Accellion Share Securely™

DEPLOYMENT GUIDE

Version 9.6

TABLE OF CONTENTS

Welcome

The Accellion system has two main types of servers: Controllers and Satellites. This guide walks you through setting up an Accellion Satellite, connecting it to a Controller, and managing the various Accellion Satellite types.

Before using this guide, you should have an Accellion Controller already setup and on your network. For details on setting up an Accellion Controller refer to the *Accellion Installation Guide* for your deployment type.

Intended Audience

This guide is intended for Administrators of Accellion systems who are adding a Satellite to an existing Controller.

Using this Guide

The following annotations are used in this guide:

Tip: .....Indicates an Accellion recommendation or best practice for administering the server.

Note: Indicates information about a menu item deemed important for the administrator to know.

Caution: Indicates a setting that, if used improperly, adversely affects the operation of the Accellion server and data may be lost.

Terms Used

Controller – Primary Accellion server that Satellites are attached to. More details are listed under Accellion Controller.

Satellite – Secondary Accellion server that attaches to a Controller. More details are listed under Accellion Satellite.

Location – Used when mapping resources (typically LDAP) on the Controller to the Satellite.

Internal User – Users within your company domain.

External User – A user outside your company domain, typically someone at another company who must access Accellion resources.

Accellion Controller

The Accellion Controller is the central server in the Accellion system. The Controller performs the following:

- Processes and keeps track of uploads and downloads events for files local to that Accellion solution.
- Processes incoming replicated files.
- Replicates files as required to other locations.
- Keeps track of all files on the network; where it was uploaded and on which locations they currently exist.

- Keeps track of User profiles.
- Connects and authenticates against LDAP/MSAD.
- Logs all web client login and send events.
- Logs all download activity throughout the network.
- Hosts the web client front-end pages, including any custom branding or envelopes.
- Hosts the Administrative interface with full access to application wide policy settings.
- Generates all user emails. This includes emails generated for recipients of files, as well as return receipts, password resets, verification code, and User invitations.

Accellion Satellite

A Satellite is an additional Accellion server that is linked to a Controller. The initial configuration of a Satellite is identical to a Controller. Many administrative tasks on the Satellite, such as software updates, can be performed from the Controller. Satellite servers have their own Administrative interface which is an abbreviated version of the Controller's Administrative interface.

Satellites can be deployed anywhere as needed in the DMZ or internal network. Specific deployment requirements are details under each Satellite Type.

Basic Setup

Before continuing, your Controller must be set up and activated. Instructions for doing this are in the *Quick-Start Guide* for your installation: Hardware, Virtual, or Hosted.

System Requirements

System Type	Number of CPUs	RAM	Storage Space
Controller	2	4 GB	500 GB + depending on usage
File Satellite	2	4 GB	Should match Controller
SMTP	2	4 GB	200 GB
SFTP	2	4 GB	500 GB + depending on usage
kitedrive Sync	2	4 GB	No additional
Kitepoint Connector	2	4 GB	200 GB
Online Viewer	2	4 GB	200 GB
Archival	2	4 GB	200 GB

Firewall Requirements

Firewalls must be configured to allow traffic to and from the Satellite and Controller as outlined in that Satellite's firewall setup. See the *Satellite Types* in this guide for specific firewall settings.

Mail Setup

Add the IP address of the Accellion servers to any mail relay or spam filter. This prevents messages from the Accellion Controller from being blocked or filtered as spam.

Note: For hosted installations, the Accellion server is external to your network. Add the IP address to your DNS records for reverse DNS lookup. Also, add the IP address to any spam filtering rules to prevent messages sent from the Accellion Hosted server from being blocked.

SSL Certificates

Verify that each Controller has a wildcard certificate as described in the Quick Start guides. This supports SSL connections to the Application and Location hostnames.

Accellion Controller and Satellites require one of the following certificate types:

- An SSL certificate specific to their own location.
- A wildcard certificate that can be used on all Controllers and Satellites.

Other Considerations

Take the following into consideration when deploying a Controller – Satellite configuration:

- All Accellion servers must be activated and accessible from the network.
- Both the Controller and the Satellite must be at the same FTA software version.
- When adding a Satellite to a Controller, the Satellite's settings are overwritten by the new Satellite configuration. This means any settings, user accounts, or files, are lost when the Satellite is added.
- Satellites can be deployed within a VPN or network subset by specifying the range of IP addresses that can access the Satellite. Specific deployment options for each Satellite type are noted under the Satellite Types section of this guide.
- Any Satellite that must be accessible both internally and externally must be resolvable via its fully qualified hostname through DNS.
- Location mapping based on the LDAP Location parameter is also used to indicate accessibility to a particular Satellite location.
- Satellite Locations can be designated as Hubs to make them accessible by everyone.
- User authentications for sending and receiving files occur only on the Controllers. DNS must point the application hostname to the Controllers only.

Multi-Controller Benefits

Up to two Accellion Controllers can be connected. This is done to provide redundancy, load balancing, or better access for geographically diverse deployment.

DNS settings determine how traffic is received on the Controllers.

Note: Application hostname is used in the download links. This is what users see as the hostname when accessing the Accellion system. Location Hostname is only used if you have multiple servers, but wish to use only one DNS hostname. This is typically done for round-robin DNS or load-balancing.

Replication

When two Accellion Controllers or a Controller and a File Satellite are set up, they can be configured to replicate information between each other. Exactly what is replicated is set by the rules under Settings → Rules. If no rules are set, user data, file transaction information, report information, and server settings are replicated. The files themselves are *not* replicated unless specified by a rule. Location Mapping will determine where files are replicated.

Load Balancing

Two Accellion Controllers can be used to distribute user transactions between them. This can be done via round robin DNS, or via a third-party load balancer. All data between the two servers are replicated, so the fact that there are two servers is transparent to the user.

Round Robin – