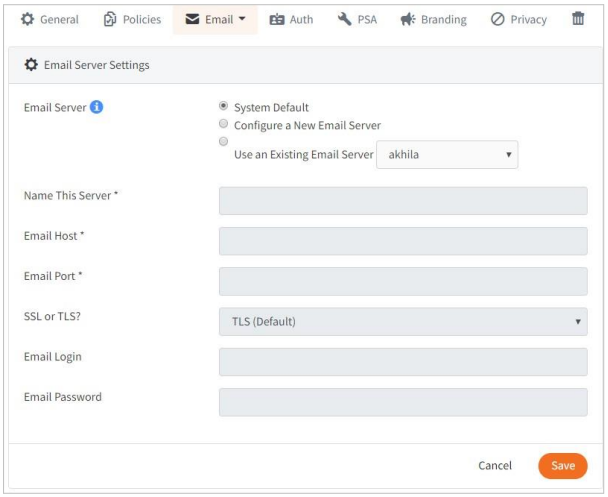
Email Errors

The administrative web portal exposes email errors when an email fails to send. You can keep track of these email errors to help troubleshoot issues. For more information, please reference instructions below.

How To Specify an Email Server

To specify an email server:

1. While in the appropriate organization, click the **Settings** tab. The *Organization Settings* page displays, showing the *General* tab.
2. Point to the *Email* tab and select **Servers**. The *Email Server Settings* section displays.



3. In the *Email Server Settings* section, set email server settings specific to your selected email server. For example:
   a. In the *Email Server* area, click the **Configure a New Email Server** radio button.
   b. In the *Name This Server* field, provide a **title** for the server.
   c. In the *Email Host* field, enter the name of the **SMTP server** (for example, smtp.gmail.com).
   d. In the *Email Port* field, enter the **email port** of the SMTP server (for example, 465).
   e. In the *SSL or TLS* field, select whether you would like to use the **TLS** (Transport Layer Security) or **SSL** (Secure Sockets Layer) protocol for data encryption. By default, TLS is selected. Some email servers may require that you use the SSL protocol for data encryption.

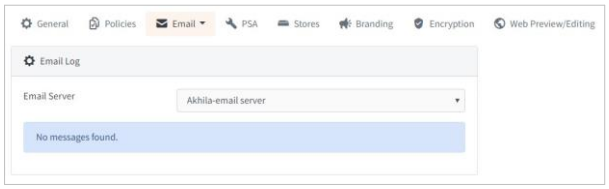
f. In the *Email Login* field, enter **login** information (for example, example@gmail.com).
g. In the *Email Password* field, enter the **password** for the email login.
h. In the *Email From Name* field, enter the **display name** from which you want emails to be sent (for example, Administrator).
i. In the *Email From Address* field, enter the **display email address** from which you want emails to be sent.

4. When you are finished, click the **Save** button.

How To Troubleshoot Email Errors

To ensure that your outbound emails are being sent, you can use the Email Log to troubleshoot errors. To review email errors:

1. While in the appropriate organization, point to the *Email* tab and select **Email Log**. The *Email Log* displays.



2. In the *Email Server* drop-down menu, select the **name of the email server** you want to review. The page will expand to display any errors connected with that email server.
3. Use the *Date* column to help you understand when these errors occurred. You can then review the *Error* column to view specific information related to the email error. Use these logs to help troubleshoot email server issues.

How to Set Custom Branding

You can configure branding options that conform to your company's—or your clients'— branding strategy. For example, you can configure the system to take on a custom

- Logo,
- Icon,
- Splash screen,
- Company name,

- Company URL,
- Program name,
- Folder name, and
- Terms of service.

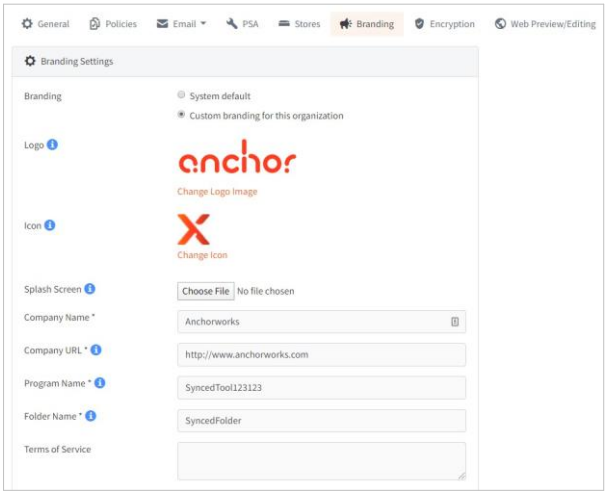
These branding settings will affect the look of the web portal, mobile apps, and the desktop client. Branding even influences the layout of informational resources like the Daily Digest email, which inherits the branded logo. When you configure custom branding for an organization, the settings will be inherited by suborganizations.

NOTE

All custom branding should be configured before deploying the desktop client to end users. Branding is inherited when desktop clients are installed; changes made to the branding will not be inherited by desktop clients that have already been deployed. If a change in branding occurs after desktop clients have been deployed, these desktop clients will need to be reinstalled. This can be done through a batch script. For more information on batch scripts, please reference the Knowledgebase.

To configure custom branding:

1. In the appropriate organization, click the **Settings** tab. The *Settings* page displays.
2. In the *Settings* page, click the **Branding** tab. The *Branding Settings* section displays.



3. In the *Branding Settings* section, click the **Custom Branding for this Organization** radio button. The *Branding Settings* section expands to display custom branding options.
   a. In the *Logo* area, click the **Choose File** button to browse your computer for a custom logo, which will be used as your organization's image file on the web. Images cannot be larger than 200px by 50px, and it is recommended that images be in PNG, transparent format.

   b. In the *Icon* area, click the **Choose File** button to browse your computer for a custom icon, which will set the desktop, explorer, and system tray icon. The icon must be in .ico format.

   c. In the *Splash Screen* area, click the **Choose File** button to browse your computer for a splash screen image, which will display to users who log in on mobile devices.

d. In the *Company Name* field, enter the **name of your organization**, which will be featured along with your organization's logo.

e. In the *Company URL* field, enter the **web address** of your company.

f. In the *Program Name* field, enter a **name** to replace the default Synced Tool program name. It will be used in conjunction with desktop icons on local machines.

g. In the *Folder Name* field, enter a **folder name** to replace the Synced Folder branding.

h. In the *Terms of Service* field, enter your organization's specific **terms of service** text.

4. When you are finished, click the **Save** button. You can now allow end users to download and install the newly branded desktop clients and apps.

How to Customize the x360Sync Web UI Stylesheet (Private Cloud)

In the *Branding* page of the administrative web portal, you can define a custom logo, icon, splash screen, program name, and more.

In addition to these options, private cloud administrators can apply a custom CSS stylesheet to override the default x360Sync stylesheet. This option allows you to control branding at the granular level, and fully customize the user experience for end users.

x360Sync Stylesheets

The x360Sync Web UI references the *main.css* stylesheet as the default stylesheet, and is accessible on the x360Sync server. The *main.css* stylesheet controls styles at the global level.

To override styles defined in *main.css*, you can create a new stylesheet, titled *styles.css*, and place it in the following directory:

[target drive]:\x360Sync Server\web\greensnake\static\themes\default\css\

Content stored in this directory will not be overwritten during x360Sync revision upgrades.

NOTE

To prevent rendering errors, do not attempt to edit the *main.css* stylesheet.

How to Override the Default x360Sync Stylesheet

1. In the x360Sync web portal, use a browser inspector to find HTML elements that you want to customize. For example:

2. Create a new file titled, *styles.css*.
3. For each HTML element that you want to customize, copy the associated CSS rule set from the *main.css* stylesheet and paste it into the new *styles.css* stylesheet. Update styles as required.
4. Save *styles.css* when you are finished.
5. Move styles.css into the following directory:

   [target drive]:\x360Sync Server\web\greensnake\static\themes\default\css

Your custom styles will now be reflected in the Web UI, and will remain intact with each revision upgrade.

How to Troubleshoot

If you notice display issues after editing the custom *styles.css* file, it is recommended that you disable the *styles.css* file.

1. On the x360Sync server, navigate to:

   [target drive]:\x360Sync Server\web\greensnake\static\themes\default\css
2. Rename *styles.css* (for example, *disabled_styles.css*).
3. Restart the Apache service. x360Sync will no longer reference *styles.css*, and will instead display all styles as defined by the *main.css* file.

How to Set Up File Server Enablement

File Server Enablement allows you to cloud-enable any folder on a machine and map it to a Team Share or a user account. In addition to local paths, you can specify a network share, a UNC path, or a NAS device, as a source for File Server Enablement.

This feature replaces the need for mapped drives (network drives), so that end users no longer need to be on-site or require the use of a VPN connection to access files and folders. With File Server Enablement, you can maintain an existing file structure while providing remote access to its contents. As an added benefit, File Server Enablement can provide a file-level backup of your file server.

When File Server Enablement is enabled for an organization, end users can access, read, and update content through the web or through their preferred device. By providing anytime, anywhere access to business assets, File Server Enablement can increase employee and organizational productivity.

Important Notes and Best Practices

NOTE

The system does not support the syncing of live databases. For more information, please reference the Knowledgebase.

TIP

When registering to a user account on a server, it is recommended that you create a service account. A service account should not be subscribed to Team Shares, should be set to use fixed space quota of .01GB, and should be configured using a predetermined naming system (such as First Name: File Server; Last Name: LDAP).

You might decide to create one service account in the master organization, and register all File Server Enablement and other server desktop clients to this one service account. Alternatively, you can create one service account for each organization. Both options will allow for the same functionality and meet established best practices.

TIP

If you are using File Server Enablement to map a network drive, it is recommended that you first run a throughput and IOPs test.

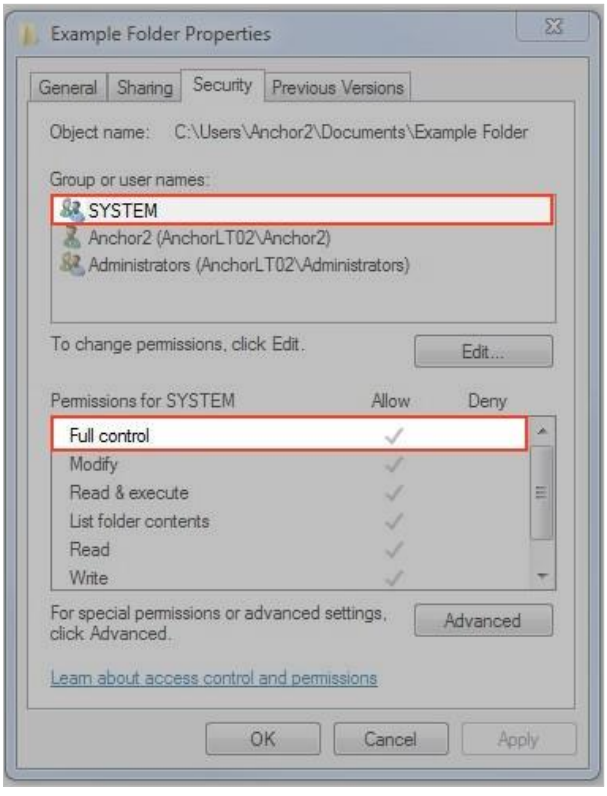
TIP

We recommend that you create an alert so that you are notified when a File Server Enablement machine is unreachable. This alert allows you to proactively monitor the state of a file server that is syncing to the cloud, ensuring that synced content is always available in its mapped location.

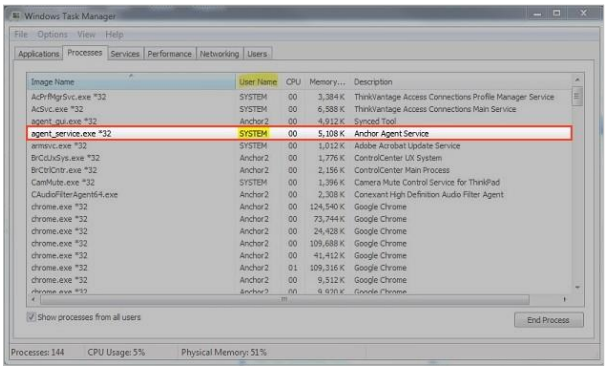
Instructions

To set up File Server Enablement:

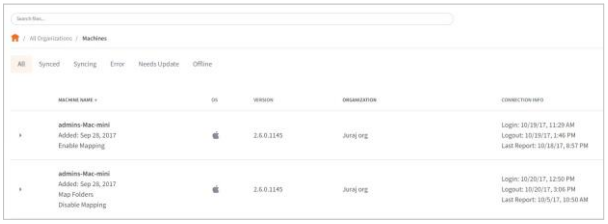
1. Log in to the server that you want to cloud-enable, and download and install the desktop client. For instructions on downloading and installing the desktop client, please reference the End User Guide.
   a. On the server, ensure that the SYSTEM user has full permissions to the folder and all of its subfolders and files.



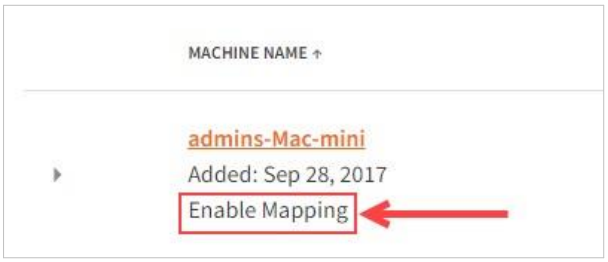
   b. Alternatively, if *agent_service.exe*32* is being run by a user name other than SYSTEM, ensure that *this* user has full permissions.



2. When the desktop client finishes the installation process, you will be asked to register the desktop client to a user account. When registering the desktop client to a user account on a server, it is recommended that you create a *service account*. A service account should not be subscribed to Team Shares, should be set to use fixed space quota of .01GB, and should be configured using a predetermined naming system (such as First Name: File Server; Last Name: LDAP).
3. Open a web browser and navigate to the administrative web portal. Log in to the administrative web portal.
4. In the administrative web portal, click the **Machines** tab. The *Machines* page displays, showing a list of all machines in the selected organization.



5. Find the File Server Enablement machine, and click the **Enable Mapping** link to set up File Server Enablement.

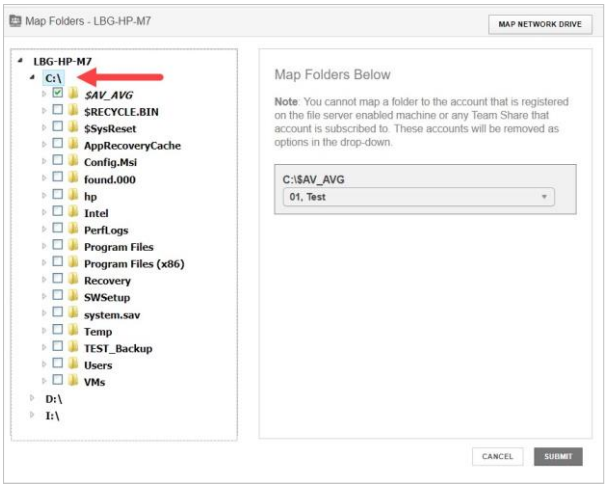


A message will display, indicating that the machine has been enabled as a file server. Additionally, a new *Map Folders* link will display, allowing you to map the machine to a Team Share or a user account.

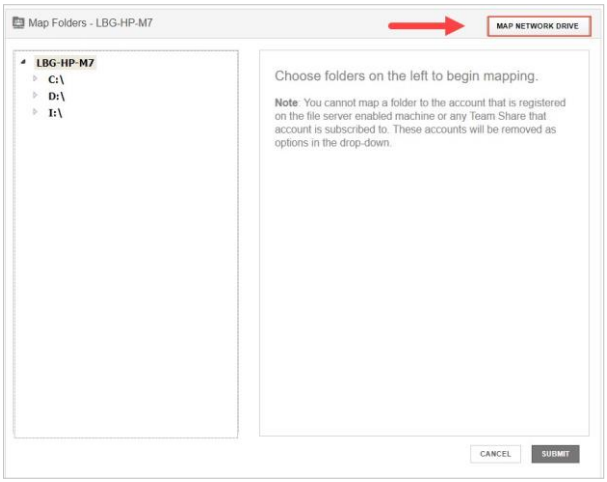
6. Click the **Map Folders** link. The *File Server Enablement* screen displays.

7. In the *File Server Enablement* screen, click to expand the machine name, and then select the folder or folders that you want to map.

   Please note that when selecting a parent folder, the mapping will include all of the parent's subfolders.



   a. Alternatively, to use a UNC path as a source for File Server Enablement, click to expand and highlight a machine name, and then click the **Map Network Drive** button.



      A *Map Network Drive* pop-up window displays.

   b. In the *Map Network Drive* pop-up window, enter information about the network drive.

      a. In the *Network Path* field, enter the UNC path.

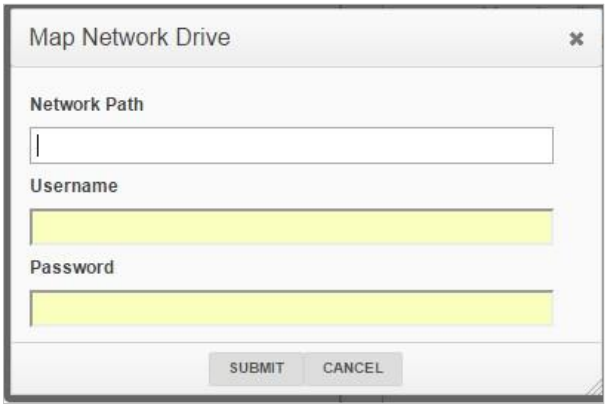
      b. In the *Username* field, enter the username of the user with access to the UNC path (*not* the username of the service account). If you encounter problems when entering credentials into the *Username* field, please try

various formats. For example, you might be able to authenticate using one of the following formats:

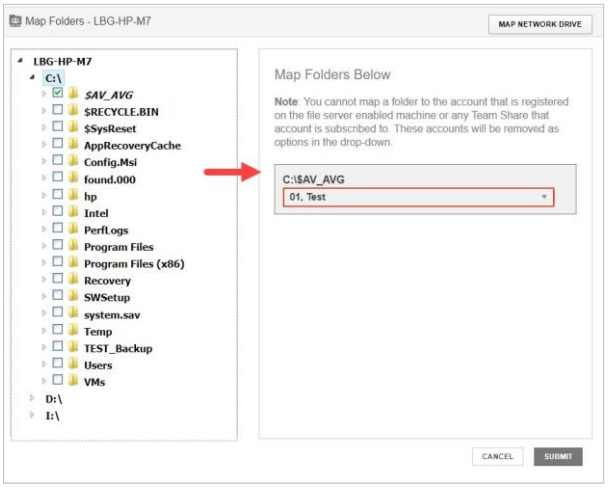
- Username
- Machine name\username
- Domain\username (if the UNC path is located on a domain server)

c. In the *Password* field, enter the password of the user with access to the UNC path.

d. Click the **Submit** button when you are finished.



8. After you select the items you want to map, use the *Map Folders Below* section of the screen to map the selected folder to a user or Team Share.

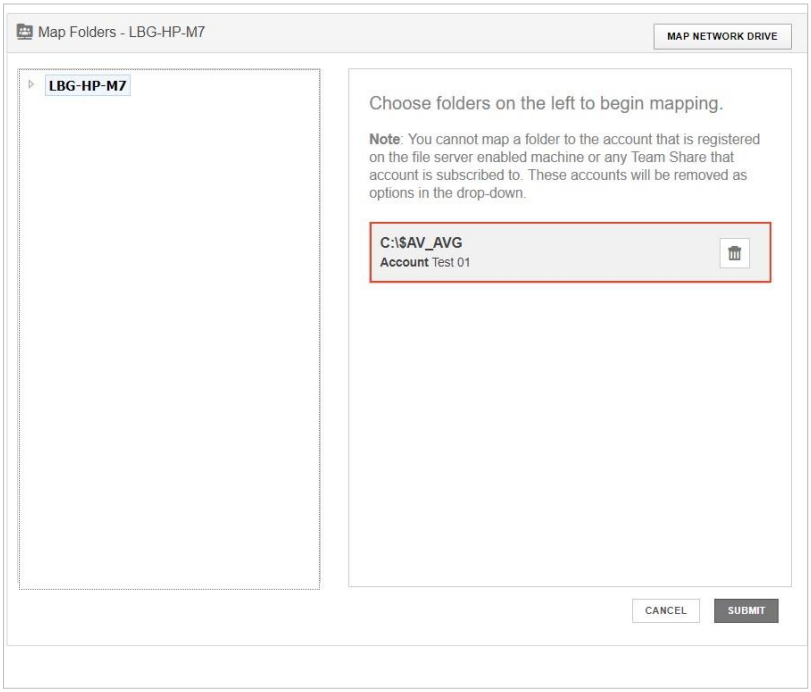


9. Click the **Submit** button when you are finished. If an update is made to a file or folder, this update will display in both locations.

You can also disable mapping between the file server and the Team Share or user account. When you do this, the already-mapped files and folders will remain in both locations, but will no longer remain linked. You might decide to disable mapping if you simply want to move or copy data to a Team Share or a user account.

To disable mapping:

1. In the *Machines* tab, find the already-mapped File Server Enablement machine and click the **Map Filers** link. The *File Server Enablement* screen displays.
2. Click the **Delete** button to remove the mapping.



The files will remain in both locations, but will no longer be linked.

How to Set Up Two-Step Authentication

Two-Step Authentication adds a second verification step when a user logs into the web portal, or when the user registers a desktop client, the Outlook add-in, or a mobile device. With Two-Step Authentication, end users will be sent an authentication code through an Authenticator Mobile App, text message, or email, depending on their own configuration settings. They must then enter their authentication code—along with their username and password—before they can access the system.

Two-Step Authentication applies to:

- The web portal—the user will be prompted to enter an authentication code whenlogging into the web portal.
- The desktop client—the user will be prompted to enter an authentication code whenregistering the desktop client.

- The Outlook add-in—the user will be prompted to enter an authentication codewhen registering the Outlook add-in, when opening a new Outlook session, or when changing credentials.
- A mobile device—the user will be prompted to enter an authentication code whenaccessing a mobile app for the first time. The user will also be asked to configure a passcode (also called a PIN if you are using an Android device) when accessing mobile apps at subsequent sessions. Configuring a passcode is required if TwoStep Authentication was configured as an organization policy; it is optional if TwoStep Authentication was configured as a user policy.

NOTE

End users need to configure Two-Step Authentication settings before installing the desktop client. End users will only be prompted to enter an authentication code if they have already configured their Two-Step Authentication preferences.

Configuring Two-Step Authentication

Two-Step Authentication can be configured in multiple ways.

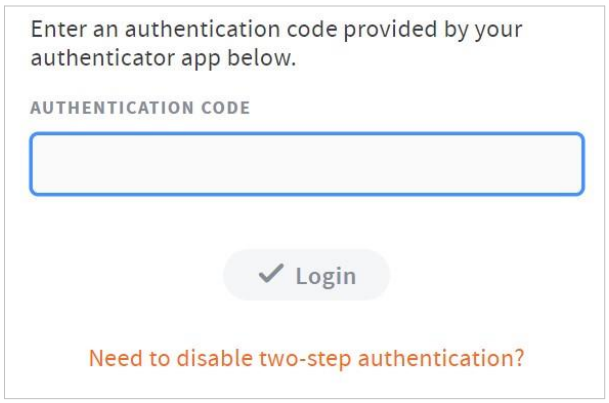
- End users can optionally configure their own Two-Step Authentication settings intheir *Account Settings* page. For more information, please reference the End User Guide.
- Administrators can turn on the Require Two-Step Authentication policy in the *Policies* section of the *Settings* tab. When this policy is enabled, end users will be prompted to configure their own Two-Step Authentication settings as soon as they log in to the web portal.

To turn on Two-Step Authentication for an organization:

1. Click the **Settings** tab. The *Settings* page displays.
2. In the *Settings* page, click the **Policies** tab. The *Policies* section displays.
3. In the *Policies* section, scroll down until you see the policy titled, Require TwoStep Authentication. Select the **Require Two-Step Authentication** checkbox.

4. Click the **Save** button when you are finished.

From an end user's perspective, when the Require Two-Step Authentication policy is enabled, he or she will be required to configure individual authentication settings when logging into the web portal. For more information, please reference the End User Guide.



How to Specify the *From* Email Address for System-Generated Emails

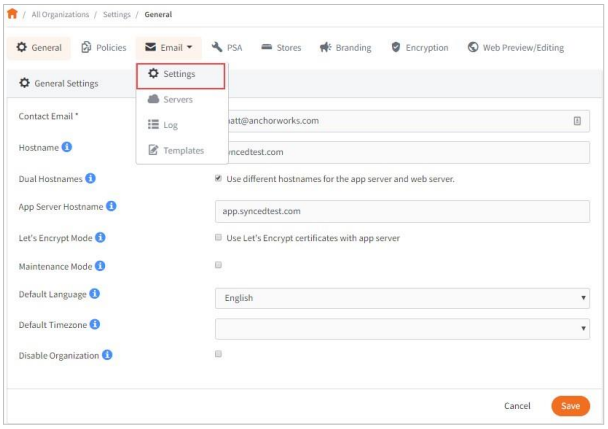
x360Sync delivers email notifications to communicate important information and activity. These emails can be user-generated or system-generated.

- User-generated emails—the *From* field of a user-generated email is populated with the name and email address of the user who initiated the action. A user-generated email communicates:
- Account, guest, and Group message emails
- Share and multiple share emails
- Team share invitation emails
- System-generated emails—administrators can customize the *From* field of all system-generated emails. A system-generated email communicates:
- Welcome emails
- Share download, upload, and expiration notifications
- New password and password reset emails
- Service Plan registration emails
- Daily Digest emails

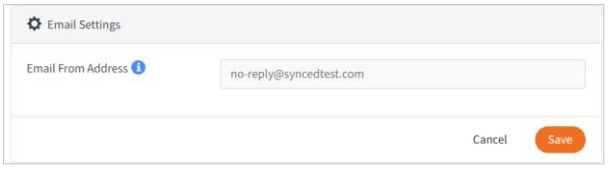
- Report emails
- Alert emails
- Two-Step Authentication code emails

To customize the *From* field in system-generated emails:

1. In the appropriate organization, click the **Settings** tab. The *Organization Settings* page displays.
2. Point to the *Email* drop-down button and select **Settings**.



The *Email Settings* page displays, showing the default *From* address.



3. In the *Email From Address* field, enter the **email address** that should display as the *From* address for all system-generated emails. All user-generated emails will still display the name and email address of the user who initiated the action.
4. Click the **Save** button when you are finished.

How to Create Email Templates

You can create email templates that are used when distributing emails related to new user accounts, new guest accounts, share emails, multiple share emails, and Team Share emails. You can customize the text of the email templates, and even use HTML to customize styles and add images.

Template Types

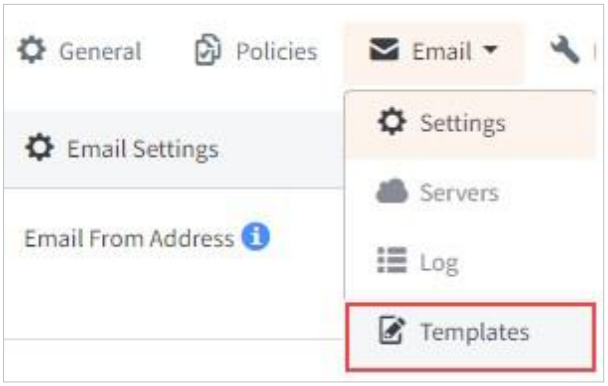
You can create email templates for the following email types:

- Welcome email—a welcome email is distributed to end users when they are firstadded to the system
- Guest welcome email—a guest welcome email is distributed to guest users whenthey are first added to the system
- Share email—a share email is distributed when an end user sends a share link to afile or folder
- Multiple share email—a multiple share email is distributed when an end user sendsmultiple share links to one recipient
- Team Share email—a Team Share email is distributed to end users when they areadded as subscribers to Team Shares

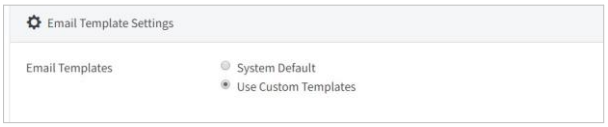
Defining Email Headers and Footers

As a first step, you can define the email header and footer for each of the available email templates:

1. In the appropriate organization, click the **Settings** tab. The *Settings* page displays.
2. In the *Settings* page, point to the *Email* tab and select **Templates**. The *Email Template Settings* section displays.



3. In the *Email Template Settings* section, click the **Use Custom Templates** radio button. The page expands to display a *Welcome Email* section, a *Guest Welcome Email* section, a *Share Email* section, a *Multiple Shares Email* section, and a *Team Share Email* section.



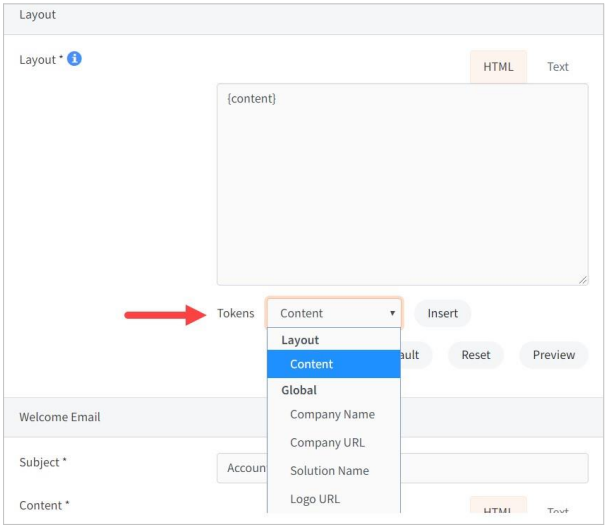
4. While still in the *Email Template Settings* section, you can optionally define the header and footer for all email templates. The *{content}* token represents the

body of the email, as defined by each individual email template. To insert additional token fields in the header (above) or the footer (below):

a. Place your cursor in the area in which you want the *token* to appear.

b. In the *Tokens* drop-down menu, select a **token** that will automatically populate based on specific user account information, or share context.

c. Click the **Insert** button. The *token* will appear in the email template.



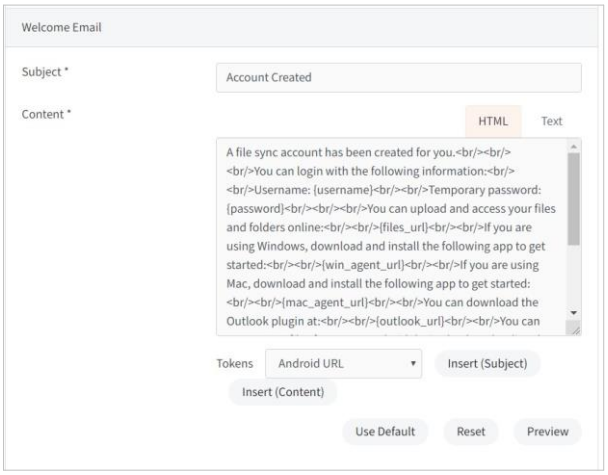
Defining Email Content

1. While still in the *Email Template Settings* page, find the template that you would like to customize and update the appropriate fields:
   a. In the *Subject* field, enter the **subject** that will display in the email subject heading.
   b. In the *Template* field, enter the **emailcontent** you want to include.
   c. While still in the *Template* field, insert **token** fields within the email content.
2. Click the **Save** button when you are finished.

Customizing HTML

You can also use HTML to customize the style of the templates and add images.

1. While still in the *Email Template Settings* page, find the template that you would like to customize.
2. In the *Template* field, insert HTML to fully customize the look of the email.



3. Optionally, click the **Preview** button to review your changes.
4. Click the **Close** button to close the preview screen, and then click the **Save** button to save your changes.

How to Integrate with a PSA System—Autotask

Autotask is a complete professional services automation (PSA) platform that allows companies to develop, sell, bill, and implement technology solutions. If your company uses Autotask, you can optionally integrate this platform with the system. Specifically, when you integrate with Autotask, you can map organizations in x360Sync to accounts within Autotask. Additionally, the system allows you to push system activities to a specific support queue within Autotask.

The general steps required to integrate Autotask with the system are:

- Create an API user in Autotask.
- Enter Autotask credentials in x360Sync.
- Configure alerts to be sent to Autotask.

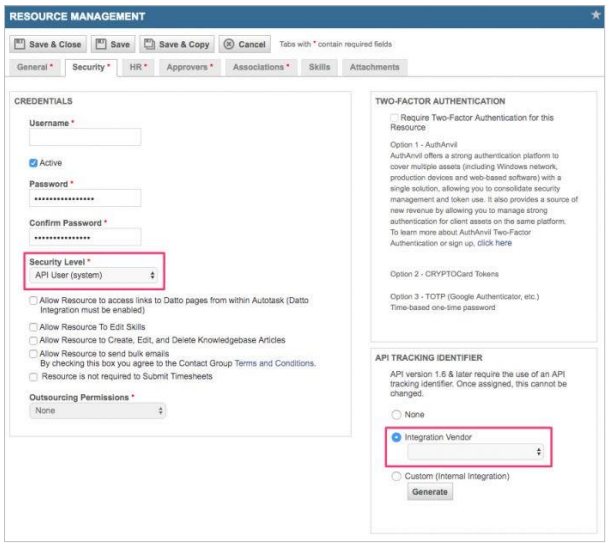
NOTE

You must have administrative access to Autotask in order to complete these integration steps.

Step 1: Create an API User in Autotask

When integrating Autotask with x360Sync, the administering Autotask resource account must be configured as an API user. You can either create a new resource account or update an existing resource account. In this example, we will create a new resource account.

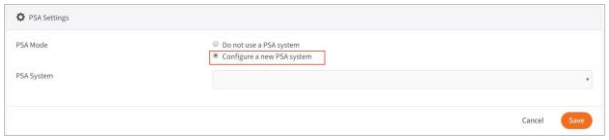
1. Hover your mouse over the *Autotask* icon to activate the main navigation menu.
2. Point to the **Admin** tab and select **Resources (Users)**.
3. Click the **New** button to create a new resource user.
4. Click the **General** tab and enter basic account information.
   a. In the *First Name* field, enter a **first name of the resource**.
   b. In the *Last Name* field, enter a **last name of the resource**.
5. Click the **Security** tab and create login credentials.
   a. In the *Security Level* field, select **API User (System)**.
   b. In the *API Tracking Identifier* field, select the **Integration Vendor** option and then select **Axcient - x360Sync** from the drop-down menu.
6. Using the main navigation menu, point to **Admin** and select **Features & Settings**.
7. Click to expand the **Resources/Users** accordion menu and select the **Protected Data Permissions** link.
8. Find the resource account and ensure the **View Protected Data** checkbox is selected.
9. Click the **Save** button when you are finished.



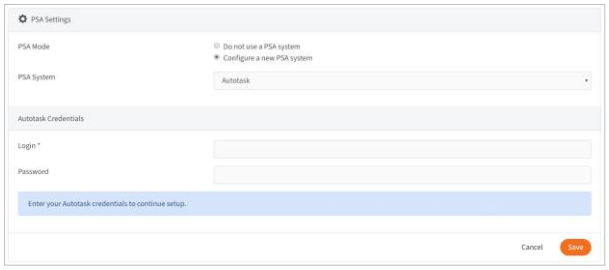
Step 2: Enter Autotask Credentials in x360Sync

After the API user is configured in Autotask, you will need to enter these credentials in the x360Sync administrative web portal.

1. In the *Organization* navigation menu, select the master level organization. The master organization displays.
2. In the master level organization, click the **Settings** tab. The *Settings* page displays.
3. Click the **PSA** tab. The *PSA Settings* section displays.
4. In the *PSA Mode* field, select the **Configure a New PSA System** radio button. The page expands to allow you to select the appropriate PSA system.



5. In the *PSA System* drop-down menu, select **Autotask**. The page expands to show Autotask credential fields.

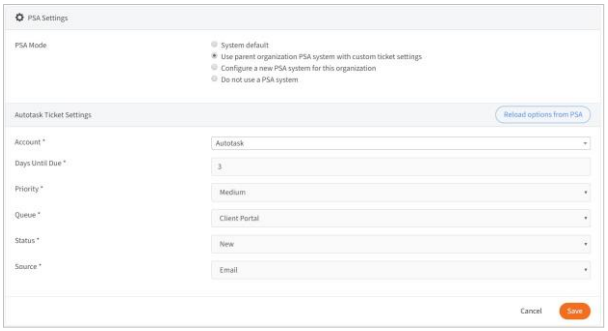


6. In the *Login* and *Password* fields, enter **credentials** for API user created in Autotask.
7. Click the **Save** button to continue. The page will expand to display the *Autotask Ticket Settings* section of the page.
8. In the *Autotask Ticket Settings* section, leave each Autotask fields set to default values (including *Account*, *Due Date*, *Priority*, *Queue*, *Status*, and *Source* fields). You will be able to customize ticket settings for each of your organizations after you configure the initial setup.
9. Click the **Save** button when you are finished.

After initial login credentials have been configured, you can link your organizations to an Autotask account.

1. In the *Organization* navigation menu, select the organization for which you want to configure Autotask settings. The organization displays.
2. In the selected organization, click the **Settings** tab. The *Settings* page displays.
3. Click the **PSA** tab. The *PSA Settings* section displays.
4. In the *PSA Settings* section, select the **Use Parent Organization PSA System with Custom Ticket Settings** radio button.

5. In the *Account* drop-down menu, select the **account** that matches the specific organization. The fields will automatically populate based on the selected account.



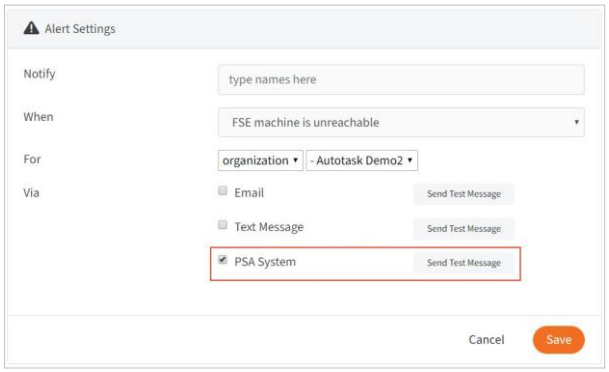
6. Click the **Save** button when you are finished.

Step 3: Set Up Alerts

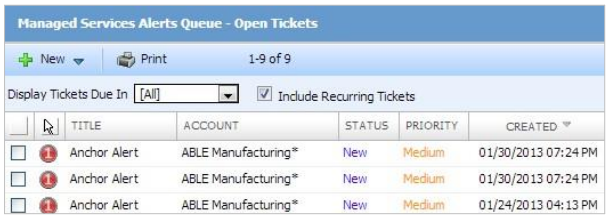
When the organization is linked with an Autotask account, you can set up alerts that will display in the Autotask system.

1. While still in the organization, click the **Activity** tab. The *Activity Log* page displays.
2. In the *Activity Log* page, click the **Create Alert** button.

   The *Alerts* page displays.
3. In the *Alerts* page, configure alerts, making sure to click the **PSA System** checkbox.



You will now be able to view alerts in Autotask for the appropriate account.



How to Integrate with a PSA System—ConnectWise

Overview

ConnectWise is a professional services automation (PSA) platform for companies that sell, service, and support technology. If you use ConnectWise as your PSA platform, you can optionally integrate this platform with x360Sync in the following ways:

- Track alerts that originate in x360Sync.
- Systematize your billing process related to number accounts, total storage, orwhether File Server Enablement is being utilized.

These integration options allow you to manage important customer information in ConnectWise, thereby decreasing the time required to track events and manage billing tasks, and decreasing the margin for human error.

NOTE
These instructions will help you configure both alert and billing integration settings. You might also decide to only configure alerts, or only configure billing.

Prerequisites

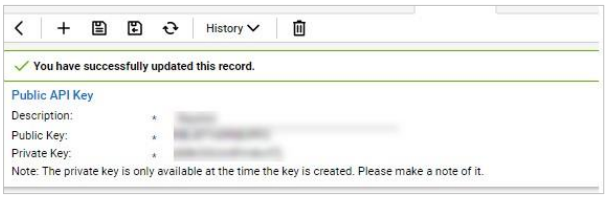
The following items are required prior to integrating with ConnectWise:

- An x360Sync Administrator Account
- A ConnectWise Account
- Existing customers in ConnectWise

Step 1: Create an API Key

You can obtain API information within the ConnectWise service. When integrating ConnectWise with x360Sync, you will need to create a new API key.

1. Log in to ConnectWise and open the *System* menu.
2. In the *System* menu, click the **Members** link.
3. In the *Members* page, click the **API Members** tab and then click the **plus** icon to create a new API Member.
   a. In the *Member ID* field, enter **Axcient**.
   b. In the *Role ID* field, make sure the role is configured with **Add**, **Update**, and **Close** tickets.
4. Click the **Save** button but do not close the window. After you save your settings, you will be given access to the *API Keys* tab.
5. Click the **API Keys** tab and then click the **plus** icon to create a new API key.
   a. In the *Description* field, type **x360Sync**.
   b. Click the **Save** button but do not close the window.
   c. Record the *public key* and *private key* before you close the window. You will not be able to view the private key again after this window is closed.



Step 2: If Configuring Billing, Set Up ConnectWise Products and Agreements

If you are integrating with ConnectWise billing, you must first select the x360Sync products for which you want to bill. You can define one or more of the following products, based on your specific billing needs.

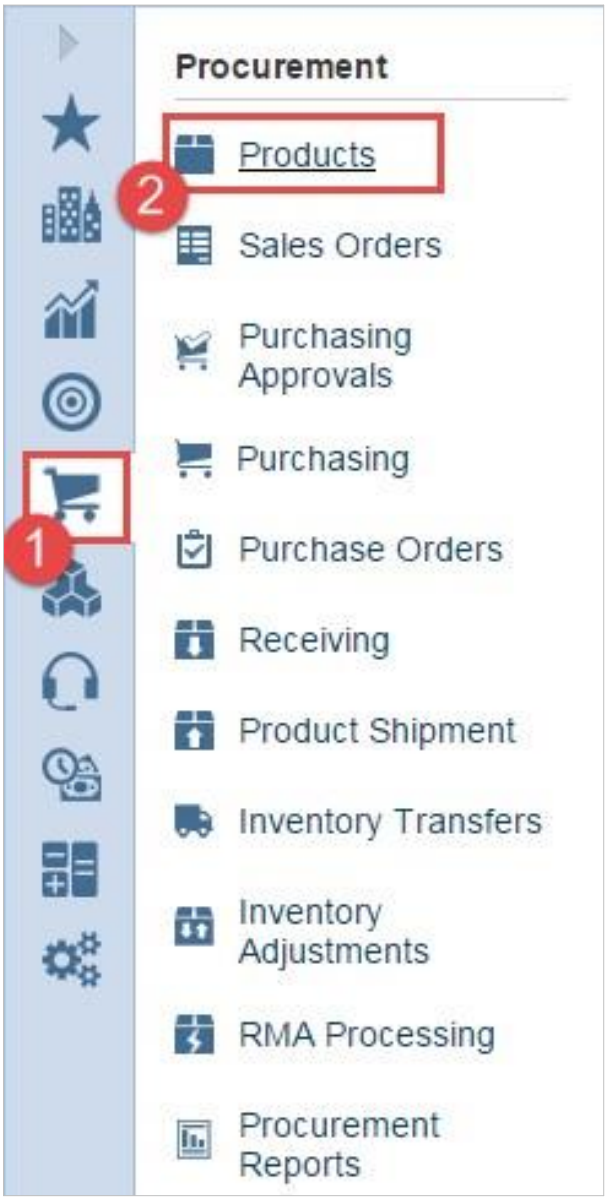
- Number of accounts
- Total storage
- File Server Enablement

After you select these products, you will then set up specific agreements for each customer. Agreements help you define how the particular customer will be billed.

Set Up ConnectWise Products

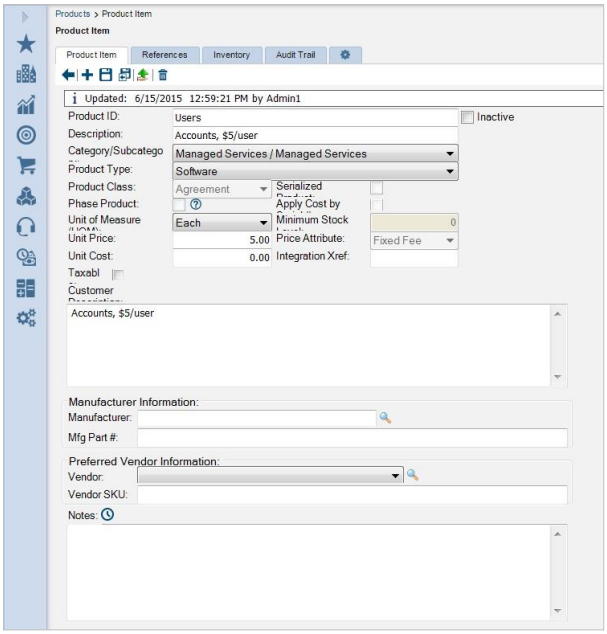
You must complete the following steps for each product that you want to define. For example, you might want to define one or all of the following products: accounts, total storage, or File Server Enablement.

1. In ConnectWise, navigate to the *Procurement* tab, and then select **Products**.



2. Click the **New Item** button and enter the following information to create a new product:
   a. In the *Product ID* field, give the product a descriptive **name**. This name must exactly match the product name that you will later configure in x360Sync.
   b. In the *Description* field, enter a **short description** for the new product. For example, *Accounts, $5/user*.
   c. In the *Category/Subcategory* drop-down menu, select **Manage Services**.
   d. In the *Product Type* drop-down menu, select **Software**.
   e. In the *Product Class* drop-down menu, select **Agreement**.
   f. In the *Unit of Measure* drop-down menu, select **Each**.
   g. In the *Unit Price* field, enter the **list price** for the product.

h. In the *Customer Description* field, enter a **simpledescription**; for example, *Accounts, $5/user*.

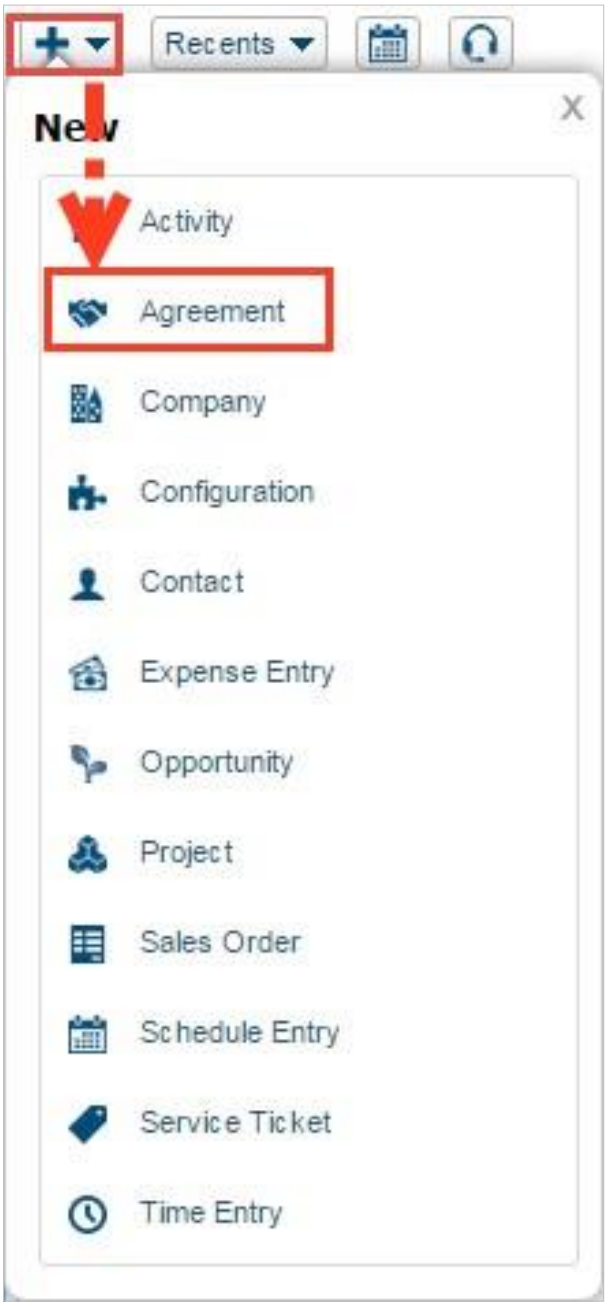


3. Click the **Save** button when you are finished.
4. Repeat the steps above for each product you want to define.

Set Up ConnectWise Agreements to Bill for x360Sync Services

After you define your products, you can set up agreements for each company that will be billed. You can also update an existing agreement.

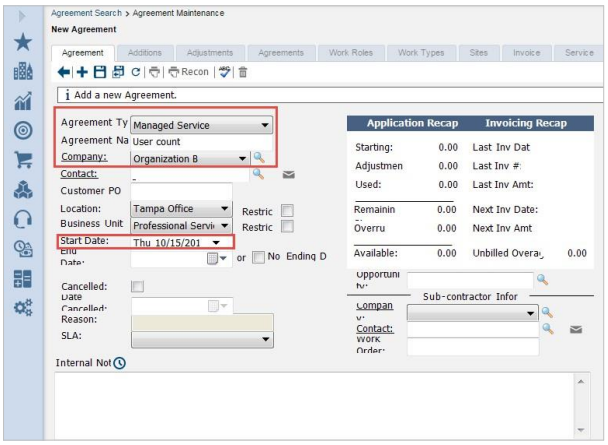
1. In ConnectWise, click the *Quick Launch* drop-down, and select **Agreements**.



2. Find the agreement to which you want to manage changes, or create a new agreement. For each new agreement, click the **New** button.
3. Enter the following information for each agreement:

1. In the *Agreement Type* drop-down field, select **Managed Services**.
2. In the *Agreement Name* field, give the agreement a **name**. This name must exactly match the agreement name that you will later configure in x360Sync.
3. In the *Company* drop-down field, select the appropriate **company** that will be associated with this agreement.

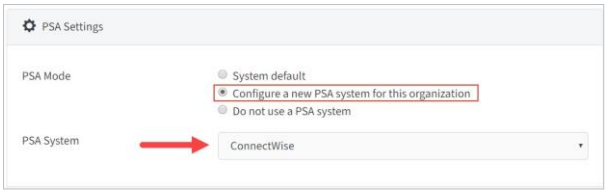
4. In the *Start Date* field, enter a **date** on which the agreement starts.



Step 3: Enter ConnectWise Credentials in x360Sync

Before you can map x360Sync organizations to ConnectWise customers, you must first enter your API information within the top-level organization in x360Sync. You can optionally configure lower-level organizations to inherit these settings.

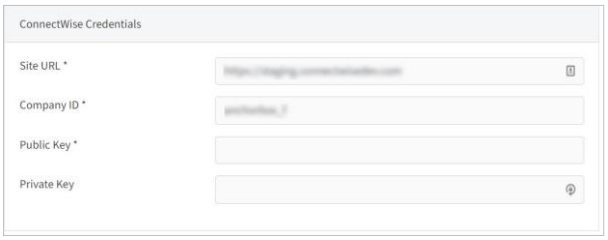
1. In the *Organization* navigation menu, select the top-level organization. The organization displays.
2. Click the **Settings** tab, and then click the **PSA** tab. The *PSA Settings* section displays.
3. In the *PSA Mode* field, select the **Configure a New PSA System** radio button. The page expands to allow you to select the appropriate PSA system.
4. In the *PSA System* drop-down menu, select **ConnectWise**.



   The page expands to show ConnectWise credential fields.
5. Enter the required credentials, including:

1. In the *Site URL* field, enter the **URL** of your ConnectWise site.
2. In the *Company ID* field, enter your **Company ID** as it appears in ConnectWise.
3. In the *Public Key* field, enter the **public key information** you configured when setting up the ConnectWise API key.

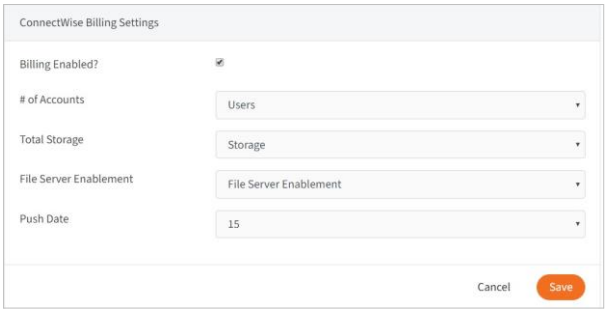
4. In the *Private Key* field, enter the **private key information** you configured when setting up the ConnectWise API key.



5. Click the **Save** button when you are finished.

After credentials are configured correctly, enter information into the ConnectWise Billing Settings section. You only need to fill out this section if you are configuring billing options. Please note that this information will only need to be configured once at the top-level organization, and you can then optionally inherit these settings within lowerlevel organizations.

1. In the *Company* drop-down field, select the **name of the company** as it exists in ConnectWise. If you do not see the name of the company, click the **Reload Options from PSA** button to refresh the connection to ConnectWise.
2. Select the **Billing Enabled** checkbox to indicate that you will be configuring billing.
3. In the *# of Accounts* field, enter the **Product ID** associated with your account product exactly how it appears in ConnectWise.
4. In the *Total Storage* field, enter the **Product ID** associated with your storage product exactly how it appears in ConnectWise.
5. In the *File Server Enablement* field, enter the **Product ID** associated with your File Server Enablement product exactly how it appears in ConnectWise.
6. In the *Push Date* field, select the **day of the month** that billing information will be pushed to ConnectWise.



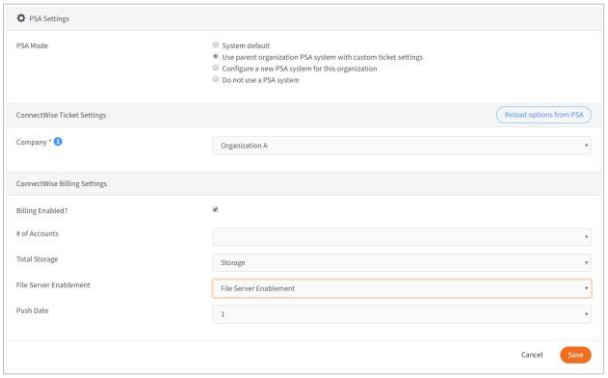
7. Click the **Save** button when you are finished.

Step 4: Map x360Sync Organizations to ConnectWise Customers

After these settings are configured at the top-level organization, you must then map each x360Sync organization to the matching ConnectWise customer.

1. Navigate to an organization that will integrate with ConnectWise.
2. Click the **Settings** tab, and then click the **PSA** tab. The *PSA Settings* section displays.
3. In the *Company* drop-down menu, select the organization's associated **company name** in ConnectWise.
4. Optionally, configure billing settings:

1. In the *ConnectWise Billing Settings* section, select the checkbox next to the appropriate **products** configured in ConnectWise. You must select at least one product. If a product is not selected, it will not be billed through ConnectWise.
2. In the *Choose Agreement* drop-down field, select the appropriate **agreement** configured in ConnectWise. If an agreement is not selected, ConnectWise will not be able to complete the billing process.
3. Click the **Save** button.

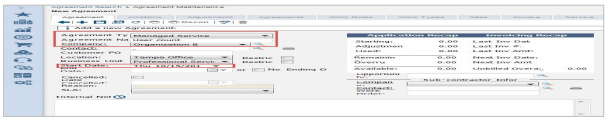


After everything is correctly mapped, you will be able to push billing information from x360Sync into ConnectWise.

Step 5: Set Up Alerts in x360Sync

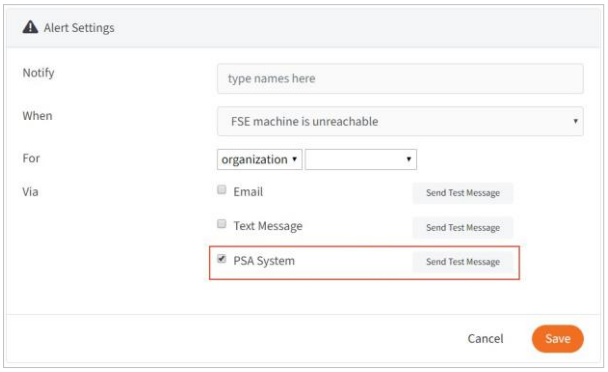
When the organization is linked with a ConnectWise customer, you can set up alerts that will display in the ConnectWise system.

1. While still in the organization, click the **Activity** tab. The *Activity Log* page displays.
2. In the *Activity Log* page, click the **Create Alert** button.



The *Alerts* page displays.

3. In the *Alerts* page, configure alerts, making sure to click the **PSA System** checkbox.



You will now be able to view alerts in ConnectWise for the appropriate customer.

How to Disable or Delete an Organization

Disabled Organizations

When you disable an organization, you temporarily restrict access to the organization and all child organizations (suborganizations). Registered desktop clients and apps will no longer sync with the server, and users will be unable to log in to the web portal. An organization can be re-enabled at any time. You might need to disable an organization when managing trials, when attempting to work with an unpaying client, or for compliance purposes.

To disable an organization:

1. In the appropriate organization, click the **Settings** The *Settings* page displays, showing the *General Settings* section.

2. In the *General Settings* section, click the **Disable Organization** checkbox to disable the organization.
3. Click the **Save** button when you are finished. The organization will remain disabled until you deselect this checkbox.

Deleted Organizations

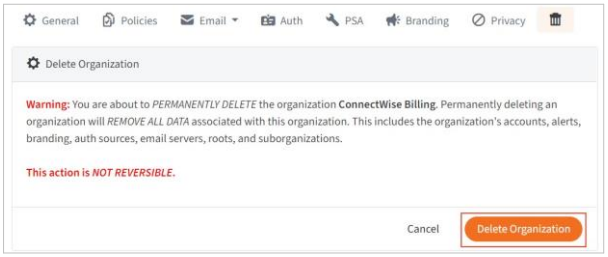
When you delete an organization, you remove all data associated with the organization, including

- Organization accounts,
- Alerts,
- Branding,
- Authentication sources,
- Email servers,
- Files,
- Roots, and
- Suborganizations.

When you delete an organization, this action cannot be undone. Please proceed with caution.

To delete an organization:

1. In the appropriate organization, click the **Settings** tab. The *Settings* page displays.
2. In the *Settings* page, click the **Delete** tab. The *Delete Organization* page displays.
3. In the *Delete Organization* page, you will be presented with a warning message indicating that when you delete an organization, you also delete all data associated with the organization.
4. Click the **Delete Organization** button to permanently delete the organization.



How to Turn on Privacy Mode

You can turn on the Privacy Mode feature for a lower-level organization and its suborganizations, which disables your ability to view data in personal folders, Team Shares, and backups. The purpose of this feature is to allow you to successfully manage the system for customers without accessing or viewing potentially sensitive customer information.

When Privacy Mode is enabled, you will still have the ability to view data within your own organization, and you will retain the necessary privileges required to manage all lower-level organizations and suborganizations.

NOTE

After Privacy Mode is enabled, there is no way to disable the feature.

NOTE

If you are interested in File Server Enablement as a best practice, File Server Enablement should be configured prior to enabling the Privacy Mode feature.

When Privacy Mode is enabled for a lower-level organization, you will not be able to

- Browse or manage the content of personal folders, Team Shares, or backups;
- View titles of files within personal folders, Team Shares, or backups;
- Create backups;
- Move accounts to a different organization;• Move Team Shares to a different organization; or
- Subscribe to Team Shares.

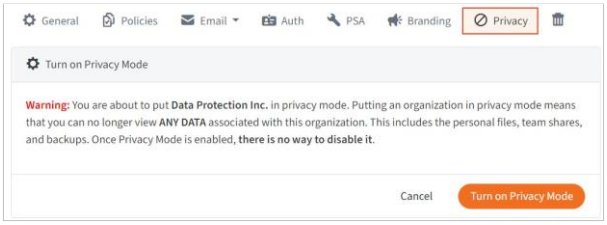
When Privacy Mode is enabled for a lower-level organization, you will *retain* the ability to

- Manage and configure the organization and its suborganizations;
- View information about the organization and its suborganizations;
- View space used by accounts, Team Shares, and backups;
- View the number of files in accounts, Team Shares, and backups; and
- Create accounts and Team Shares.

By default, organization administrators will still have the ability to browse user files within your own organization; the Privacy Mode feature only prevents organization administrators from viewing data within lower-level organizations and suborganizations.
To change this setting, refer to the instructions below.

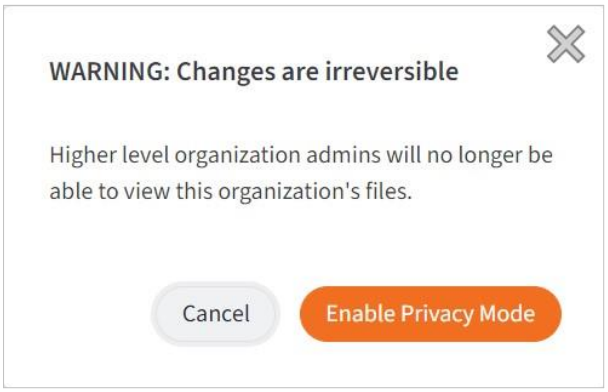
To turn on Privacy Mode:

1. In the appropriate organization, click the **Settings** tab. The *Settings* page displays.
2. In the *Settings* page, click the **Privacy** tab.



The *Privacy Mode* page displays, warning that when Privacy Mode is enabled, it cannot be disabled.

3. In the *Privacy Mode* page, click the **Turn on Privacy Mode** button. A pop-up message displays, warning that higher level organization administrators will be prevented from viewing the organization's files.

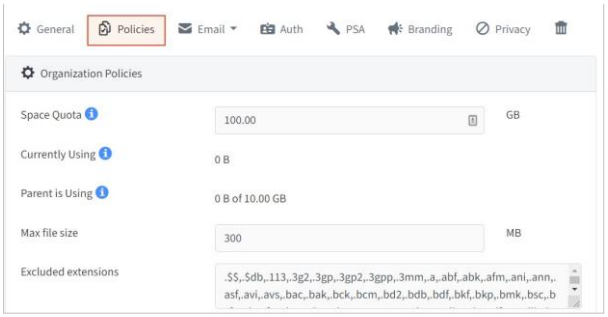


4. In the pop-up window, click the **Enable Privacy Mode** button to continue. The *Privacy Mode* page will refresh to indicate that Privacy Mode has been enabled.

By default, you will still have the ability to browse user files within their own organization; the Privacy Mode feature only prevents you from viewing data within lower-level organizations and suborganizations.

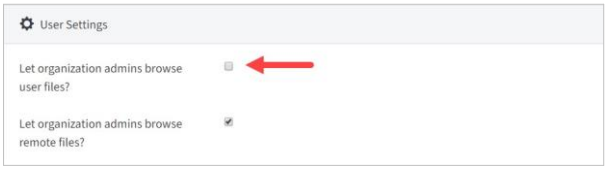
To disable the ability for organization administrators to browse user files within their own organization:

1. Within the appropriate organization, click the **Settings** tab. The *Settings* page displays.
2. In the *Settings* page, click the **Policies** tab.



The *Policies* section displays.

3. In the *User Settings* area, uncheck the **Let organization admins browse user files** checkbox. Organization administrators assigned to this suborganization will no longer have the ability to view users' data.



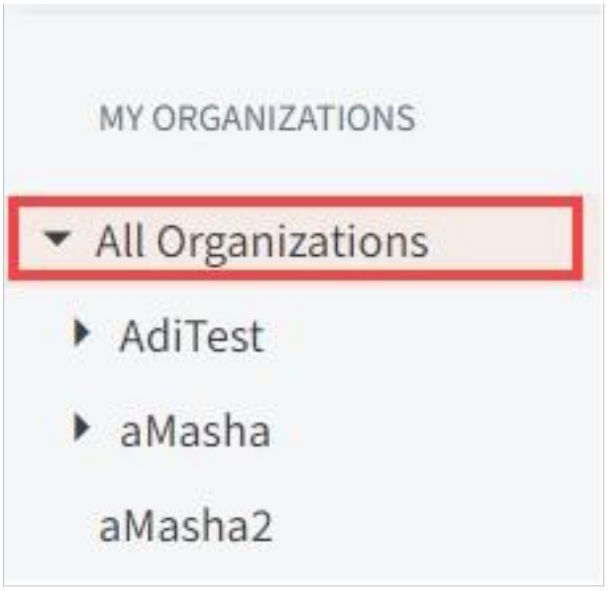
How to Configure the Web Preview Server (Private Cloud)

The Web Preview tool allows users to browse files and view shared items in the web portal and on mobile devices, without needing to fully download content.

The Web Preview tool is hosted within Axcient's server environment; however, private cloud partners can utilize the Web Preview tool by pointing to Axcient's Web Preview Server. These settings can be configured within the administrative web portal.

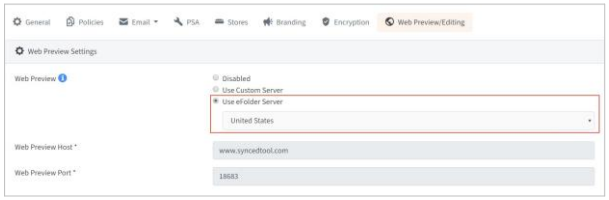
How to Configure Server Settings

1. In the x360Sync administrative web portal, navigate to the top-level organization.



2. Click the **Settings** tab, and then click the **Web Preview/Editing** button.

3. In the *Web Preview Settings* page, click the **Use Server** radio button, and then use the drop-down menu to select the server most closely matching your environment's geographic location.



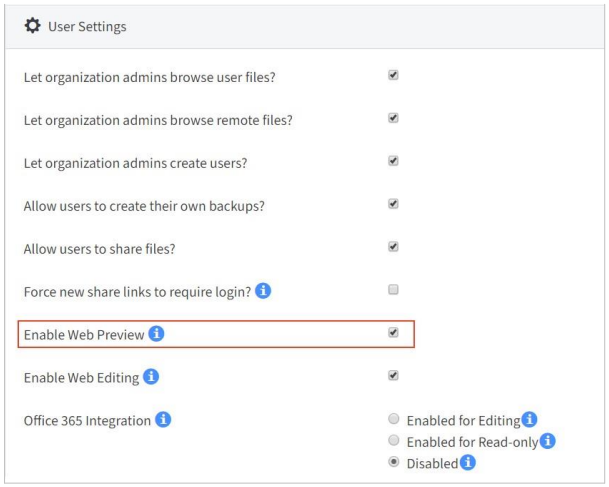
   The *Web Preview Host* field and the *Web Preview Port* field will populate based on your selection.

4. Click the **Save** button when you are finished.

How to Turn On the Web Preview Policy for Individual Organizations

After your server settings are configured, you can then turn on the Web Preview policy for individual organizations.

1. In the appropriate organization, click the **Settings** tab, and then click the **Policies** button. The *Organization Policies* page displays.
2. In the *User Settings* section of the page, click the **Enable Web Preview** checkbox.



3. Click the **Save** button when you are finished.

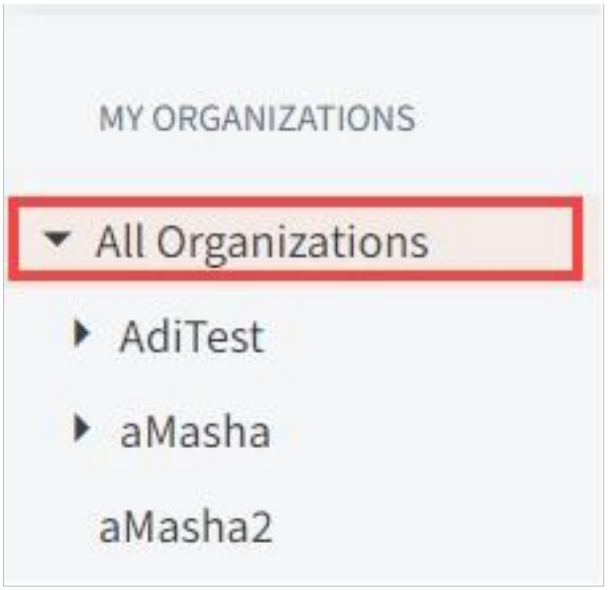
How to Configure the Web Editor Server (Private Cloud)

The Collaborative Web Editor allows you to edit documents, spreadsheets, and presentations when working in the web portal, without needing to download a separate application or navigate away from the system. Additionally, the Collaborative Web Editor allows you to make these changes simultaneously with multiple coauthors, and lets you see each edit in real time..

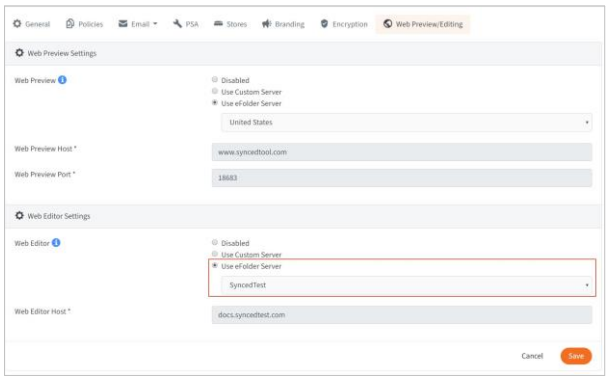
The Collaborative Web Editor is hosted within Axcient's server environment; however, private cloud partners can utilize the Collaborative Web Editor by pointing to Axcient's Web Editor Server. These settings can be configured within the administrative web portal.

How to Configure Server Settings

1. In the x360Sync administrative web portal, navigate to the top-level organization.



2. Click the **Settings** tab, and then click the **Web Preview/Editing** button.
3. In the *Web Editor Settings* page, click the **Use Server** radio button, and then use the drop-down menu to select the server most closely matching your environment's geographic location.



The *Web Editor Host* field will populate based on your selection.

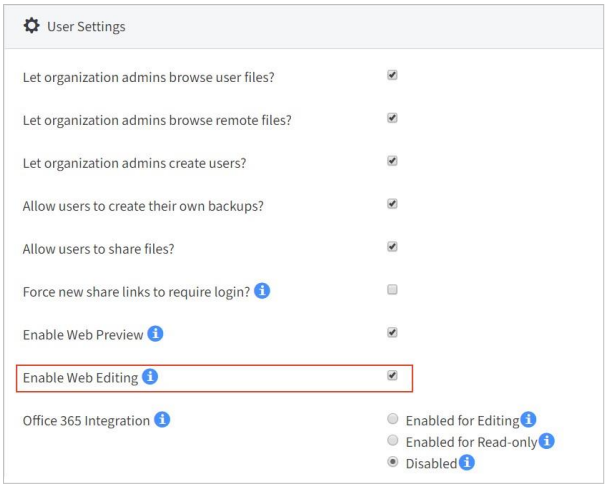
4. Click the **Save** button when you are finished.

How to Turn On the Web Editor Policy for Individual Organizations

After your server settings are configured, you can then turn on the Web Editor policy for individual organizations.

1. In the appropriate organization, click the **Settings** tab, and then click the **Policies** button. The *Organization Policies* page displays.

2. In the *User Settings* section of the page, click the **Enable Web Editing** checkbox.



3. Click the **Save** button when you are finished.

How to Create Service Plans

Service plans are bundles of features and policies that customers can opt-into through a registration form. When a customer submits a registration form, organizations are automatically created with a trial account based on service plan settings and information collected from the form.

Service plans allow you to

- Invite customers and prospects to sign up for a trial of your system,
- Create tiered offerings, and
- Enable and disable features and functionality for individual organizations.

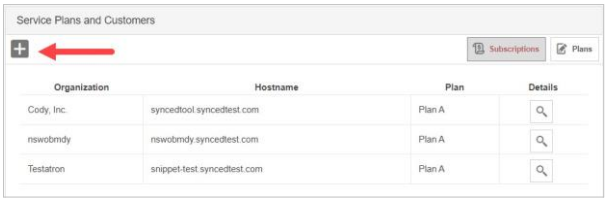
Service Plans can be enabled for organizations and suborganizations. After an organization has been created through a service plan, you can optionally make custom changes to the organization in the *Policies* tab in the administrative web portal.

NOTE

f you edit service plan settings after organizations have been created through the registration form, the existing organizations will not reflect these updated settings. Organizations are not connected to service plan settings after they have been created.

To create service plans:

1. In the dashboard ribbon, click the **Service Plans** link. The *Service Plans and Customers* page display, showing a list of existing subscriptions, if any.
2. In the *Service Plans and Customers* page, click the **Add Plan** button to add a new service plan.



   The *Plans* page displays.
3. In the *Plans* page, enter general settings for the new service plan, including:
   a. In the *Organization* drop-down menu, select the **name of the higher-level organization** that will act as the parent organization to any new organizations created from the service plan.
   b. In the *Plan Name* field, enter a **title** for the service plan.
   c. In the *Plan Code or SKU* field, enter an **abbreviation or accounting code** to represent the service plan.
   d. In the *Notify Email* field, enter an **email address** that should be notified when a new registration form is submitted.
   e. In the *Trial Length in Days* field, enter the length of the **trial period**, in days.
   f. In the *Monthly Cost* field, enter the **cost per month** of the service plan.
   g. In the *Currency Sign* field, enter a **currency symbol** (for example, $).
   h. In the *Min Number of Users* field, enter the **minimum number of user accounts** allowed by the service plan.
   i. In the *Max Number of Users* field, enter a **user limit** that will be allowed for the organization. Enter **0** for an unlimited number of user accounts.
   j. In the *Max Number of Suborganizations* field, set the **maximum number of child organizations** allowed under the higher-level organization. Alternatively, enter **-1** to disable the creation of suborganizations, or enter **0** to allow an unlimited number of suborganizations.
   k. In the *Space Quota* field, enter the **space** that will be allotted to organizations created under the service plan. This number can exceed the

disk space that is currently available; however, you will be warned when an organization reaches capacity.

l. In the *Max File Size* field, set the **maximum size of individual files** that can be uploaded into the system through desktop clients. By default, this is set to 300MB.

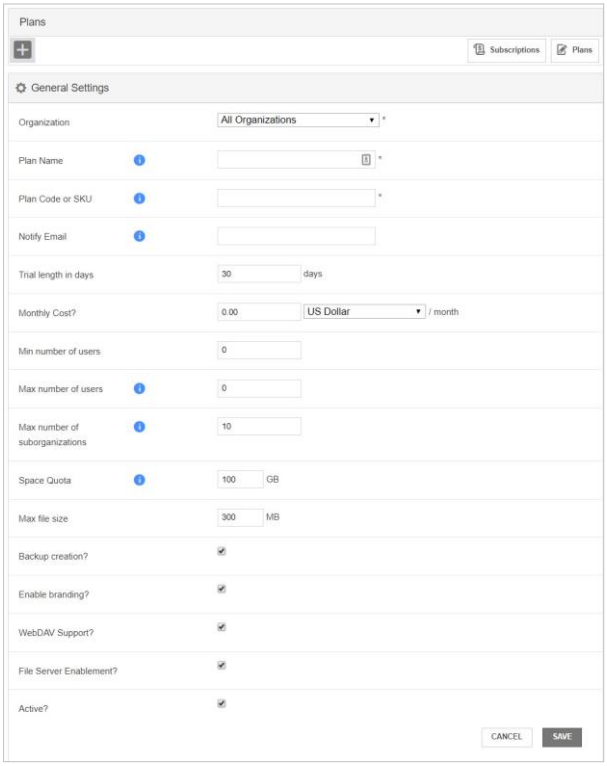
m. Select the **Backup Creation** checkbox to allow the creation of backups.

n. Select the **Enable Branding** checkbox to allow custom styles and logos.

o. Select the **WebDAV Support** checkbox to support WebDAV connections, which is another way for end users to view and edit files—both personal and through Team Shares—located in the cloud. WebDAV is useful when you do not want local copies of large files being stored on external machines. For more information, please reference the End User Guide.

p. Select the **File Server Enablement** checkbox to allow machines to be cloudenabled. With File Server Enablement, you can keep the existing file structure on the server while allowing remote access to files and folders.

q. Select the **Active** checkbox to indicate that the service plan is currently available for use.



Creating and Managing Accounts and Machines

After creating organizations or suborganizations, you can create user accounts manually, from an authentication source (such as Active Directory), or import user accounts from a CSV file.

When new user accounts are created, you can optionally turn on automatic email notifications so that end users receive account information and a link to access the web portal.

From the web portal dashboard, end users will see files, folders, and any Team Shares to which they have been subscribed. They will also have the ability to download a desktop client to their local machines, and use it to manage and upload files to the cloud. Users can also download and install tablet or smart phone apps—including apps for Android devices, iOS devices, and Windows Phones—to access their files. When these machines are attached to a user account, you can track and manage these machines in the *Machines* tab.

For more information about how end users use the system, please reference the End User Guide.

How to Manually Create User Accounts

You have many options for creating user accounts, including bulk-importing users through Active Directory and CSV files. In some instances, however, you might want to manually create individual user accounts.

To manually create user accounts:

1. In the *Organization* navigation menu, select the organization in which you want to create the new user account. The selected organization displays.
2. Click the **Accounts** tab. The *Accounts* page displays.

3. In the *Accounts* page, click the **Create User** button.

The *Account Settings* page displays.

4. In the *Account Settings* page, enter account details for the new account, including:
   a. In the *First Name* field, enter the user's **first name**.
   b. In the *Last Name* field, enter the user's **last name**.
   c. In the *Email* field, enter the user's **email address**. Each user account must have its own unique email address associated with it.
   d. In the *Password* field, enter **password** credentials; alternatively, click the **Auto-Generate** checkbox to allow the system to automatically generate a password for the user. The user will be prompted to change an automatically generated password when he or she first logs in to the web portal.
   e. In the *Confirm Password* field, retype to confirm the **password** if it was manually typed into the *Password* field.
   f. Use the *Password Expires* field if you would like to generate a time-sensitive password for the new user account. You can select from **6 hours**, **12 hours**, or **24 hours**. If you do not want to generate a time-sensitive password, leave this drop-down field set to **Never**.
   g. In the *Mobile Phone Number* field, enter the **mobile phone number** of the user.
   h. In the *Language* drop-down menu, select the user's preferred **language**, which controls the language settings displayed in the web portal and mobile apps, as well as number formatting. Leave this field blank to use the organization's default language setting.
   i. In the *Timezone* drop-down menu, select the user's preferred **timezone**, which controls the display of dates and times. Leave this field blank to use the organization's default timezone setting.
   j. Click the **Shared Quota** checkbox if you want the user to be assigned a shared pool of space within the organization.
   k. In the *Individual Space Quota* field, enter a specific **quota** for the user if he or she is not part of the shared quota pool for the organization.

l. In the *Email User When They Reach* field, select a **percentage** checkbox to indicate if a user should be notified when approaching a certain percentage of his or her quota.

m. Select the **Send Welcome Email** checkbox to send a welcome email to the user. Uncheck this checkbox if you would like to send the welcome email at a later date; for example, when you finish configuring the organization and setting up Team Shares.

n. Select the **WebDAV Access** checkbox to give the user WebDAV access, which is another way for end users to view and edit files. WebDAV is useful when you do not want local copies of large files being stored on external machines. For more information, please reference the End User Guide.

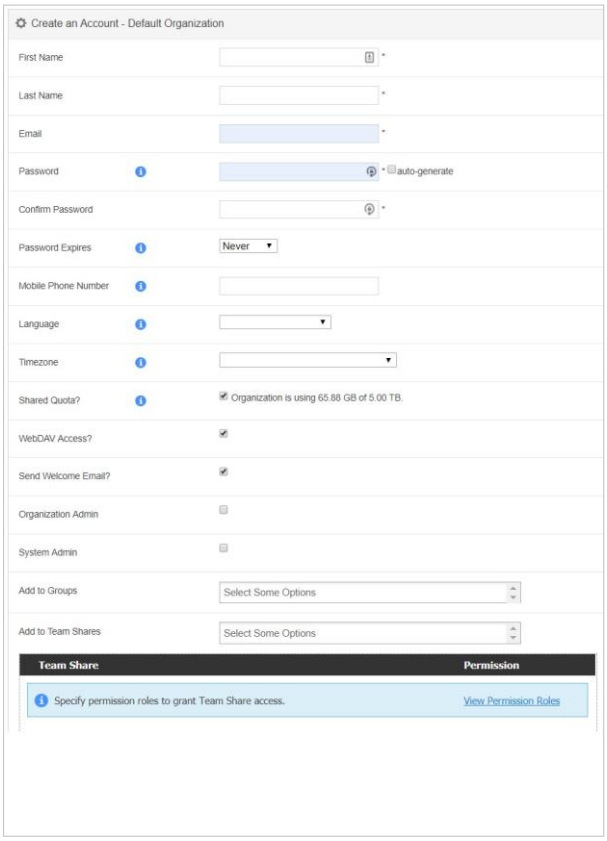
o. Select the **Organization Admin** checkbox to give the user administrative privileges. Users should only be given this level of access if they will be conducting administrative tasks within the system.

p. Select the **System Admin** checkbox to give the user advanced administrative privileges. Users should only be given this level of access if they will be conducting system-related tasks within the system.

q. In the *Add to Groups* search box, type the name of the **group(s)** to which the user should be added, if any.

r. In the *Add to Team Shares* search box, type the name of the **Team Share(s)** to which the user should be given access, if any. Alternatively, click the **All** button to add the user to all Team Shares, or click the **None** button to clear your selection.

s. If you added the user to a Team Share, you can use the *Team Share* section of the page to define the user's permission role within the selected Team Share. By default, the Collaborator role is assigned, giving the user the ability to do anything except trim (delete revisions to files) and purge (permanently delete files and folders). Click the **Collaborator** button to change this setting. For more information on permission roles, please visit the *How to Create a New Team Share* section of this guide.



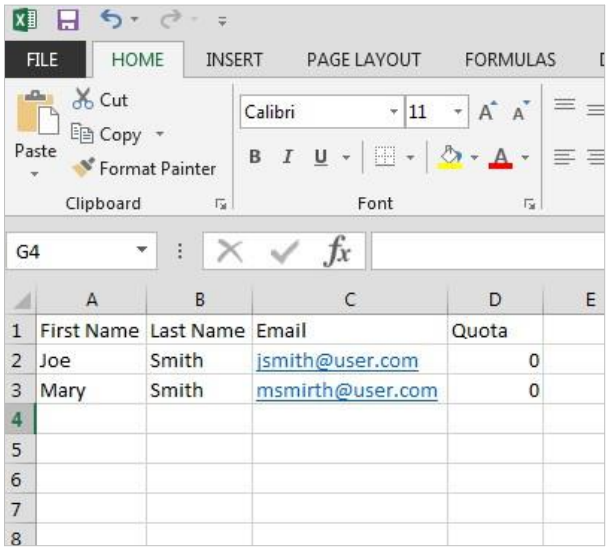
5. Click the **Save** button when you are finished.

How to Import User Accounts from a CSV File

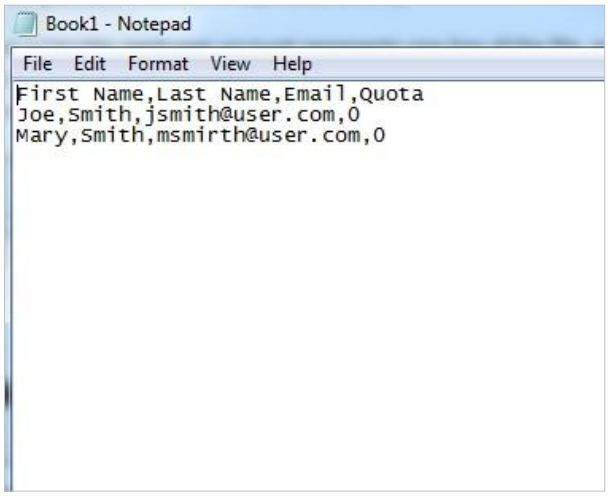
In addition to manually creating individual user accounts, you can also bulk-import users using Active Directory or a CSV file (comma-separated values).

When you use a CSV file, each user account represents one line of the file, and each line contains metadata for one specific user account. You must format each line correctly so that the system can identify the metadata values. The format of each line must be: *First Name*, *Last Name*, *Email*, *Quota* in gigabytes (0 represents unlimited).

For example, you might start with an Excel file filled with user accounts, and then save the file in CSV format.



Alternatively, you can start with a text file and save your file in CSV format. Make sure each value is separated by a comma.

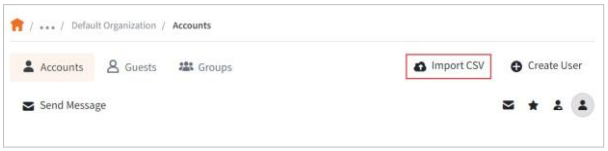


The first line of your file can serve as the header row, but you must indicate this by clicking the **CSV Has a Header Row** checkbox when you upload your file.

To import user accounts from a CSV file:

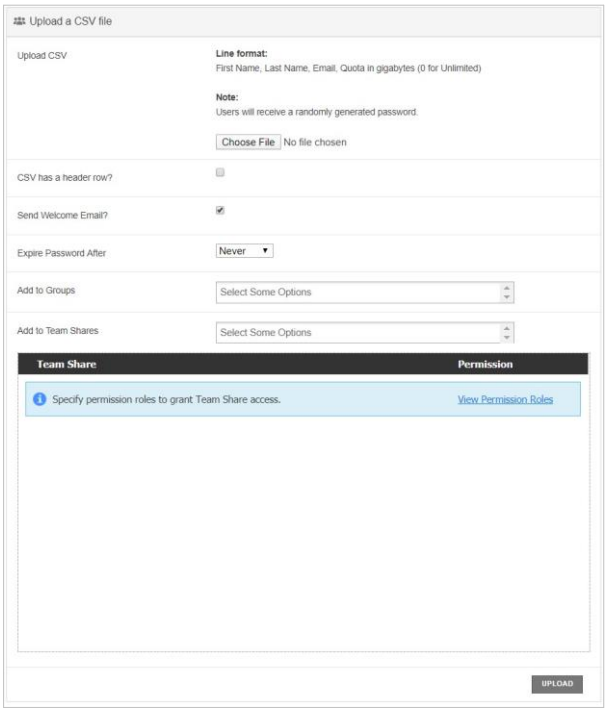
1. Ensure the CSV file has been saved in one of the following formats:
   - CSV (MS-DOS)
   - CSV (comma delimited)
2. In the *Organization* navigation menu, select the organization in which you want to create the new user accounts. The selected organization displays.
3. Click the **Accounts** tab. The *Accounts* page displays.

4. In the *Accounts* page, click the **CSV Import** button.



The *Create Multiple Accounts* page displays.

5. In the *Create Multiple Accounts* page, upload your CSV file into the system.
   a. Click the **Choose File** button, and select the CSV file from your local machine.
   b. Select the **CSV Has a Header** checkbox if the first line of your file includes header information (formatted as *First Name*, *Last Name*, *Email*, *Quota*).
   c. Select **the Send Welcome Email** checkbox to send a welcome email to each newly created user account.
   d. Click the **Expire Password After** drop-down menu to determine whether or not the newly generated passwords will expire after a certain time period. You can choose from *Never* (default), *6 hours*, *12 hours*, or *24 hours*.
   e. In the *Add to Team Shares* box, select the **Team Shares** to which the user should be given access, if any.
   f. In the *Add to Groups* box, select the **Groups** to which you would like to add the users, if any.
   g. Click the **Upload** button when you are finished.



6. When the CSV file finishes uploading, the *Create Multiple Accounts* page will refresh, displaying a list of imported accounts. Use this list to confirm that all of your accounts uploaded successfully.

   An account marked with an *Email address already in use* message indicates that the email address currently exists in the system. Duplicate accounts will not be imported and the existing record will not be updated.
7. To clear this form and re-upload a new CSV file, click the **Reset Form** button.

How to Import User Accounts from an Authentication Source

Overview

Active Directory, or any LDAP authentication source, can act as a source for user accounts within the system. When an authentication source is configured, an imported user can log in to the web portal using the credentials attached to his or her authentication source account.

You can integrate with an authentication source in one of two ways: using the *machine method*, or using the *server method*.

- *Machine Method*—If you use the machine method, you will first need to download the desktop client onto the server that houses the authentication source. You will then register that desktop client to any user within the system. For instructions on how to install and register the desktop client, please reference the End User Guide.
- *Server Method*—Using the server method, you can connect to your authentication source without installing a desktop client on the machine that houses the authentication source. This server must be publicly accessible in order to use this method.

TIP

When registering the desktop client to a user account on a server, it is recommended that you create a *service account*. A service account should not be subscribed to team shares, should be set to use fixed space quota of .01GB, and should be configured using a predetermined naming system.

Notes to Consider

- If you have already manually created user accounts, and want to convert these existing user accounts to AD user accounts, you must ensure that the email addresses match. If an email address matches, then the system will successfully convert the existing user account to an AD user account, and there will be no need to uninstall and reinstall desktop clients.
- Additionally, when you integrate with Active Directory, desktop clients can be silentlypushed, installed, and registered to end users without needing to alert the end user.

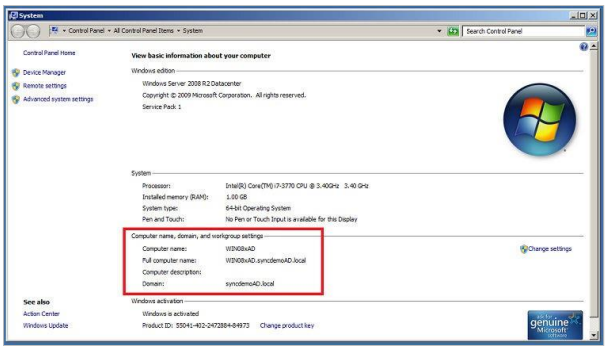
  For more information about silent installations, please reference the *How to Silently Install Desktop Clients* section of the Guide.
- While x360Sync will successfully integrate with any LDAP authentication source, itwill not integrate with non-LDAP sources, such as Azure AD. While Azure AD supports internal LDAP authentication, it does not currently support external LDAP authentication. For more information, please reference this TechNet Blog.

Machine Method

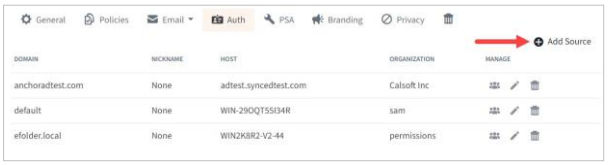
To integrate with Active Directory using the machine method:

1. On the server that houses Active Directory, download and install the desktop client. For instructions on installing the desktop client, please reference the End User Guide.
2. After you install the desktop client, register the desktop client to a user account. For instructions on registering the desktop client, please reference the End User Guide.
3. While still in the server that houses Active Directory, record the full computer name.
   a. Click the **Start** menu, right-click *Computer*, and select **Properties**. The *System* window displays.
   b. In the *System* window, find the informational field titled, *Full Computer Name*.

Record the full name of the computer so that it can be referenced later.

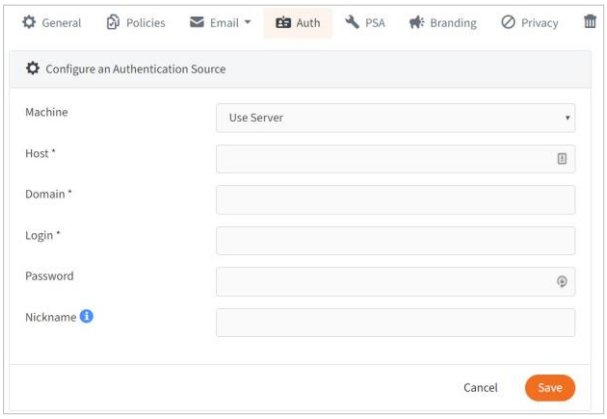


4. When you are finished installing and registering the desktop client, return to the administrative web portal.
5. While in the appropriate organization, click the **Settings** tab. The *Settings* page displays.
6. In the *Settings* page, click the **Authentication** tab. The *Authentication* section displays.
7. In the *Authentication* section, click the **Add Source** button to add an authentication source.



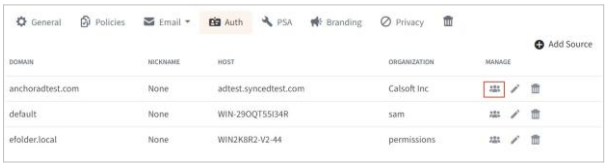
The page refreshes to display a *Configure an Authentication Source* section of the page.

8. In the *Configure an Authentication Source* section of the page, configure your authentication source.
   a. In the *Machine* drop-down menu, select the **name of the machine** that houses your Active Directory.
   b. In the *Host* field, enter the full **computer name** that you recorded above.
   c. In the *Domain* field, enter the **Active Directory Fully Qualified Domain Name** (FQDN) (for example, *anchor.com*).
   d. In the *Login* field, enter a **username** that has administrative access to Active Directory.
   e. In the *Password* field, enter the corresponding **password** for the administrative user.
   f. Click the **Save** button when you are finished.



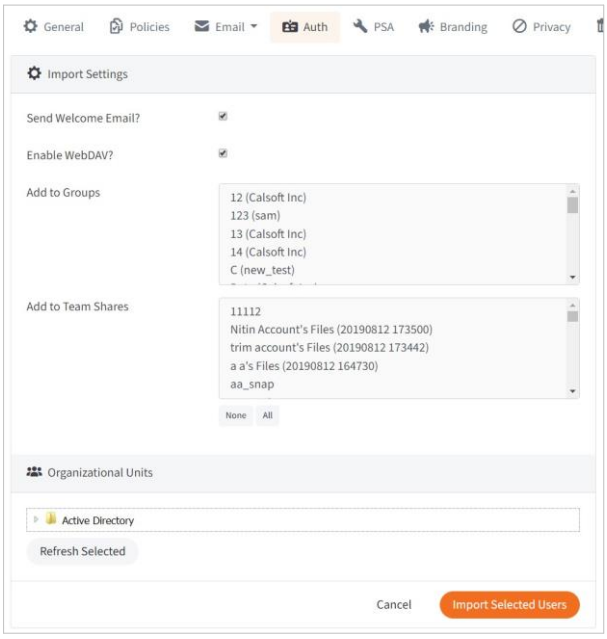
After you have entered information for Active Directory, the page will refresh to show you a listing of all current authentication sources.

9. In the *Manage* column, click the **Import Users** button.



The page refreshes to show import settings.

10. Configure settings for importing users.
    a. Select the **Send Welcome Email** checkbox to send a welcome email as soon as users are imported into the system.
    b. Select the **Enable WebDAV** checkbox to enable WebDAV.
    c. Use the *Add to Team Shares* box to select the Team Shares to which all user accounts should be added. Alternatively, click the **All** button to add all user accounts to all Team Shares, or click the **None** button if you do not want to add user accounts to Team Shares. Please note that you can add user accounts to Team Shares after they have been created.



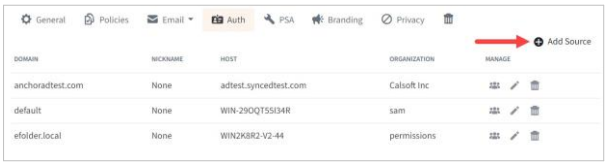
11. In the *Organizational Units* box, browse and select the **Active Directory users** that should be imported; alternatively, select specific organizational units (OUs) to be added to the system.

12. Click the **Import Selected Users** button to import the users into the system. End users can now log in to the system using their AD email address and password.

Server Method

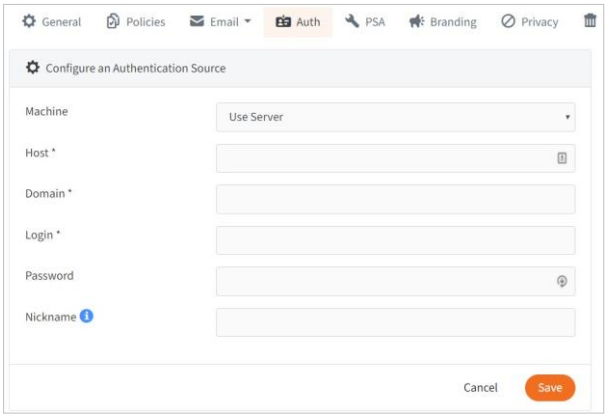
To integrate with Active Directory using the server method:

1. While in the appropriate organization, click the **Settings** tab. The *Settings* page displays.
2. In the *Settings* page, click the **Authentication** tab. The *Authentication* section displays.
3. In the *Authentication* section, click the **Add Source** button to add an authentication source.



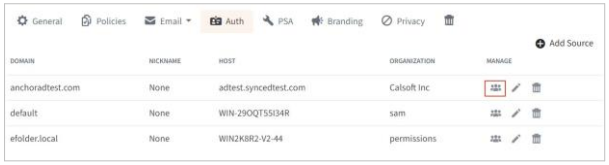
The page refreshes to display a *Configure an Authentication Source* section of the page.

4. In the *Configure an Authentication Source* section of the page, configure your authentication source.
   a. In the *Machine* drop-down menu, select **Use Server**.
   b. In the *Host* field, enter the **internal IP address** of the Active Directory server machine if it is on the same network as the x360Sync Server. If the Active Directory server machine is outside of your network, enter the **publicly resolvable host name or IP address**.
   c. In the *Domain* field, enter the **Active Directory Fully Qualified Domain Name** (FQDN) (for example, *anchor.com*).
   d. In the *Login* field, enter a **username** that has administrative access to Active Directory.
   e. In the *Password* field, enter the corresponding **password** for the administrative user.
   f. Click the **Save** button when you are finished.



After you have entered information for Active Directory, the page will refresh to show you a listing of all current authentication sources.

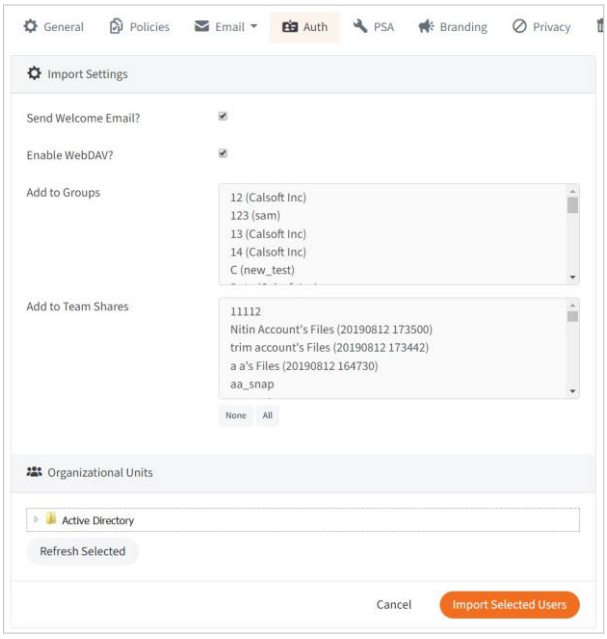
5. In the *Manage* column, click the **Import Users** button.



The page refreshes to show import settings.

6. Configure settings for importing users.

a. Select the **Send Welcome Email** checkbox to send a welcome email as soon as users are imported into the system.
b. Select the **Enable WebDAV** checkbox to enable WebDAV.
c. Use the *Add to Team Shares* box to select the Team Shares to which all user accounts should be added. Alternatively, click the **All** button to add all user accounts to all Team Shares, or click the **None** button if you do not want to add user accounts to Team Shares. Please note that you can add user accounts to Team Shares after they have been created.



7. In the *Organizational Units* box, browse and select the **Active Directory users** that should be imported; alternatively, select specific organizational units (OUs) to be added to the system.

8. Click the **Import Selected Users** button to import the users into the system. End users can now log in to the system using their AD email address and password.

How to Silently Install the Desktop Client

A desktop client can be installed and registered in unattended mode (silently) by running the desktop client's executable file from the command line.

Installing a Desktop Client in Unattended Mode

First, the desktop client must be installed. The following arguments can be used to control the installation process:

--help	Display the list of valid options
--revision	Display product information
--unattendedmodeui	Unattended Mode UI **Default**: none **Allowed**: none, minimal, minimalwithdialogs
--mode	Installation mode **Default**: win32 **Allowed**: win32 unattended
--installer-language	Language selection **Default**: en **Allowed**: en ar bg ca da nl et fr fi de el es es_AR he hr hu it ja ko pl pt_BR pt ro ru no sl sk sq sv tr zh_TW zh_CN va cy cs
--create_shortcuts	Creates Desktop shortcut with value of 1 **Allowed**: 0, 1 **Default**: 1
--host	Host name **Note**: Do not include http or https protocol; do not include port number, if applicable
--port	Server Port **Default**: 443
--httpport	Server Web Port **Default**: 80

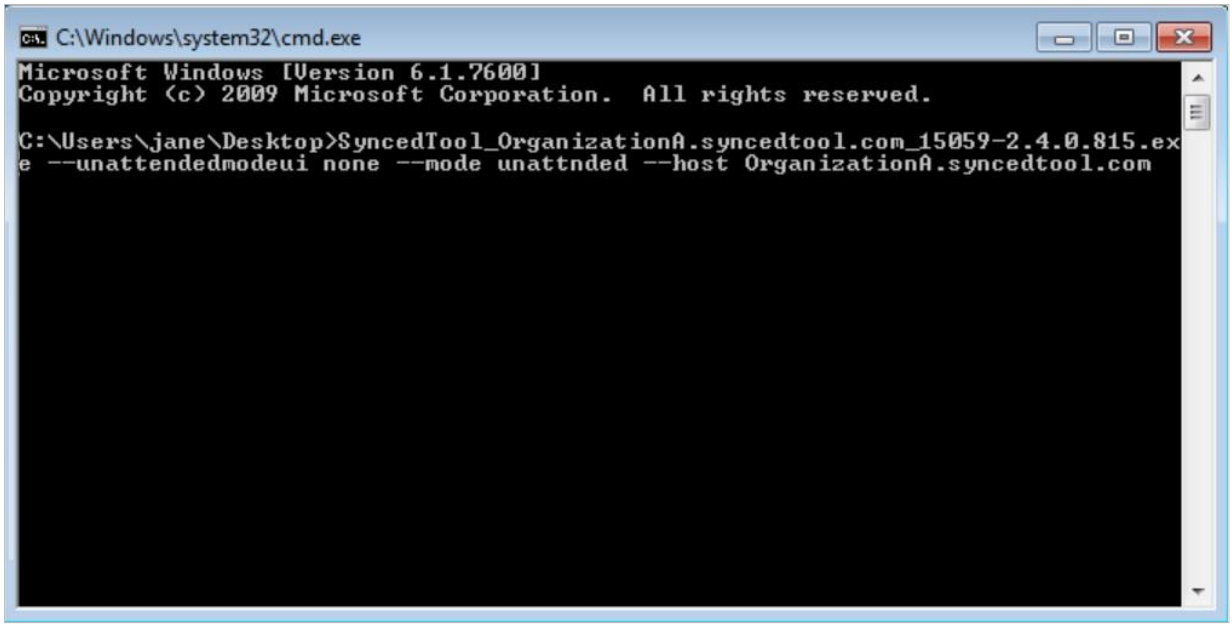
The following example will install the desktop client silently without registering it:

1. From the command-line, navigate to the location of the executable file (installation file). Please note that you should not rename the downloaded executable file when conducting a silent installation. The name of the executable file determines both branding settings and the current revision of the desktop client. If you alter the name of the executable file, branding settings will not be reflected, and the current revision of the desktop client will not be installed. For example, if the executable file exists on the Desktop, run the following commend:

```
cd C:\Users\jane\Desktop
```

2. Run the executable file from the command-line using the following arguments, making sure to replace the information appropriate to the specific environment and user.

```
SyncedTool_OrganizationA.syncedtool.com_15059-2.4.0.815.exe --unattend
```



Registering a Desktop Client in Unattended Mode

After the installation process completes, the desktop client can then be registered to a user silently. The following arguments can be used to control the registration process:

--help	Produce help message
--config	Config file
--action	Action to perform (required) [register|filestatus|userinfo]
--user	Username (email or domain\ad_username)
--password	Password
--auth_code	Two-Factor Authentication code (when the Two-Factor Authentication policy has been enabled and configured)
--localuser	Local user
--path	Path

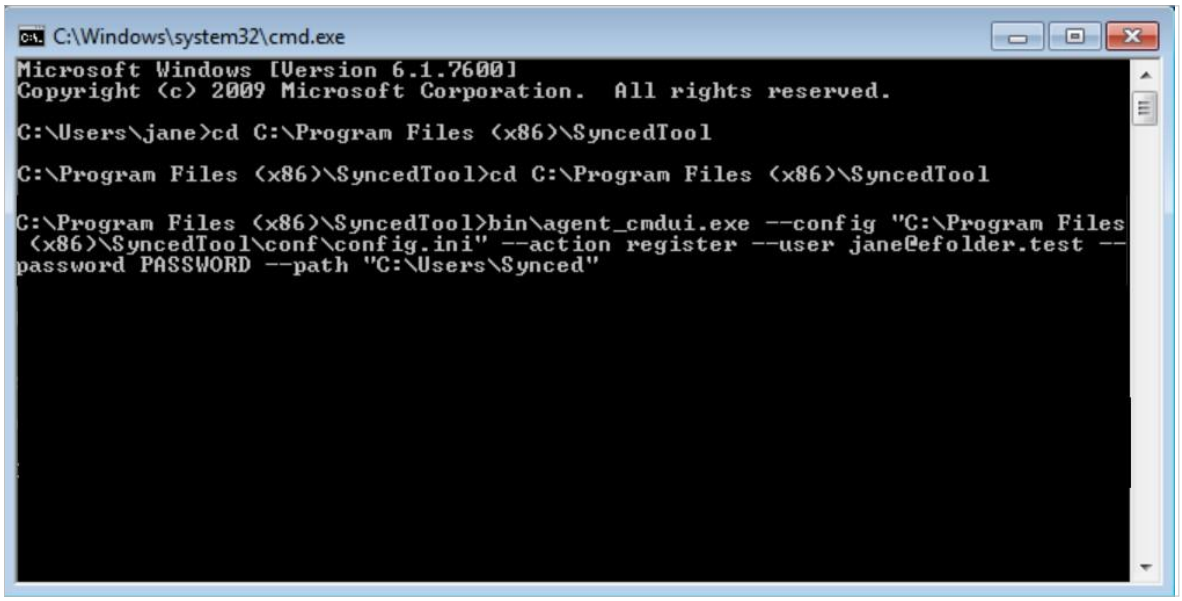
The following example will register the desktop client using the desktop client_cmdui.exe file located in the installation directory bin folder.

1. From the command-line, navigate to the Synced Tool installation directory (for example, C:\Program Files (x86)\SyncedTool).

   ```
   cd C:\Program Files (x86)\SyncedTool
   ```

2. Run the desktop client_cmdui.exe file using the following arguments, making sure to replace the text with information appropriate to the specific environment and user. Please note that you should execute agent_cmdui.exe from its parent folder (for example, C:\Program Files (x86)\SyncedTool) as noted in the example above.

   ```
   bin\agent_cmdui.exe --config "C:\Program Files (x86)\SyncedTool\conf\c
   ```



Troubleshooting

After silently registering the user, you might notice that the application UI still indicates that registration is not complete. Run the following command from the installation directory BIN folder (for example, C:\Program Files (x86)\SyncedTool\bin):

```
agent_gui.exe --message check_registration
```

How to Manage User Accounts

When new users have been added to your system, you have many options for managing user accounts. Using the *Accounts* page, you can view a list of user

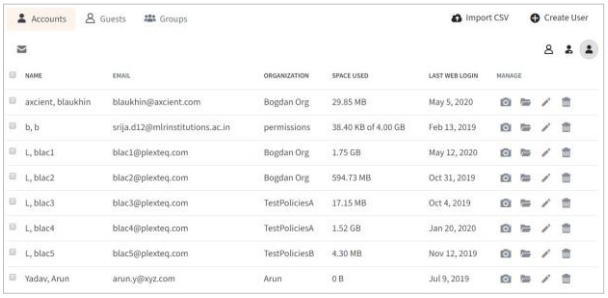
accounts, send email messages to user accounts, edit user accounts, and delete user accounts.

TIP

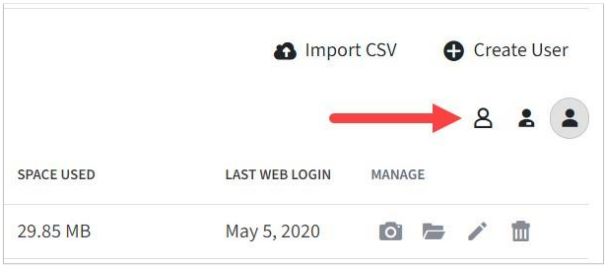
If you want to see a list of all user accounts from every organization and suborganization, make sure your master organization is selected when you access the *Accounts* page.

To manage user accounts:

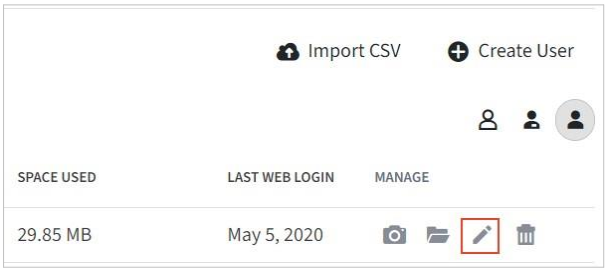
1. In the *Organization* navigation menu, select the organization in which you want to manage user accounts. The selected organization displays.
2. Click the **Accounts** tab. The *Accounts* page displays, showing a list of all user accounts in the selected organization.



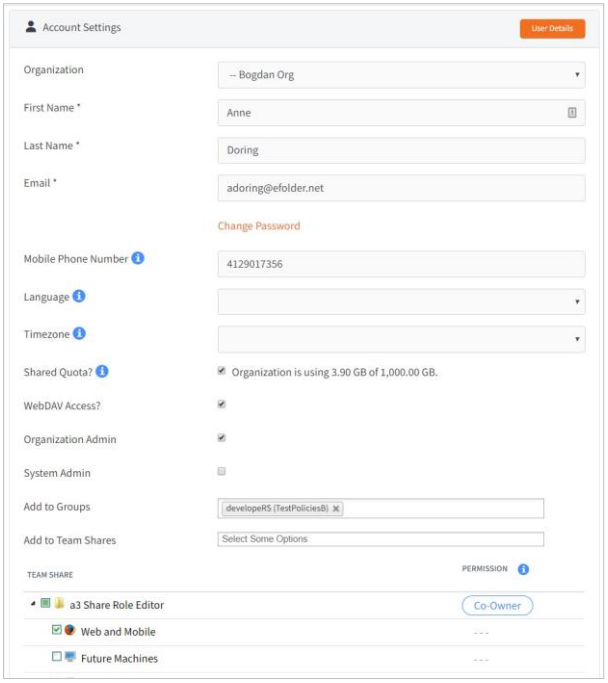
3. In the *Accounts* page toolbar, you can search for individual user accounts using the *Search* field, or filter to view only admins by clicking the **Admin** button, or invited users by clicking the **Invited** button.



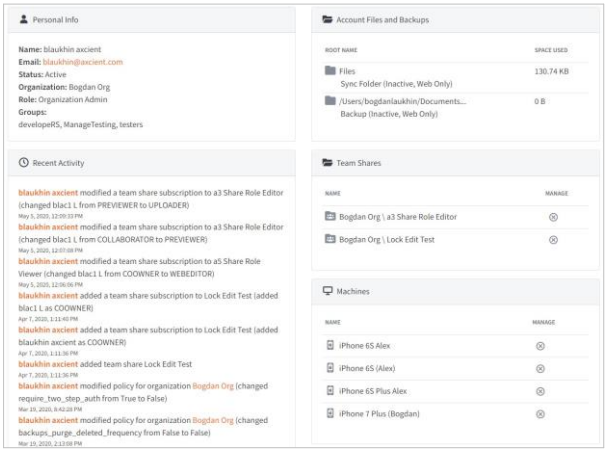
4. In the *Accounts* page, you can optionally edit user account settings.
5. Click the **Edit** button next to the account you want to edit.



The *Account Settings* page displays.



6. In the *Account Settings* page, you can:
   a. Click the **User Details** button to view account activity, such as recent activity, linked machines, account files and backups, Team Shares, and space usage.



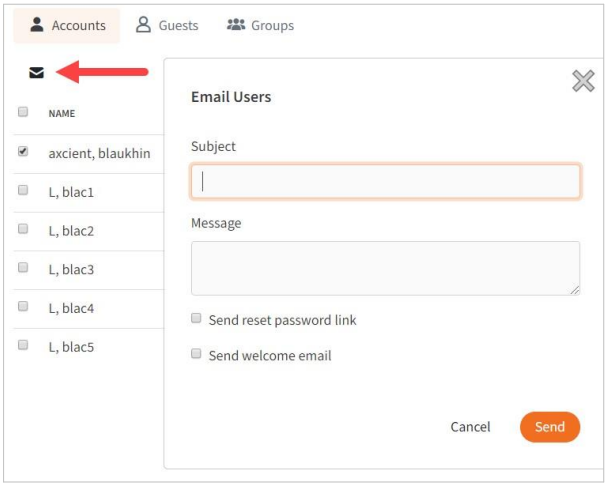
b. Change account details, such as name, login credentials, and settings.

c. Click the **Save** button when you are finished.

7. Also in the *Accounts* page, you can optionally send an email message to selected user accounts.

   a. Click the **checkboxes** to select the users who should receive the email.

   b. Click the **Send Message** button. An *Email Users* dialog box displays.



   c. In the *Email Users* dialog box, enter a **subject** and a **message**.

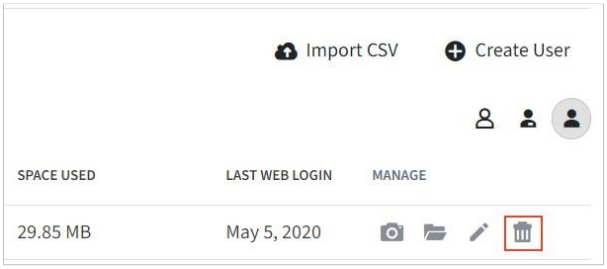
   d. Optionally, click the **Send Reset Password Link** checkbox to resend the selected users' passwords.

   e. Optionally, click the **Send Welcome Email** checkbox to resend a welcome email to the selected users.

   f. Click the **Send** button when you are finished.

8. Optionally, in the *Accounts* page, you can delete users by clicking the **Delete** button.

   The selected user accounts will be deleted from the system.



How to Unlock User Accounts

Overview

To help protect against events such as common brute force and dictionary attacks, the system will lock out user accounts after five failed login attempts. These accounts will remain locked for 30 minutes. If necessary, an administrator can unlock these user accounts from the administrative web portal.

Unlocking LDAP and Activate Directory Accounts

User accounts that have been imported by an LDAP authentication source, such as Active Directory, should be managed within the original source. The Unlock feature does not support LDAP-imported accounts.

Forgot Password Page

To prevent account lockouts, users can click the **Forgot Password** link in the *Login* page when they are having trouble remembering their login credentials.

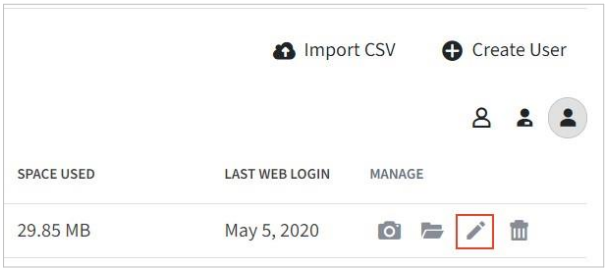
NOTE

Note: The same 30 minute lockout rule applies for users in the Forgot Password page. After five failed reset attempts, users will be locked out for 30 minutes.

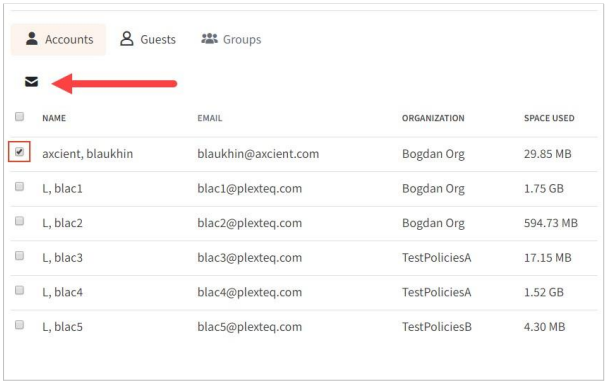
Instructions for Unlocking a User Account

To unlock a user account:

1. In the Organization navigation menu, select the user's organization. The selected organization displays.
2. Click the **Accounts** tab. The *Accounts* page displays, listing all existing accounts.
3. Find the locked out user account and click the **Edit** button.

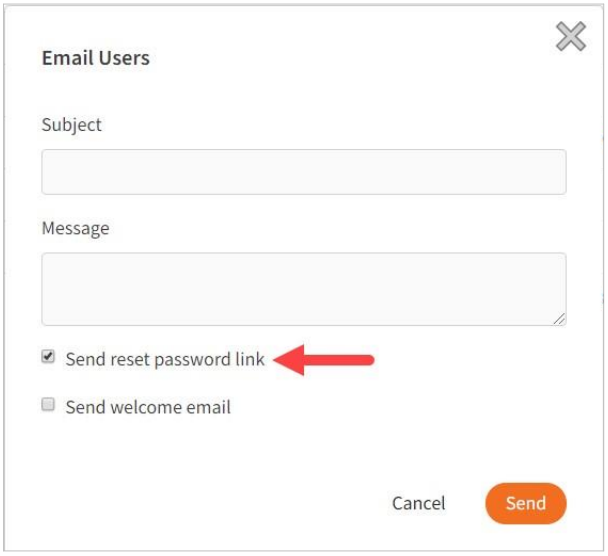


4. In the *Account Overview* section of the *Account Settings* page, click the **Unlock Account** button. The user account is now unlocked, and will be able to log back into the system.
5. Optionally, you can allow the user to reset his or her password from the *Accounts* page. Return to the *Accounts* page and select the checkbox next to the appropriate account.
6. With the account selected, click the **Send Message** button.



An *Email User* dialog box displays, allowing you to compose an email message directly from your web browser

7. Click the **Send reset password** link checkbox to provide the selected user account with a link to reset his or her password.



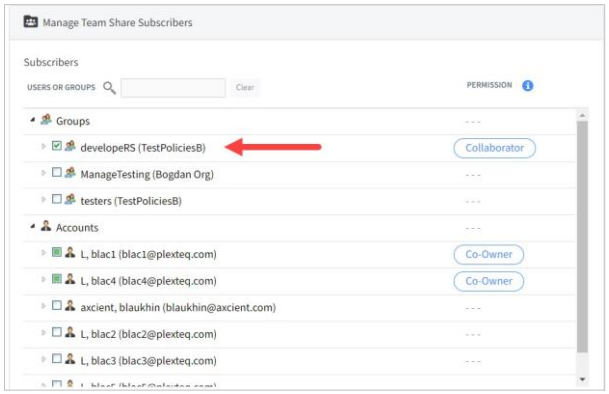
8. Click the **Send** button when you are finished.

How to Create Groups

You can organize end users into Groups to help you manage accounts. When you create a Group, you select accounts that are included in the group, so that the group acts as a single entity within x360Sync.

For example, when creating Team Shares, you can add one single Group to the Team Share, rather than selecting and managing separate accounts. You can even assign a permission role to the group, and each member of the group will inherit that

permission role within the Team Share. Ultimately, this feature helps you manage groups of users within one central location.

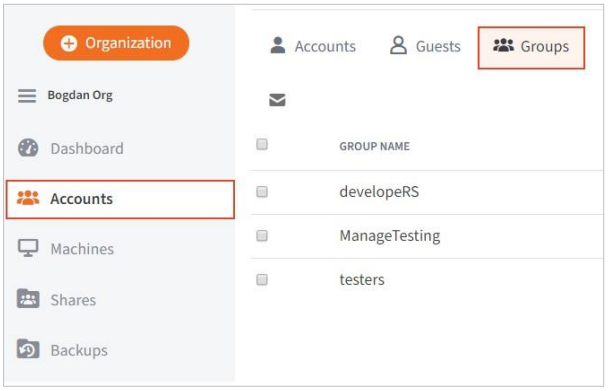


The benefits of Groups include:

- You can easily manage a single Group—rather than multiple accounts—as a subscriber to a Team Share.
- When adding a Group to a Team Share, you can optionally define machine subscription settings and permission roles for the entire Group.

To create groups:

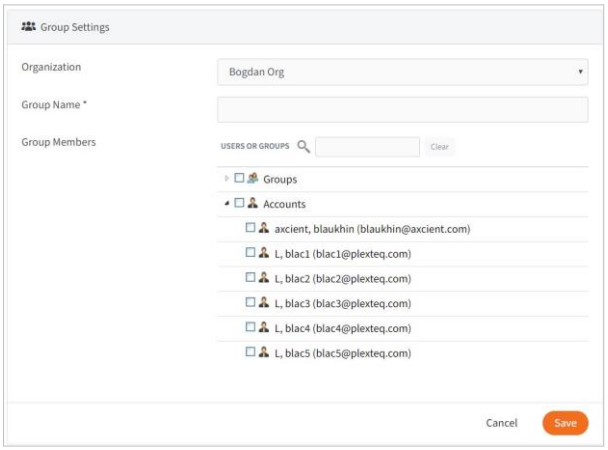
1. In the *Organization* navigation menu, select the organization in which you want to create Groups. The selected organization displays.
2. Select the **Accounts** tab, and then click the **Groups** tab.



   The *Groups* page displays, listing all of your existing Groups.
3. In the *Groups* page, click the **Create Group** button.


Accounts
Guests
Groups
Create Group
GROUP NAME
ORGANIZATION
MANAGE
developeRS
TestPoliciesB
ManageTesting
Bogdan Org
testers
TestPoliciesB

The *Group Settings* page displays, allowing you to configure settings for the new Group.



a. In the *Organization* display field, view the current organization in which the Group will be created.

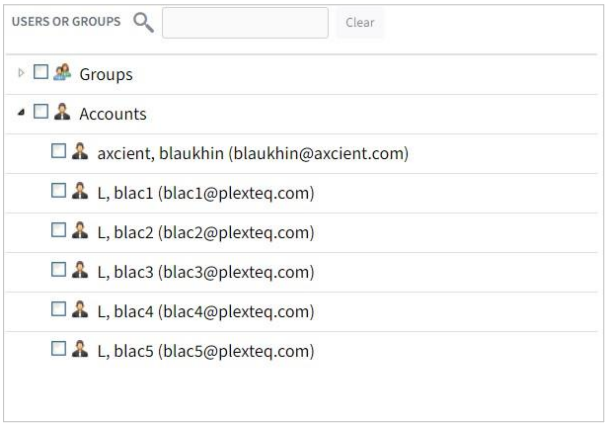
b. In the *Group Name* field, enter a **descriptive name** of the Group. The name will be used as an identifier to help you manage the Group.

c. In the *Group Members* section of the page, select **accounts** or other **Groups** that should be included as members. You can:

   a. Use the *search box* to search for existing Groups or accounts.

   b. Click to expand the *Groups* section, and use the checkboxes to select existing **Groups**. Alternatively, select the top-level **Groups** checkbox to include all Groups.

   c. Click to expand the *Accounts* section, and use the checkboxes to select existing **user accounts**. Alternatively, select the top-level **Accounts** checkbox to include all accounts.



d. Click the **Save** button when you are finished.

After you create Groups, you can add Groups to Team Shares.

How to Manually Create Guest Accounts

In addition to collaborating and sharing content with internal users, end users can also share files and folders with outside third parties. These outside users are called guests. Guest accounts are intended for users who are not members of an organization. These guest users have limited access to the system, allowing for the sharing of files or folders or for collaboration on specific content.

Guest accounts *can*:

- Access a shared file or folder through the web portal
- Manage their account information and change their passwordGuest accounts

  cannot:

- Utilize the desktop client, WebDAV, or mobile apps
- Subscribe to Team Shares

When an end user sends a secure share to a person outside of your organization, they are automatically creating a guest account within the system, and giving that guest access to the file or folder that was shared. For more information, please reference the End User Guide.

NOTE

End users can only create guest accounts if you have enabled the *Allow Users to Share Files* setting, which can be found in the *Policies* tab. You can also manually create guest accounts using the *Guests* tab inside the web portal. Optionally, these guest accounts can be turned into standard user accounts, if necessary.

TIP

You can use guest accounts to replace the use of an FTP server as a file-sharing tool.

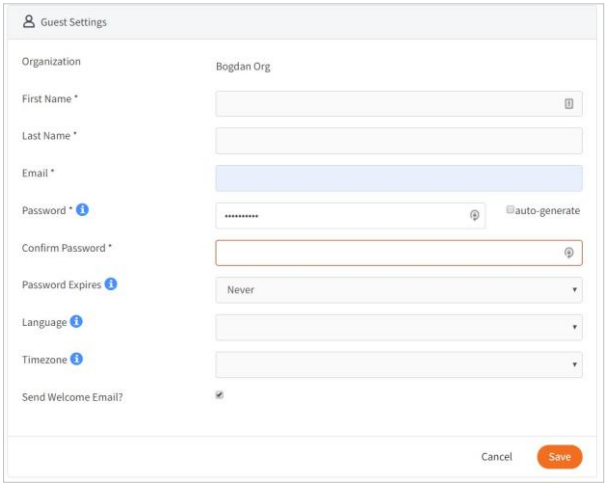
To manually create guest accounts:

1. In the *Organization* navigation menu, select the organization in which you want to manually create guests. The selected organization displays.
2. Click the *Accounts* tab, and and then click the **Guests** button. The *Guest Accounts* page displays, listing all of your existing guests.
3. In the *Guest Accounts* page, click the **Create Guest Account** button.

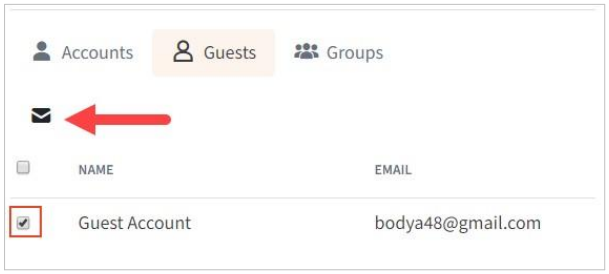
   The *Guest Settings* page displays.
4. In the *Guest Settings* page, enter information about the guest account, including:
   a. In the *First Name* field, enter the user's **first name**.
   b. In the *Last Name* field, enter the guest user's **last name**.
   c. In the *Email* field, enter the guest user's **email address**.
   d. In the *Password* field, enter **password credentials**; alternatively, click the **Auto-Generate** checkbox to allow the system to automatically generate a password for the guest user. The user will be prompted to change an automatically generated password when he or she first logs in to the web portal.
   e. In the *Confirm Password* field, retype to confirm the **password** if it was manually typed into the *Password* field.
   f. Use the *Password Expires* field if you would like to generate a time-sensitive password for the new guest user. You can select from 6 hours, 12 hours, or 24 hours. If you do not want to generate a time-sensitive password, leave this drop-down field set to Never.
   g. In the *Language* drop-down menu, select the user's preferred **site language**, which also affects numbering formats. Leave this field blank to use the default language set for the organization, which you will see displayed when you hover over the blue Question icon.
   h. In the *Default Timezone* drop-down menu, select the user's **preferred timezone**, which affects dates and times displayed across the system. You can also leave this field blank to use the system default, which you will see displayed when you hover over the blue Question icon.
   i. By default, the *Send Welcome Email* checkbox is selected, which will send a welcome email to the new guest, containing information about how to access the system. Uncheck this checkbox if you do not wish to send a welcome

email. This option is useful when you prefer to fully control messaging at a later time. For example, you might need to complete outstanding administrative tasks prior to inviting guests, like creating Team Shares, rebranding the tool, and so forth. You can then manually send log-in information at a later date.

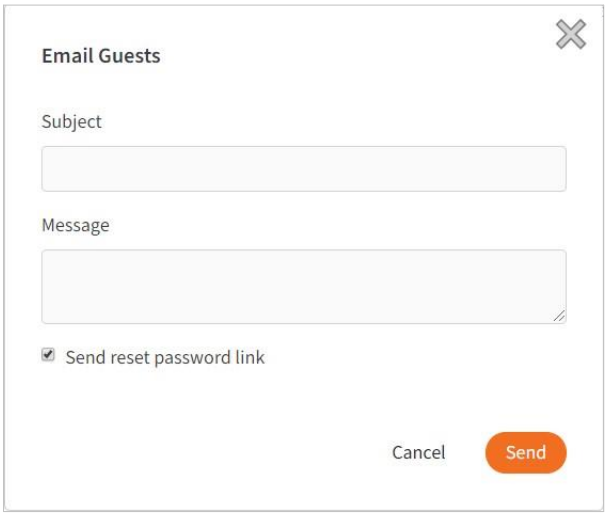
j. Click the **Save** button when you are finished.



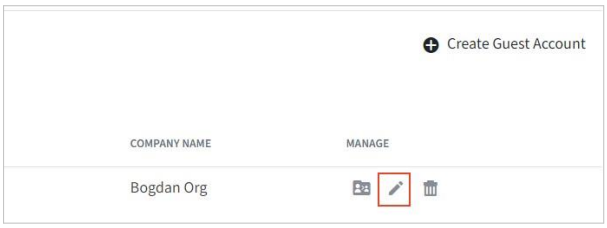
5. When the new guest user is created in the system, the guest user will receive a welcome email with instructions on how to access the system.
6. Optionally, to send a message to a guest user, select the checkbox next to the appropriate account, and click the **Send Message** button.



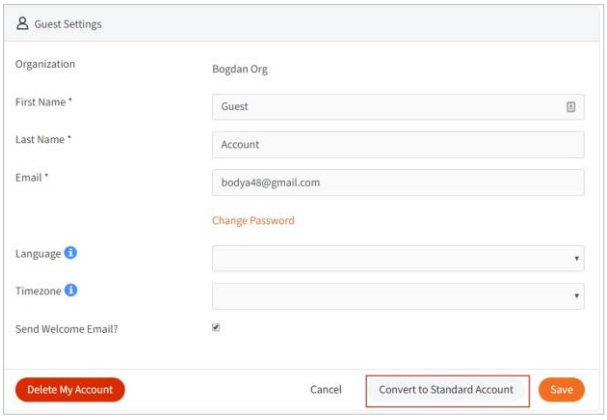
An *Email Guests* dialog box displays, allowing you to compose an email message directly from your web browser. Optionally, click the **Send reset password link** checkbox to provide the selected guest account with a link to reset his or her password.



7. Optionally, convert a guest account to a standard user account.
   a. To convert a guest account to a standard user account, click the **Edit** button.



   The *Guest Account Settings* page displays, allowing you to edit the guest account.
   b. In the *Guest Account Settings* page, click the **Convert to Standard Account** button.



   You will be asked to confirm this change.
8. In the *Guest Accounts* page, you can optionally delete a guest account by clicking the **Delete** button.

How to Manage Machines

When new end users receive their welcome email, they are often provided a direct link to download file sync tools, including the desktop client and device-specific apps. Alternatively, end users can access links to download tools from the web portal. For more information, please reference the End User Guide.

When end users install desktop clients, they are asked to register the desktop clients to their user accounts. These registered devices are listed as *machines* in the administrative web portal. When a machine (such as a computer or a mobile device) is attached to a user account, you can track and manage these machines by clicking the *Machines* tab in the administrative web portal. In the *Machines* page, you can view a list of machines, see the user accounts that are attached to the machines, and view logs for each machine.

In addition to these tasks, you can also use the *Machines* page to unlink machines from user accounts. Unlinking machines from user accounts is helpful in instances when end users lose a device, and you want to prevent unauthorized access to the system.

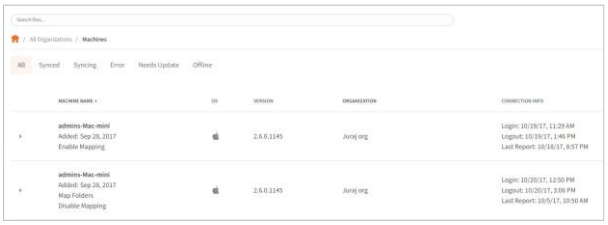
NOTE

The remote wipe process will not initiate while the desktop client is offline. When the desktop client comes back online, it will then complete the remote wipe process.

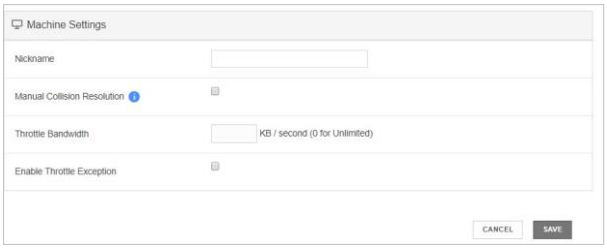
Managing Machines

Use the *Machines* page to manage machines and track issues.

1. In the *Organization* navigation menu, select the organization in which you want to manage machines. The selected organization displays.
2. Click the **Machines** tab. The *Machines* page displays, showing a list of all machines in the selected organization.



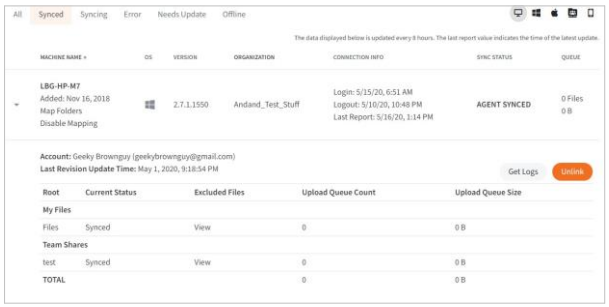
3. You can use the columns to track machine status. For example, the *Connection Info* column displays information that will help you understand connection history of the specific machine. You can also use the visual indicators in the *Status* column to understand each desktop client's current sync and backup status
4. Click the **name** of a machine. The *Machine Settings* page displays for the selected machine, allowing you to manage machine settings.
   a. In the *Nickname* field, you can give the machine a **short name** to help you identify it in the system.
   b. Optionally, deselect the **Manual Collision Resolution** checkbox to disable manual collision resolution. In most instances, it is recommended that you enable manual collision resolution. You can optionally turn off the manual collision resolution feature on machines that are not monitored daily (for example, file servers).
   c. In the *Throttle Bandwidth* field, enter specific throttle **bandwidth settings** to help regulate traffic and minimize bandwidth congestion. You can also configure this field for an entire organization using policy settings.
   d. Select the **Enable Throttle Exception** checkbox to configure times when bandwidth throttling is not enabled for this machine. If you select this option, you will be prompted to specify a time period during which exceptions will be scheduled. You can also configure this field for an entire organization using policy settings.
   e. Click the **Save** button when you are finished.



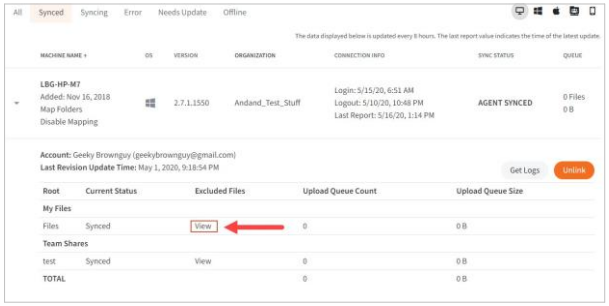
5. In the *Machines* page, you can optionally click the **Enable Mapping** link to set up File Server Enablement.

6. While still in the *Machines* page, click the **drop-down arrow** next to a machine name.

The machine expands to show the associated user account, as well as information about roots (files, Team Shares, and backups), current status, upload queue count, and upload queue size.



7. Optionally, click the **View** link to view excluded files associated with the machine.

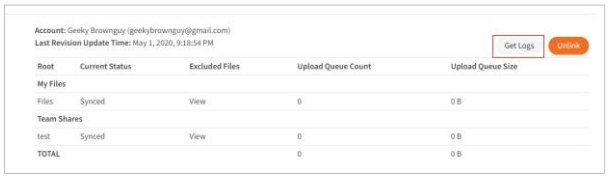


Files that have been excluded from upload will display in a pop-up window.

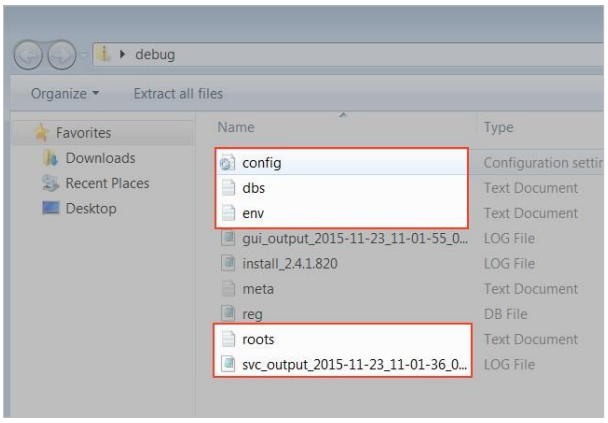
Accessing Log Files

Using the *Get Logs* button, you can troubleshoot desktop client-related issues on Windows or Mac machines.

1. Click the **Get Logs** button to view logs for a machine.



A zip file will download, giving you access to multiple files.



2. Unzip the downloaded folder, and use its contents to troubleshoot issues.
   a. Open *Config.ini* to view key desktop client settings. This file can also be useful as the initial troubleshooting step if a user is unable to register the desktop client, or if the desktop client is not able to connect to the server.
   b. Open *Dbs.txt* and *roots.txt* to view the location of roots created on this desktop client device.
   c. Open *Env.txt* to view information on the system state, running process, and operating system.
   d. Open *Svc_out_<Date-LogID>* to investigate and troubleshoot file sync and other related errors.

Unlinking a Machine (Remote Wipe)

You can also unlink a machine from a user account, which is helpful in the event of a lost or stolen device.

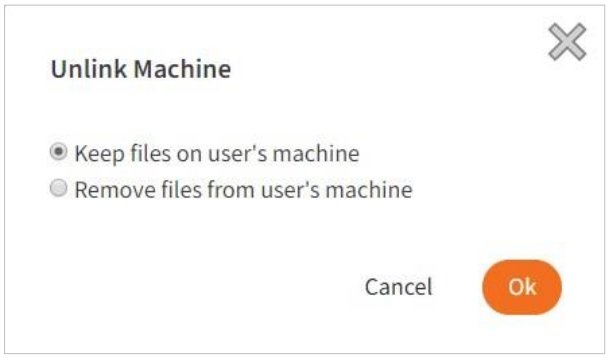
NOTE

Note: The remote wipe process will not initiate while the desktop client is offline. When the desktop client comes back online, it will then complete the remote wipe process.

1. In the *Machines* tab, click to expand the appropriate machine.
2. Click the **Unlink** button to unlink the machine form the user account.

An *Unlink Machine* pop-up window will display.

3. Click the **Keep Files on User's Machine** radio button to keep the files on the user's machine. Alternatively, click the **Remove Files From User's Machine** radio button to remove the files from the user's machine.

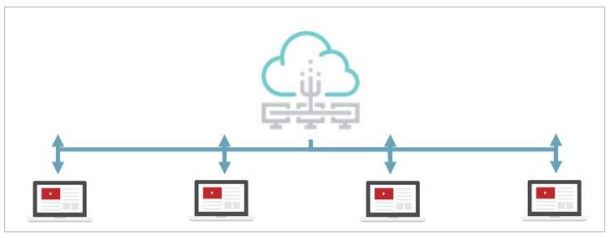


4. Click the **OK** button when you are finished.

How to Manage LAN Sync

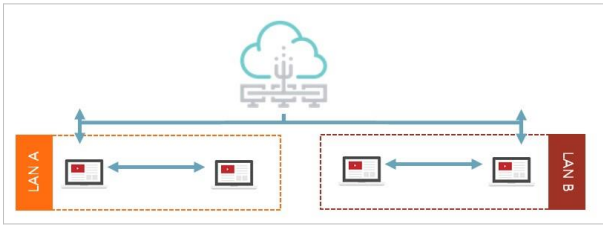
Overview

LAN Sync refers to a file synchronization approach that accelerates the sync process when a Team Share file or folder already exists on a Local Area Network (LAN). Typically, under a standard sync method, when a file is created in a Team Share, each subscribed device begins an individual sync process with the x360Sync Server.



With LAN Sync, when a new Team Share file is created, one desktop client will synchronize with the x360Sync server, and all other desktop clients will synchronize

from one another within the LAN. LAN Sync is a faster and more efficient process, and is particularly useful in environments with limited bandwidth.



NOTE

LAN Sync requires that desktop clients are connected to the x360Sync server; LAN Sync is not intended to support off-line mode.

Bandwidth Information

If bandwidth throttling is configured for a LAN sync-enabled machine, transfers between desktop clients within a LAN will not adhere to bandwidth throttling settings. Only transfers outside of the LAN (between desktop client and server) will adhere to bandwidth throttling settings.

LAN Sync Requirements

- LAN Sync requires that desktop clients are connected to the x360Sync server; LANSync is not intended to support off-line mode.
- Desktop clients must be operating within the same subnet or broadcast address.For example, in a typical office setting, all machines are connected to a single router, and are therefore operating within the same network (subnet). If a LAN uses multiple routers to extend its network, a LAN sync-enabled machine will operate within the network to which it belongs.
- LAN sync requires access to TCP port 16800 and UDP port 16800 to enable communication between desktop clients. The UDP port is responsible for sending data, and the TCP port is responsible for connecting to the recipient and delivering data. The TCP port is encrypted.
- Before LAN sync starts, inbound and outbound firewall rules must be configured toallow access to the appropriate TCP port and UDP port. To prevent conflicts,

please ensure that other applications are not using these same ports (for example, Skype).

LAN Sync Scenarios

End users can turn on the LAN Sync option from the desktop client *Properties* dialog box on their local machines. These end users must also be connected to the x360Sync server and operate within a Local Area Network.

It is important to note that because a desktop client's file only represents its latest revision, the LAN Sync process will take effect when a new Team Share file is created within a LAN. More specifically, LAN Sync will take effect during the following scenarios:

A new file is created within the LAN:	1. A desktop client will synchronize with the x360Sync server. 2. Desktop clients that need the file will synchronize from other desktop clients within the LAN.
A new file is created outside of the LAN:	1. A desktop client will synchronize with the x360Sync server. 2. The new file will be distributed across the LAN. In some instances, the desktop client that synchronized with the x360Sync server will distribute the file, and in other instances, multiple desktop clients will help with the distribution process. The exact process is determined by the load balancer.
A new desktop client joins the LAN:	• The new desktop client will synchronize files from other desktop clients within the LAN.

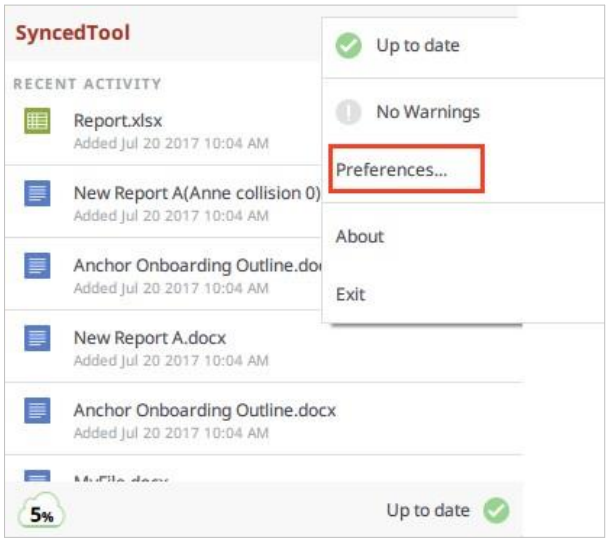
Technical Details

LAN Sync desktop clients communicate with one another through TCP and UDP ports. The TCP port is responsible for reliable data transfer, and is encrypted.

How To Turn On LAN Sync

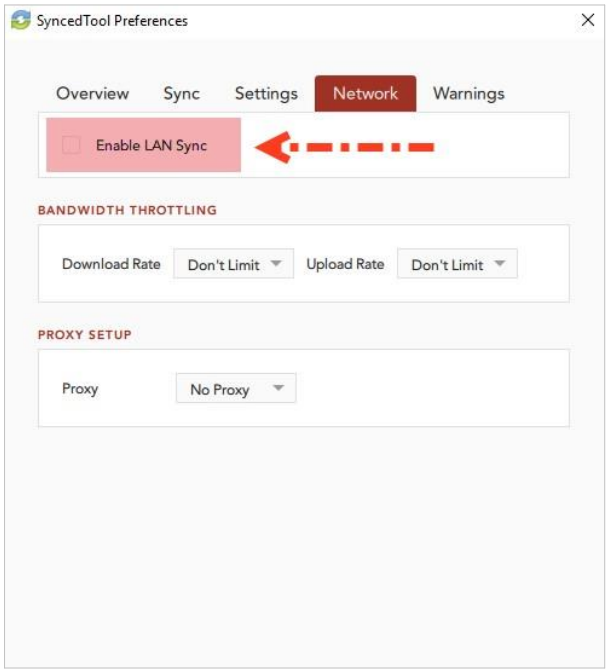
To turn on LAN Sync on a Windows or Mac Machine:

1. In the system tray, click the **Synced Tool** icon, click the **Settings** button, and select **Preferences**.



The *Preferences* dialog box displays.

2. Click the **Network** tab.
3. In the *Network* tab, click the **Enable LAN Sync** checkbox. By default, the checkbox is unchecked.



LAN Sync is now enabled for the desktop client.

Creating and Managing Team Shares and Share Links

In addition to using standard files and folders, end users can collaborate and share content using both Team Shares and share links.

- Team Shares are shared folders that can be accessed by groups of users. TeamShares can be configured for users in your organization; guest accounts cannot be added to Team Shares.
- Share links allow you to share a direct link to a file or folder, rather than sharing anentire area. Share links can be configured for users in your organization and outside of your organization. You can send a *public share* to recipients inside or outside of your organization; alternatively, you can send a *secure share*, which requires login credentials. If you send a secure share to a recipient outside of your organization, the system will create a guest account for that user.

Using the administrative portal, Team Shares and share links can be managed and reviewed.

While end users can create their own Team Shares, and send share links, you can create Team Shares for your end users. Additionally, Team Shares can be configured so that supported Microsoft files automatically lock when they are opened for editing. File locking allows end users to edit files and folders while preventing others from accessing the content at the same time.

NOTE

You might find it useful to set up Team Shares for groups of users who collaborate on a regular basis, such as departments and project teams.

How to Create a New Team Share

How to Create a New Team Share

In addition to working with standard files and folders, end users can work together in shared spaces called Team Shares. Using Team Shares, groups of users—called subscribers—can collaborate on shared content in one central area. Team Shares can

only be configured for users in your organization; guest accounts cannot be added to Team Shares.

End users can create their own Team Shares; alternatively, administrators can create Team Shares for end users. For example, you might create separate Team Shares for each department, or for project teams.

File Locking Feature

To prevent Team Share subscribers from accessing and editing the same file at the same time, you can optionally turn on the File Locking feature, which allows end users to lock files and folders before they begin making changes. For more information on File Locking, please reference the *Managing File Locking and Collisions* section of the Guide.

Permissions

To support the collaboration process, subscribers can be assigned to roles that control their access rights within the Team Share. Roles can be assigned at the Group level, or to individual user accounts.

Roles

The following roles can be assigned to each account or Group subscribed to the Team Share:

- The Co-Owner has total control over content. This role is the best option for administrators.
- The Collaborator (default role) has the ability to seamlessly work with others by creating share links and modifying all content locally and on the web. This role is the best option for team leaders and project managers.
- The Editor is similar to the Collaborator, but without the ability to generate sharelinks. This role is the best option for individual contributors who need to collaborate or modify content locally and on the web.
- The Web Editor is similar to the Editor, but without the ability to download or synccontent locally. Web Editors can edit the content within the Collaborative Web

Editor only. This role is the best option for users who need to collaborate with guests outside of the organization.

- The Viewer is a restricted role, only giving users the ability to view content. This roleis the best option for individual contributors who need to view content locally or on the web, but who do not need to edit content.
- The Previewer is a restricted role, only giving users the ability to preview content inthe web portal. This role is the best option for publishing content externally to the public on the web.
- The Uploader is a restricted role, only giving users the ability to view folder structures (not files) and upload files and folders on the web. This role is the best option for securely requesting content from external parties.

The following table provides a description of each permission type.

Item (File or Folder)	
Owner:	Can change the permission of the file or folder
Trim:	Can trim revisions (delete revisions) of the file or folder
Purge:	Can permanently purge the file or folder
Delete:	Can delete the file or folder
Share:	Can create a share link to the file or folder
Sync:	Can download and sync the file or folder (and folder contents) to devices
File	
View:	Can preview file contents (cannot download or print)
Print:	Can print
Read:	Can download and sync the file to devices
Write:	Can modify the file

Web Edit:	Can modify the file on the web only
Folder	
List:	Can view the list of contents within a folder (does not imply any access to listed files)
Create:	Can create a folder or file within this folder
Delete:	Can delete a folder of file within this folder

Permissions and Windows ACL Settings

Please note that permission roles are enforced based on a user's ACL settings, which ensures the best possible user experience. If you have configured custom ACL permissions for files and folders in a Team Share, permission roles will be updated by x360Sync's desktop client to align them with the user's assigned role.

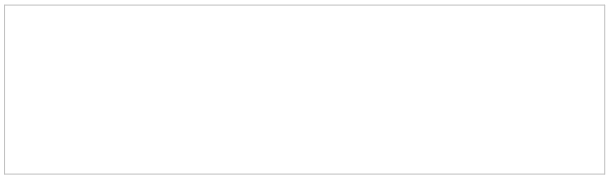
Planning for Team Shares

Before you create Team Shares, it is a best practice to carefully consider how content should be organized and accessed within the system. On one hand, you should consider how groups of users work and collaborate within an organization (through departments, project teams, and so forth). On the other hand, you should also consider the type of content contained in Team Shares.

Content that is contained in Team Shares will sync (and therefore, download) to each subscriber's connected device. If Team Share content does not need to be accessed from each device, you can set subscription rules to help reduce storage and bandwidth requirements.

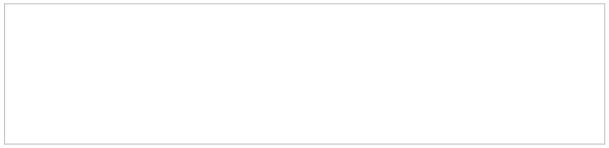
You can select from multiple subscription rule options.

- Web and Mobile—this setting allows Team Share subscribers to access TeamShare content from only the web portal and any registered mobile device.
- WebDAV—this setting allows Team Share subscribers to access Team Share content from the WebDAV interface (a mapped drive connection).
- Future Machines—this setting allows Team Share subscribers to access TeamShare content from all future devices, including the desktop client.

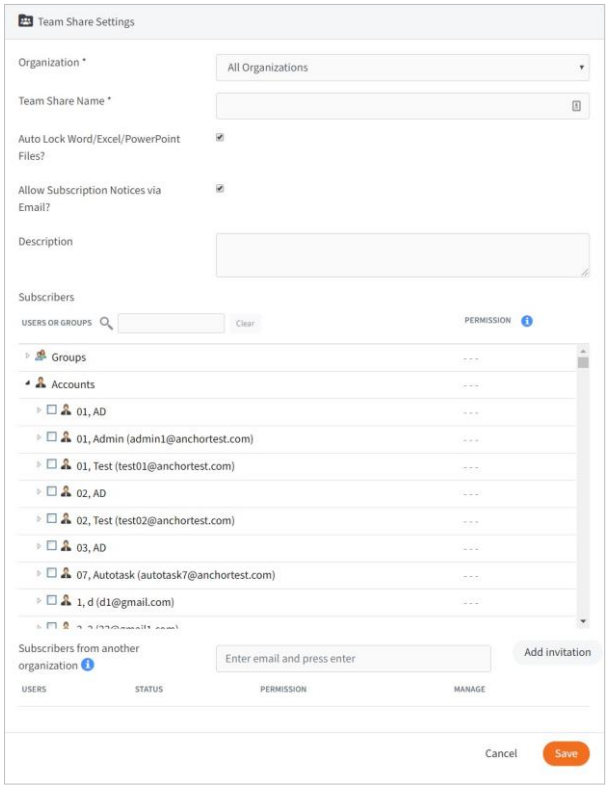


To create a new Team Share:

1. In the *Organization* navigation menu, select the organization in which you want to create the new Team Share. The selected organization displays.
2. Click the **Shares** tab. The *Team Shares* page displays, listing existing Team Shares, if any.
3. In the *Team Shares* page, click the **New Team Shares** button.

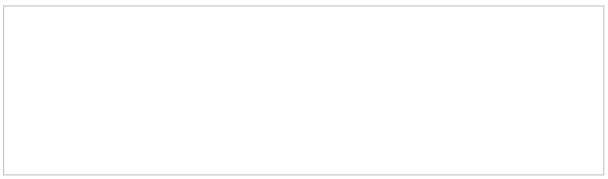
   

   The *Team Share Settings* section of the page displays.

4. In the *Team Share Settings* section of the page, configure the Team Share settings, including:

a. In the *Team Share Name* field, type a descriptive **name** for the Team Share so that it can be easily recognized by subscribers.
b. Select the **Auto Lock** checkbox to enable to the auto locking feature for Microsoft files.
c. Select the **Allow Subscription Notices via Email** checkbox to send email notices when a new subscriber has been added to the Team Share.
d. In the *Description* field, type a **description** of the Team Share. This field is useful for keeping track of information about the Team Share, such as a list of departments that have been subscribed, or how the Team Share is being utilized.
e. In the *Subscribers* box, select the **users** or **Groups** who will have access to the Team Share. End users who have been created for this organization will appear in the *Subscribers* box.
    - Optionally, click to expand a username; you will see a list of machines associated with the user account.



Using the checkboxes, you can specify how the user account can (or cannot) access the Team Share.

i. Click the **Web and Mobile** checkbox to allow the user to access the Team Share from the web portal and any connected mobile device.
ii. Click the **WebDAV** checkbox to allow the user to access the Team Share from the WebDAV interface (a mapped drive connection).
iii. Click the **Future Machines** checkbox to allow the user to access the Team Share from all future devices.

> **Note:** This option affects whether or not a Team Share can be downloaded to a local machine. If the *Future Machines* setting is selected, and the user later registers a desktop client on his or her local machine, then the machine name will appear under this section with a checkmark after it is registered. In this instance, the Team Share will download and appear within user's local Synced Folder after the registration process is complete.
>
> If the *Future Machines* setting is unchecked, and the user later registers a desktop client on his or her local machine, then the local machine name will still appear under this section after it is registered, but without a checkmark. In this instance, the Team Share will *not* download or appear within the user's local Synced Folder.

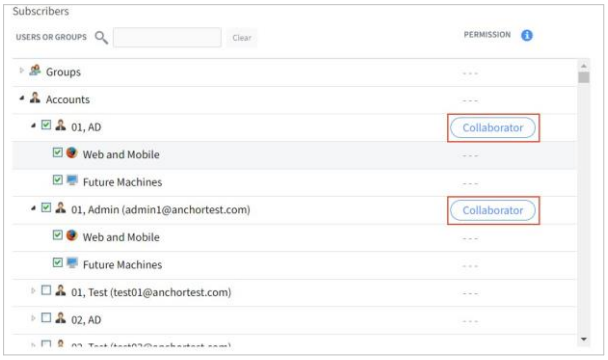
iv. Click the **<Machine Name>** checkbox to allow the user to access the Team Share from his or her desktop client (local machine). This option will only display after the user registers a desktop client on his or her local machine.

v. Click the checkbox next to the user account name to allow the user to access the Team Share from the web portal, WebDAV, and any connected (or future) device.

> **Note:** When all access methods are manually checked, this checkbox will automatically appear as selected. If at least one of the access methods is not selected, the checkbox will appear as a green square.

f. After each group and account has been selected, use the *Permission* column to assign a role at the Group or Account level.

i. By default, each selected subscriber is assigned the *Collaborator* permission. Click the **Collaborator** button to edit the user's permission.

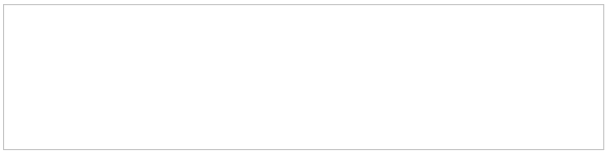


ii. Select the appropriate role for the user. For a description of each role, please reference the table above.

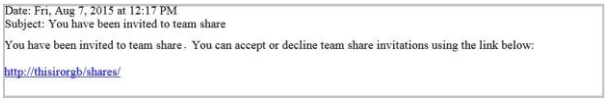
iii. After permissions are set, you can optionally view all roles assigned to the user. For a complete listing of roles, click the **Effective Permissions** button.

g. Optionally, you can also invite outside users to subscribe to this Team Share. These cross-organization subscribers must have an existing account in the system. Enter the **email address** of the registered user account and click the **Add** button. You can then use the *Permissions* column to set specific permissions for each of the invited subscribers.

This option is useful when end users in the same system, but in unrelated organizations, need to collaborate on the same files and folders.



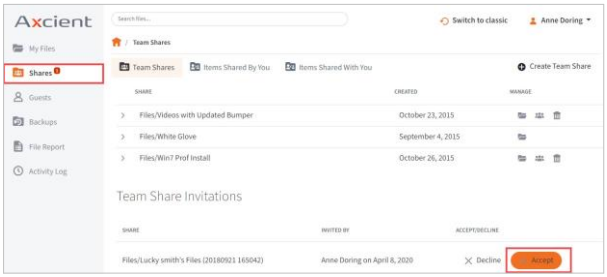
When you click the **Save** button to create the Team Share, the users who were added in the *Invite Subscribers* box will receive an email notification with a link to accept or decline the Team Share invitation.


Date: Fri, Aug 7, 2015 at 12:17 PM
Subject: You have been invited to team share

You have been invited to team share. You can accept or decline team share invitations using the link below:

http://thisirorgb/shares/

The invited subscribers will also see a notification in the *Shares* tab when they log into the web portal. When they click the **Shares** tab, they can review a list of outstanding Team Share invitations and accept or decline as appropriate.



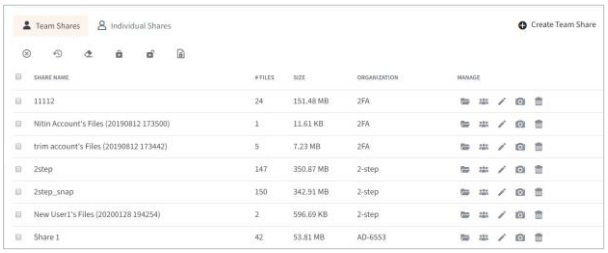
If the subscriber accepts the invitation, you will be able to manage his or her connected devices in the Team Share page.

How to Manage Team Shares

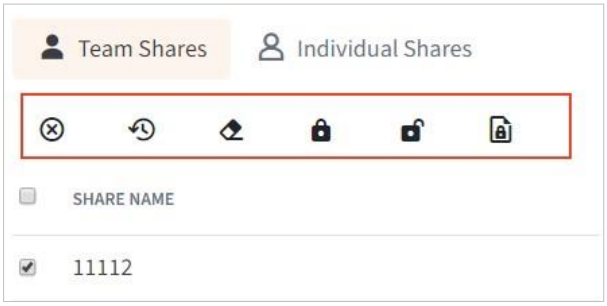
All Team Shares—whether they are created by you or an end user—can be managed by clicking the **Shares** tab in the administrative web portal. In the *Team Shares* page, you can view a list of all Team Shares, manage content in Team Shares, edit subscribers to Team Shares, edit Team Share settings, and deactivate Team Shares.

To manage Team Shares:

1. In the *Organization* navigation menu, select the organization in which you want to manage Team Shares. The selected organization displays.
2. Click the **Shares** tab. The *Team Shares* page displays, listing existing Team Shares.



3. In the *Team Shares* page, you can optionally use the *Search* box to find a Team Share.
4. In the *Team Shares* page, you can also manage individual Team Shares.
   - Click the **checkbox** next to a Team Share. The toolbar will expand to display additional actions.



     a. Click the **Erase Delete Files** button to permanently remove files that have been deleted from the selected Team Share.
     b. Click the **Restore Deleted** button to restore files that have been deleted from the selected Team Share.
     c. Click the **Trim** button to erase previous revisions to files in the Team Share.
     d. Click the **Lock** button to lock the Team Share, so that items in the Team Share cannot be edited.
     e. Click the **Unlock** button to unlock the Team Share.
5. While still in the Team Shares page, click the **Browse** button to browse the content of the selected Team Share.

6. While still in the *Team Shares* page, you can edit subscribers to the Team Share.
   - Click the **Subscribers** button.

   The *Subscribers in This Organization* section of the page displays, allowing you to configure subscribers and update permission settings.

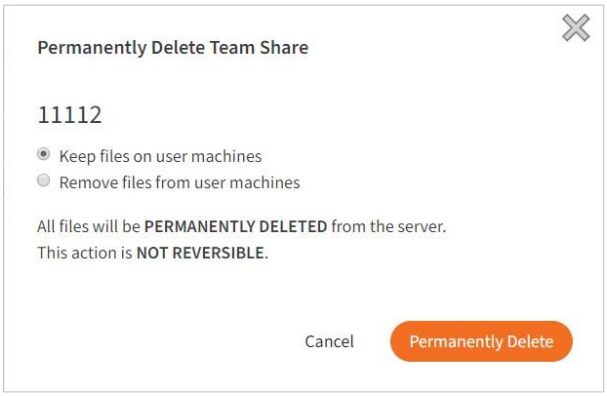
7. While still in the *Team Shares* page, you can edit Team Share settings.
   - Click the **Edit** button.

   The *Edit Share Settings* page displays, allowing you to edit Team Share settings. For more information, please reference the *How to Create Team Shares* section of the Guide.

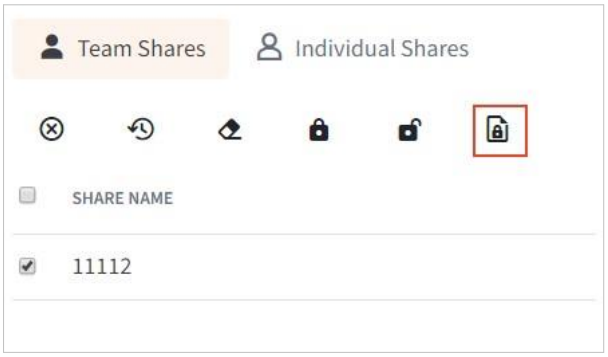
8. Optionally, you can deactivate the Team Share.
   - Click the **Deactivate** button.

   A *Delete Team Share* pop-up window displays.

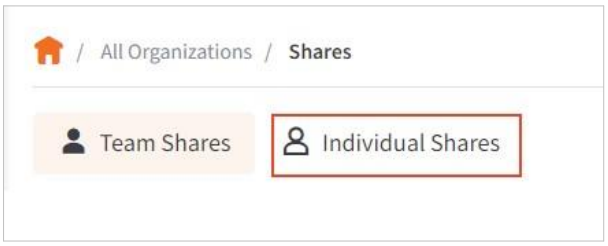
   a. In the *Delete Team Share* pop-up window, click the **Keep Files on User Machine** radio button to keep the Team Share files and folders on the machines registered to the subscribers.
   b. Alternatively, click the **Remove Files from User Machines** radio button to remove the Team Share files and folders from the machines registered to the subscribers.
   c. When you are finished, click the **Remove** button.



9. Click the **Enable Auto Locking** button to enable auto-locking for the selected Team Share. To enable auto-locking, please reference the *How to Enable AutoLocking of Files in Team Shares* section of the Guide.



10. Click the **Individual Shares** button to view a list of individual shares that have been created by end users.

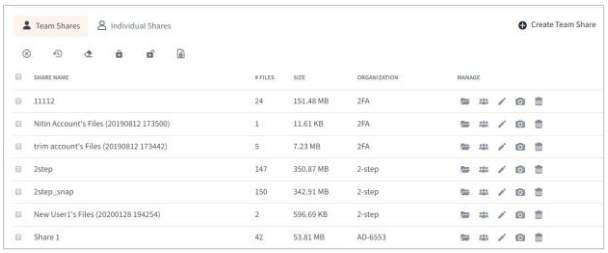


How to Manage Share Links

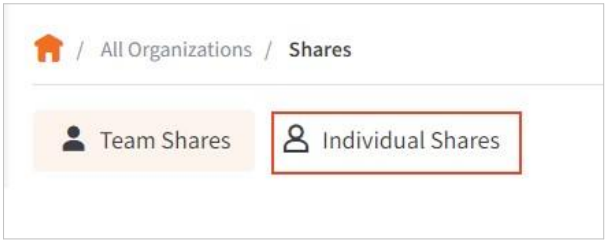
All share links can be managed by clicking the **Shares** tab in the administrative web portal. In the *Team Shares* page, you can view details about share links, including the account that received each share link, the number of views, and the number of downloads. You can also deactivate entire share links, or remove specific accounts from share links.

To manage share links:

1. In the *Organization* navigation menu, select the organization in which you want to manage share links. The selected organization displays.
2. Click the **Shares** tab. The *Team Shares* page displays, listing existing Team Shares.



3. Click the **Individual Shares** button to view a list of share links that have been created by end users.



The page refreshes to show the *Individual Shares* section of the page, displaying a list of share links.

4. In the toolbar, you can search for individual shares using the *Search* field.
5. Use the subscription details area to view details about the individual share, including the account who received the individual share, the number of views, and the number of downloads.
   a. Optionally, click the **Manage** button to view a link to the individual share.

   b. Optionally, click the **Deactivate Share** button to deactivate the individual share.


Team Shares
Individual Shares
SHARED ITEM
VIEWS
DOWNLOADS
SHARED BY
EXPIRES
MANAGE
Files/Uploads/2017-04-14-service-stuck-merging-agent_service.exe_170414_105300.zip 4 8 / Unlimited Kevin Hoffman 2017-10-31
Files/Uploads/2017-04-19-syncedtool-logs.zip 2 0 / Unlimited Kevin Hoffman 2017-05-31
Files/Uploads/ReplibitDrop 0 0 Kevin Hoffman Never

How to Enable WebDAV

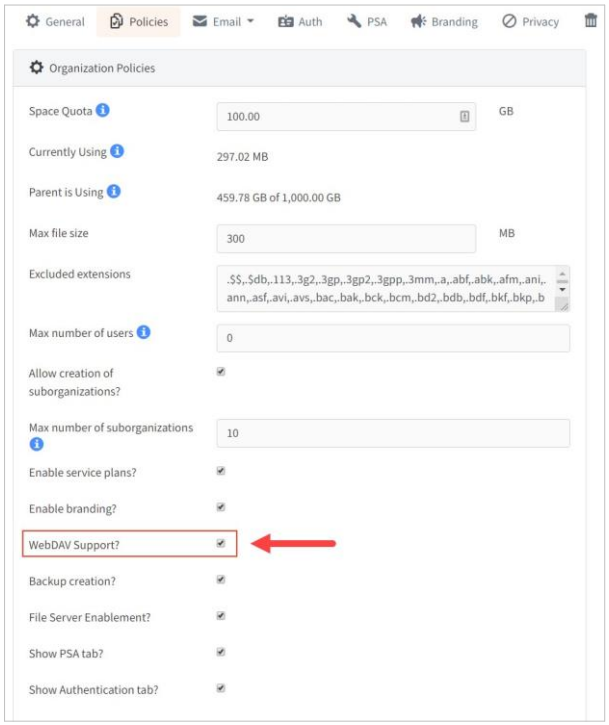
Using WebDAV, your end users can view and edit files located in the cloud. For information on known issues, please reference the *Supporting WebDAV* section of the Guide.

NOTE

For WebDAV to work on Server 2003, you will first have to download this Windows update.

To enable WebDAV for an organization:

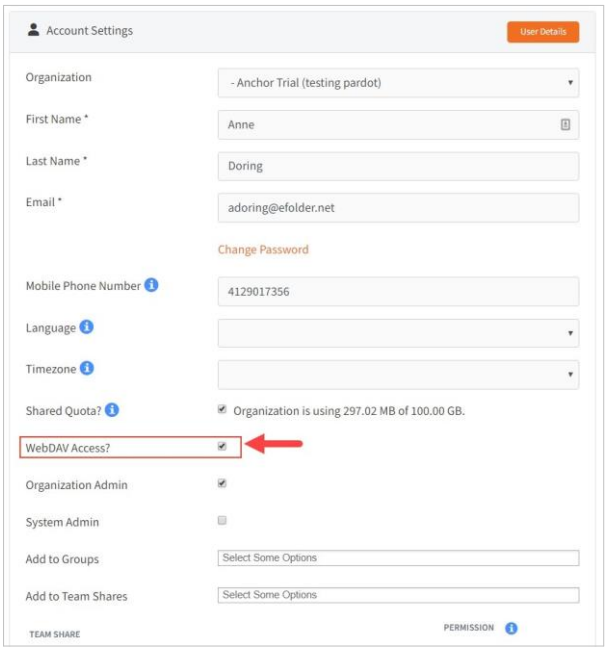
1. Within the appropriate organization, click the **Settings** tab. The *Settings* page displays.
2. In the *Settings* page, click the **Policies** tab. The *Policies* page displays.
3. In the *Organization Policies* section of the page, click the **WebDAV Support** checkbox.



4. Click the **Save** button when you are finished.

To enable WebDAV for individual user accounts:

1. Within the appropriate organization, click the **Accounts** tab. The *Accounts* page displays.
2. In the *Accounts* page, find the appropriate user account, and click the **Edit** button.
   The *Account Settings* page displays.
3. In the *Account Settings* page, click the **WebDAV Access** checkbox.



4. Click the **Save** button when you are finished.

When end users connect to WebDAV, they can enter the address listed in the *Hostname* field found in the *Settings* tab. Alternatively, when working in a dual hostname environment, they can enter the address listed in the *App Server Hostname* field. For information on mapping a drive on a local machine, please reference the End User Guide.

Supporting WebDAV

x360Sync supports Web Distributed Authoring and Versioning (WebDAV), which is an extension of the HTTP protocol. WebDAV is another way for end users to view and edit files—both personal and through team shares—located in the cloud.

NOTE

For private cloud environments, existing Certificate Authority signed SSL certificates must be modified to allow for WebDAV functionality. For more information, please reference Configuring your x360Sync Server for WebDAV Support [43].

Benefits

Benefits of using WebDAV include:

- End users do not need to install desktop clients
- Shared files are not stored locally
- Folders and files are accessible through the end users' native explorer (for example,a mapped drive in Windows explorer)
- Authentication through Active Directory login credentials is supported
- The ability to enable WebDAV for all users of a given organization, or on a user-by-user basis

Limitations and Expected Behaviors

While WebDAV can provide a number of benefits for an organization, it is important to note that WebDAV is an extension of the HTTP protocol, and is unrelated to the x360Sync system. Some of its limitations and known issues may be not be controlled by the x360Sync support team.

WebDAV and x360Sync's Context Menu

When working through WebDAV, end users will not have access to x360Sync's rightclick context menu. Without the right-click context menu, end users will not be able to lock files, create a share link, launch the web portal, or view file revisions from their local machines. This is expected behavior, and is not related to the x360Sync service.

WebDAV and x360Sync's File Locking Feature

When using x360Sync's file locking feature, errors may occur when accessing and saving files through WebDAV. This is an expected behavior, and is due to the fact that

file permissions cannot be changed by x360Sync through WebDAV, but will be honored when the file is saved on the server. For example, if User A locks a file through the web portal, and User B accesses the same locked file through WebDAV, User B will be able to access the locked file and make changes. However, when User B attempts to save the file in WebDAV, an error will display, and the changes will not be saved.

Multiple Login Prompts

In some instances, end users might be prompted to log in each time they open or save a Microsoft 365 file while working in WebDAV. While the x360Sync support team cannot prevent Microsoft 365 from prompting for credentials, it might be possible to configure Microsoft 365 so that end users do not have to enter credentials each time they open or save files in a mapped drive. For more information on this issue and a potential workaround, please reference the x360Sync Knowledgebase.

Other Known Issues

Other known WebDAV issues have been noted related to accessing files through WebDAV. For example:

- Uploading large files (over 100 MB) might fail (refer to this Technet article for more information)
- Microsoft Word files might open in Read-only mode (refer to this TechCenter discussion for more information)
- WebDAV might disconnect at random intervals
- WebDAV might fail to restore mapping after rebooting the operating system
- WebDAV might not behave as expected when certain Microsoft Windows patchesare applied to local machines

These known issues are not related to x360Sync, but might be connected with one of the following:

- Security such as firewalls, packet sniffing, deep packet inspection, intrusion prevent-ing, and so forth
- Unstable internet connection at the client's site
- Microsoft and Mac clients poorly handling the WebDAV connection

In some instances, you might see improved performance when using a third-party application (such as Cyberduck or WebDrive) to replace MS Explorer or Mac Finder. Please note however, that these third-party applications are not supported by the x360Sync support team.

Managing File Locking and File Sync Warnings

x360Sync allows users to place locks on files and folders in Team Shares, giving subscribers the ability to set read-only permissions on shared content. This feature prevents other Team Share subscribers from editing and overwriting content while changes are being made. Users can place locks on a whole Team Share, a subfolder in a Team Share, or a file in a Team Share. When an item is locked, a lock icon is placed over the file or folder, alerting other Team Share subscribers that it is in readonly mode. Administrators have the ability to unlock any file or folder. Locks are enforced across desktop clients, the web interface, and mobile devices.

Benefits

The file locking feature is useful when an end user wants to prevent other user accounts from accessing items when changes are being made, preventing file sync warnings. Additionally, this feature allows for the creation of read-only Team Shares. For example, you can create a read-only Human Resources Team Share that houses employee forms and policies; end users can read and download files, but cannot edit or delete files.

Configuration Options

To give end users the ability to lock files, you must first turn on the File Locking policy for an organization within the Policies page of the Settings tab. Administrators can configure the file locking feature in a number of ways, depending on the needs of the individual organization.

For example:

- Administrators can decide to turn on or off the *Auto Lock* feature for individual Team Shares.

  When the *Auto Lock* feature is turned *on* for Team Shares, subscribers are automatically prompted to lock supported Microsoft files each time they are opened. If this feature is turned *off*, users must remember to manually lock and unlock files and folders using the desktop client's right-click context menu.

- Administrators can configure the *Use Filesystem Permissions* policy to determine whether locks are *hard* or *soft*.

  When *hardlocks* are configured, the desktop client changes the NTFS permissions on Windows, or HFS Plus permissions on Mac, in order to prevent changes by other users. These permissions allow for a much stronger lock, and are especially important for File Server Enablement environments where mapped drive users must be notified by the filesystem when a file is in use.

  A *soft lock* does not utilize NTFS permissions or HFS Plus permissions, and instead allows a user to make changes to his or her local copy.

TIP
In most instances, it is recommended that administrators enable hard locks and turn on the *Auto Lock* feature for Team Shares. This configuration ensures the best possible user experience, and helps prevent file sync warnings.

Expected Behavior

- This feature applies to .doc, .docx, .xlsx, .ppt, and .pptx files. This feature also applies to .xls, .odt, .ods, and .odp documents if the documents are opened with LibreOffice or OpenOffice.
- This feature is not supported for *Word for Mac* and *.xls* files opened with Excel.
- This feature is only accessible from the desktop client installed on local machines.

Locking and File Server Enablement

If a Team Share has been mapped to a file server through File Server Enablement, locks *will* be honored both in the Team Share and on the file server. If NTFS permissions are modified on the file server, however, these modifications *will not* be honored in the Team Share.

Additionally, when you specify a network path as a source for File Server Enablement, the content on the network path *will not* support the *Auto Lock* feature.

File Sync Warnings

If an end user does not utilize the File Locking feature, he or she might encounter a file sync warning. End users are responsible for resolving their own file sync warnings. Two different file sync warnings can occur if end users do not utilize the file and folder locking feature:

- Collision—A collision occurs when one file is modified in two different places at thesame time. When this happens, only one of the revisions will successfully sync to the server, and the other revision will be marked as a collision. For example, User A and User B both open the same file from two separate locations, without locking the file. User A edits and saves her file, and this new revision is synchronized to the server. User A edits and saves her file again, and this updated revision is again synchronized to the server. User B is now editing an older revision of the file. When User B saves his revision of the file, it will *not* synchronize to the server, and will instead be marked as a collision.

  You can optionally turn off the manual collision resolution feature on machines that are not monitored daily (for example, file servers). For more information, please reference the *How to Manage Machines* section of the Guide.
- Locked Change Warning—A locked change warning occurs when a user attemptsto modify a file that has been previously locked by another user, either at the file level or the folder level. For example, User A locks a file and the file is marked with a lock icon. Later, User B opens the file, ignoring the lock icon, and begins modifying the file. When User B attempts to save his revision, it does not immediately synchronize with the server, and is instead marked as a locked change warning. When User A unlocks the file, User B's revision will automatically synchronize to the server without any additional action on his part. This type of file sync conflict only occurs if hard locks have not been enabled through policy settings.

Allowing End Users to Overwrite Collisions

By default, when an end user encounters a collision, he or she is able to resolve the collision by either renaming or deleting their own local copy of the file.

In addition to these two default options, you can optionally turn on the *Allow Users to Overwrite Collisions* policy, which allows end users to resolve collisions by syncing

their own local copy as the latest server revision. For more information, please reference the *How to Update Polices for an Organization* section of the Guide.

For more information on how end users resolve their own collisions, please reference the End User Guide.

Monitoring File Sync Warnings

Important desktop client events—including collisions and collision resolutions—are visible within the Windows Event Viewer and the OS X Console utilities, allowing you to proactively track activity and address issues that directly affect end users.

Within the Windows Event Viewer, the following events can be found in the Application section, and are categorized at the Information level. The Source of these events is listed as the name of the branded desktop client.

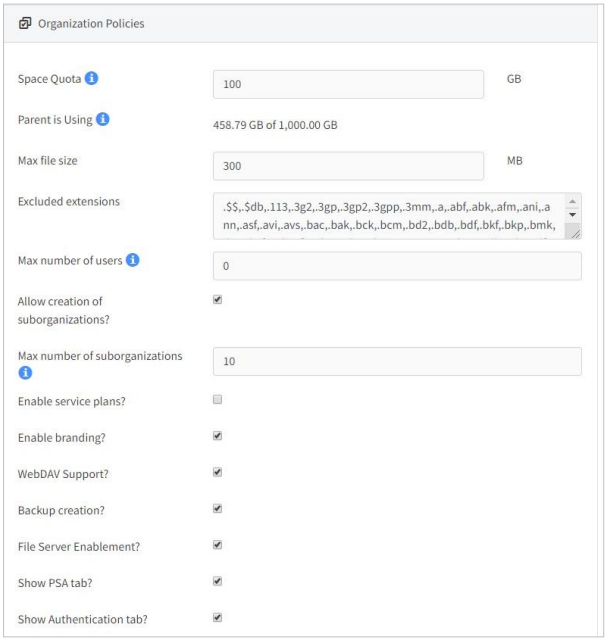
Event Type	Description	Event ID
Service Start	The desktop client service is starting.	512
Collision Created	A collision is logged.	768
Collision Resolution	The collision is resolved.	769
Collision Failed	A collision was logged, but the conflicting content disappeared while attempting to resolve. Please contact Axcient Support.	770
Collision Message	A message has been generated in relation to a collision event.	771

How to Turn File Locking On and Off

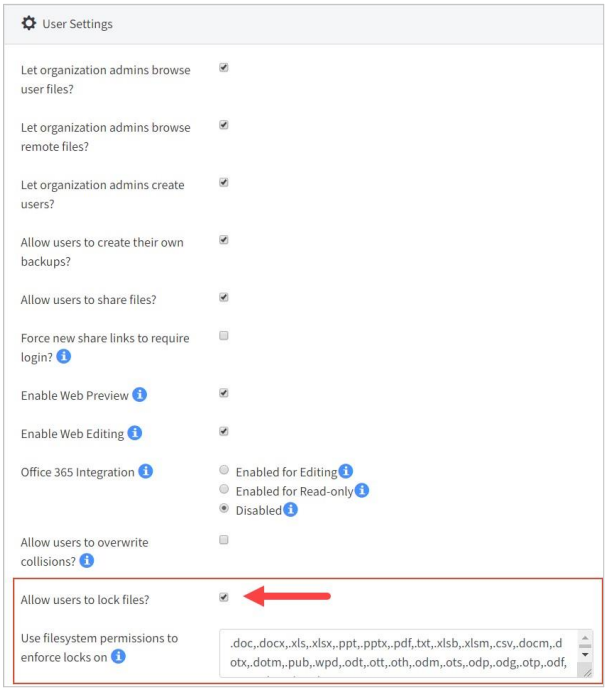
By default, the File Locking policy is turned on. In most cases, it is a recommended best practice to allow end users to lock and unlock files and folders within Team Shares. This feature is useful when an end user wants to prevent other user accounts from editing and syncing items when changes are being made, preventing sync collisions from occurring. This setting can be changed in the *Policies* tab of the administrative web portal.

To turn file locking on or off:

1. In the *Organization* navigation menu, select the organization in which you want to manage file locking. The selected organization displays.
2. Click the **Policies** tab. The *Organization Policies* section displays, showing organization policies that were configured when the organization was created.



3. In the *User Settings* section of the page, check the **Allow Users to Lock Files** checkbox to allow end users to lock and unlock files and folders.



End users will now have the ability to lock and unlock files and folders.

4. Optionally, edit the extensions listed in the *Use Filesystem Permissions to Enforce Locks On* field. This field allows you to specify extensions on which you would like the desktop client to enforce locks through filesystem permissions (also called hard locks). This field is especially important for File Server

Enablement environments where mapped drive users must be notified by the filesystem when a file is in use.

When a lock is placed, the desktop client will change the NTFS permissions on Windows, or HFS Plus permissions on Mac, in order to prevent edits by other users.

On Windows, hard locks are implemented by setting the following DENY ACE for the EVERYONE SID:

- Create files/write data
- Create folders/append data
- Write attributes
- Write extended attributes
- Delete

On OS X, the UF_IMMUTABLE flag is set (essentially a user lock).

How to Enable Auto-Locking for Files in a Team Share

Overview

In addition to allowing end users to lock and unlock files within Team Shares, you can set up Team Shares so that certain files automatically lock when they are opened for editing. This feature is a best practice, as it prevents collisions from occurring, especially in shared folders with many subscribers. When files are closed, they automatically unlock.

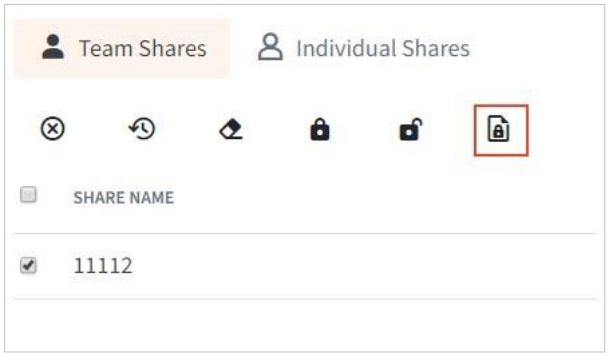
Expected Auto-Locking Behavior

- This feature applies to .doc, .docx, .xlsx, .ppt, and .pptx files. This feature also applies to .xls, .odt, .ods, and .odp documents if the documents are opened with LibreOffice or OpenOffice..
- This feature is not supported for *Word for Mac* and *.xls* files opened with Excel.
- This feature is only accessible from the desktop client installed on local machines.

To enable auto-locking in a Team Share:

1. In the *Organization* navigation menu, select the organization in which you want to manage auto-locking. The selected organization displays.
2. Click the **Shares** tab. The *Team Shares* page displays, listing existing Team Shares.

3. Click the **Enable Auto Locking** button to enable auto-locking for the selected Team Share.



A pop-up window displays in your browser, prompting you to confirm your selection. Auto-locking is now enabled for the selected Team Share.

How to Disable Manual Collision Resolution

When an end user forgets to lock a file or folder before making changes, instances might occur where another user has made changes to the same item at the same time. This is called a collision. By default, when a collision occurs, the system will notify the end user of the conflict with a *Need User Action* message, allowing the end user to resolve the collision in one of three ways.

- *Rename My revision*: The copy is renamed to include the term *collision* appended to the end. When this option is selected, you will see two files: the *original_file_name* file and the *original_file_name_collsion* file.
- *Discard My revision*: The copy will be discarded without its changes being saved.

- *Open Folder*: This option will open the location of the file, allowing end users to view the file before making a decision.

For more information on resolving collisions, please reference the End User Guide.
In some instances, you might want to disable this manual collision resolution process; for example, this option if useful for file servers, or for machines that are not constantly monitored by end users.

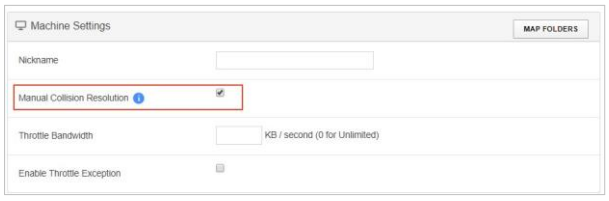
TIP

It is considered a best practice to allow for manual collision resolution. Only in special circumstances—such as when a machine is not being monitored—should you consider turning off this feature.

To disable manual collision resolution for a machine:

1. In the *Organization* navigation menu, select the organization in which the specific machine resides. The selected organization displays.
2. Click the **Machines** tab. The *Machines* page displays, showing a list of all machines in the selected organization.

3. Click the **name** of the machine. The *Machine Settings* page displays for the selected machine.
4. In the *Machine Settings* page of the selected machine, uncheck the **Manual Collision Resolution** checkbox, and click the **Save** button.



Manual collision resolution has now been disabled for the selected machine.

Creating and Managing Backups

End users can create backups of files and folders that exist on their local machines. Alternatively, you can create backups of files and folders for your end users.

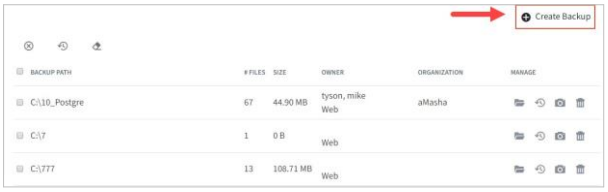
When you or end users create a backup of a file or folder, all new changes are continuously backed up. The backup can be accessed from the web portal, but it does not reside in Synced Folder, and it cannot be shared.

How to Create a New Backup

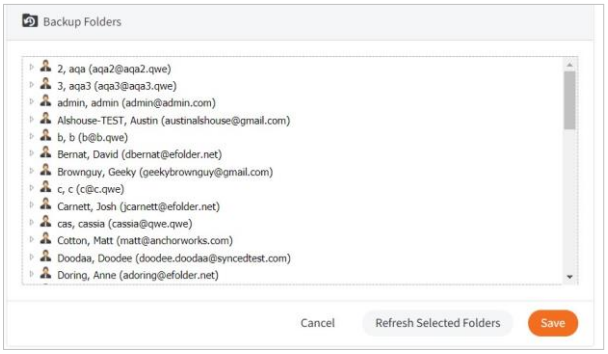
You can create backups of files and folders within registered machines.

To create a backup:

1. In the *Organization* navigation menu, select the organization in which you want to create backups. The selected organization displays.
2. Click the **Backups** tab. The *Backups* page displays, showing a list of all existing backups in the selected organization.
3. In the *Backups* page, click the **New Backup** button.



The *Backup Folders* page displays, listing all registered machines within the selected organization.



4. Click to expand a machine name, and select the specific folder that you want to back up.

5. After the item has been selected, click the **Save** button. The selected item is now backed up.

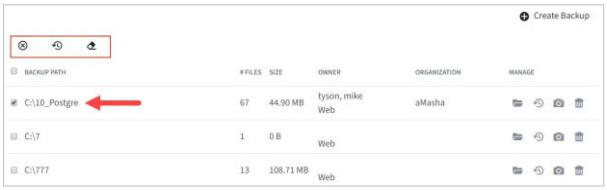
How to Manage Backups

You can manage all backups—whether they were created by you or end users—by clicking the **Backups** tab. In the *Backups* page, you can manage the content of backups, browse the content of backups, and delete backups.

When a user account is deleted from the system, the backup will deactivate, but will still be accessible in the *Backups* tab of the administrative web portal.

To manage backups:

1. In the *Organization* navigation menu, select the organization in which you want to manage backups. The selected organization displays.
2. Click the **Backups** tab. The *Backups* page displays, showing a list of all existing backups in the selected organization.
3. In the *Backups* page, find the backup that you want to manage. Optionally, use the *Search* box to search for a backup using the owner's name.
    a. Click the **checkbox** next to a backup. The toolbar will expand to display additional actions.

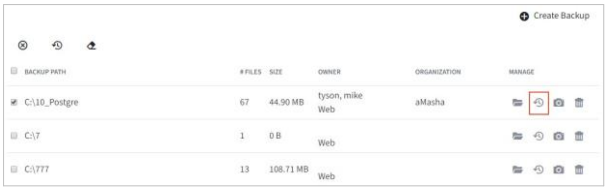


    b. Click the **Erase Deleted Files** button to permanently remove deleted files in the selected backup.
    c. Click the **Deactivate Selected Backups** button to remove the backup.
    d. Click the **Restore Deleted** button to restore the contents of the backup to a specified location.
    e. Click the **Trim** button to erase previous revisions to files in the backup.
4. While still in the *Backups* page, you can browse the contents of the backup.
5. Click the **Browse** button.

The backup opens, allowing you to browse its content.

6. Inside the backup, you can:
   a. Click the **Create Folder** button to create a new folder inside the backup.
   b. Click the **Upload Files** button to add files to the backup.
   c. Click the **Rollback** button to restore all files within the entire folder to an earlier revision before a selected date. The Revision Rollback feature is particularly useful in situations where a file might have been corrupted by ransomware; it utilizes a file's revision history, and restores all currently-existing content in the folder to a healthy revision at a specified point-in-time. In these cases, you can use the Activity Log to determine when the infected revisions were uploaded, and then roll back files prior to the point of infection.
   d. Click the **Show Deleted** button to show files that have been deleted within the backup
   e. Click the **Restore Deleted** button to return any deleted files to the backup.
   f. Click the **Trim** button to erase previous revisions to files in the backup.

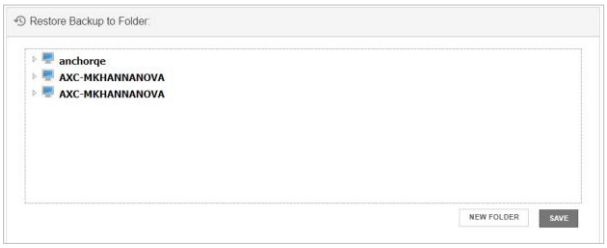
7. In the *Backups* page, you can restore a backup to a specific location. You can also restore a backup to a different machine, as long as a desktop client is installed on that machine.
   a. Click the **Restore** button.



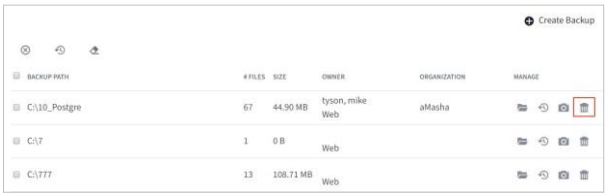
A *Restore Backup* page displays.

b. In the *Restore Backup* page, browse the selected machine to select a restore point. Optionally, click the **New Folder** button to create a new folder as a restore point.

c. Click the **Save** button when you are finished.



8. Optionally, in the *Backups* page, click the **Delete** button to delete a backup.



The backup will delete from the selected machine.

Managing and Monitoring x360Sync

In addition to managing and sharing files and folders, organization administrators can also keep track of file listings and activity directly from the administrative web portal. Additionally, you can create reports and schedule recurring reports.

With the activity log, you can track all usage across the system, view audit trails, and track activity on Team Share users and guest accounts. Use the *Activity Log* page in the administrative web portal to filter activity based on a set of criteria.

With reports, you can view various activities within the system, and export the report to your local machine. Use the *Reports* page in the administrative web portal to generate these reports.

How to Monitor Activity

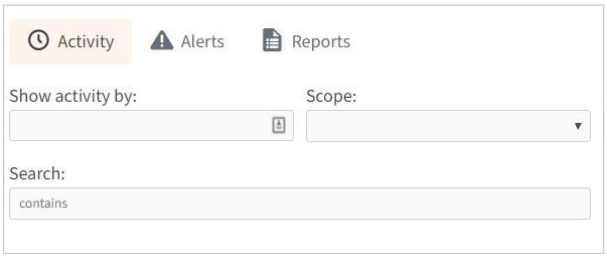
With the activity log, you can track all usage across the system and create alerts on accounts, data usage, machines, roots, organizations, and guests. Use the *Activity Log* page in the administrative web portal to filter activity based on a set of criteria.

To monitor activity in the Activity Log:

1. In the *Organization* navigation menu, select the organization in which you want to monitor activity. Alternatively, click the top-level organization to view all activity across all organizations.
2. Click the **Activity** tab. The *Activity Log* page displays.

3. Use the Activity Log filters to filter activity.
   a. Use the *By* field to filter activity performed by a specific account, including administrators, user accounts, and guest accounts.
   b. Use the *Scope* drop-down field to filter activity by a certain item type. For example, select *Organization* to view activity related to an organization.

c. Use the *Search* field to filter based on the name of the specific item that you want to track. For example, if you previously selected **Organization**, type of the **name** of the organization you want to review.



d. To browse activity by date, select the specific **start** and **end** dates.

How to Create Activity Alerts

In addition to tracking usage, you can use the *Activity Log* page to create alerts so that you are notified when these events occur. These alerts help you stay informed of important events that take place within the system.

For example, at the very minimum, it is recommended that you create a few important alerts, including:

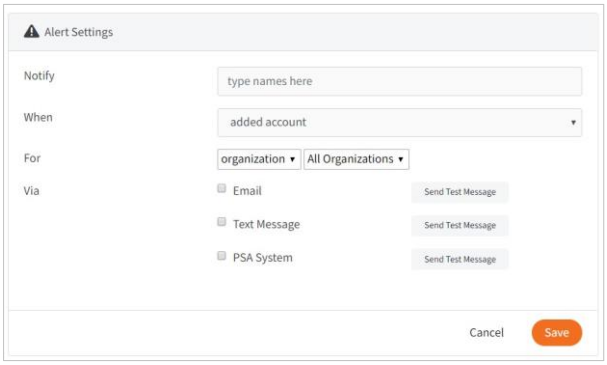
- An organization reaches a certain percentage of its quota
- Email server settings have been modified• A File Server Enablement

  machine is unreachable To create activity alerts:

1. In the *Organization* navigation menu, select the organization in which you want to create an activity alert. The selected organization displays.
2. Click the **Activity** tab. The *Activity Log* page displays.
3. In the *Activity Log* page, click the **Alert** tab and then click the **Create Alert** button.

The *Alerts* page displays.

4. In the *Alerts* page, configure alert settings.
   a. In the *Notify* field, enter the **names** of users who should receive the activity alert. The field will populate as you type, based on the characters that you enter.
   b. In the *When* drop-down menu, select the **action** that will trigger the alert.
   c. In the *For* field, enter the **actor** (organization or user) that will trigger the alert, depending on which setting you selected in the *When* drop-down field.
   d. In the *Via* field, enter your preferred **method of delivery**. Optionally, click the **Send Test Message** button to test the delivery method.
   e. Click the **Save** button when you are finished.



The activity alert is now configured.

How to Create Reports

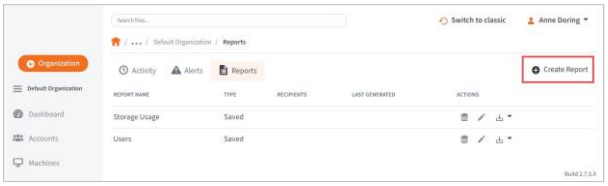
With reports, you can track various activities within the system, and export the report to your local machine. You can also set up recurring reports. Use the *Reports* page in the administrative web portal to generate these reports.

NOTE

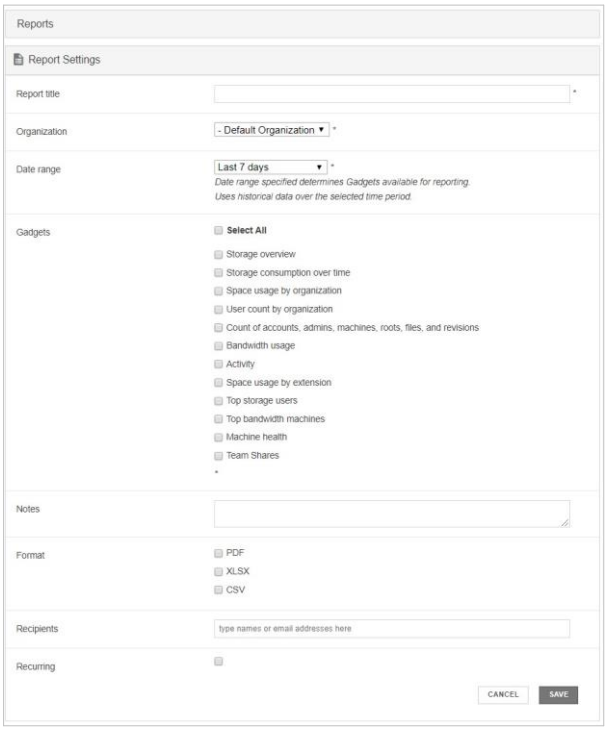
Administrators commonly use reports to track machine health and system activity. Reports are also utilized for billing purposes.

To create a report:

1. In the *Organization* navigation menu, select the organization in which you want to create a report. The selected organization displays.
2. Click the **Reports** tab. The *Reports* page displays.
3. In the *Reports* page, click the **Create Report** button. The *Report Settings* section displays.



4. In the *Report Settings* section, enter information for the new report.
   a. In the *Report Title* field, enter a **name** for the report.
   b. In the *Organization* drop-down menu, select the **organization** for which the report will apply.
   c. In the *Date Range* drop-down menu, select **Now** to use data available from the point in time when the report is run. Alternatively, select a **time period** to report on historical data.
   d. In the *Gadgets* checkbox area, select the **type of report** you want to review. For example, you can view storage information, user information, bandwidth usage, activity, space usage, machine health, and so forth.
   e. In the *Notes* field, enter a **descriptive summary or text** that will help you identify the report.
   f. In the *Recipients* field, enter the **names** of users who should receive the report. The field will populate as you type, based on the characters that you enter.
   g. Select the **Recurring** checkbox to schedule a recurring report. The page will expand to allow you to schedule the report and optionally set an end date.
   h. Click the **Save** button when you are finished.



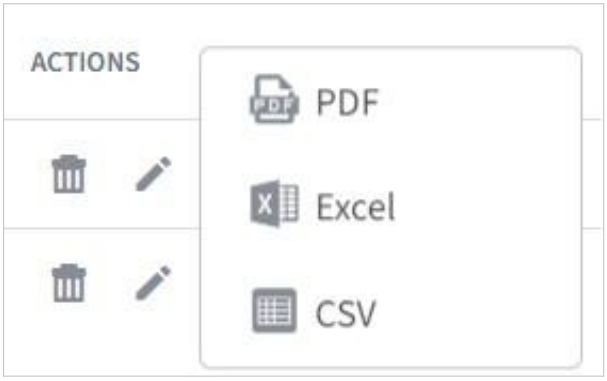
The report will be saved in the *Reports* page.

5. Optionally, use the *Actions* buttons to manage reports.

a. Click the **Delete Report** button to remove the report.

b. Click the **Edit Report** button to edit the report.

c. Click the **Download** drop-down button to download the report to a PDF file, an Excel file, or a CSV file.



d. Click the **Send** button to immediately send the report to the recipients specified in the *Recipients* field. This button only displays if a recipient is listed.

How to Review Web-Access Log Events (Private Cloud)

In addition to reviewing the activity log and monitoring reports through the administrative web portal, private cloud partners also have access to the web-access.log file, which provides detailed information on captured events. The web-access.log file can be found in the x360Sync server log folder, and records the following actions:

- access denied
- authenticated via APIv1
- authenticated via OAuth2
- authenticated via password reset token
- authenticated via web
- changed password
- failed login
- file download request
- folder download request
- granted org admin privileges
- granted system admin privileges
- moved team share
- removed from share
- revoked org admin privileges
- revoked system admin privileges
- subscribed to share
- subscribed to team share
- unsubscribed from team share
- organization created
- organization updated
- organization deleted
- web editor session

To review the web-access.log file:

1. On the server that houses your x360Sync server service, navigate to [target drive]:\x360Sync Server\logs\directory.
2. Click to launch the *web-access.log* file.

Reading the Web-Access.Log File

The web-access.log file is formatted as follows:

```
ip_address|datetime|actor_type|actor_id|actor_name|action|acted_on_type|a
c
```

For example, a *failed login* event will display as:

```
10.255.251.213|2017-04-07 13:30:56|person|2|User Name
(username@email.com
```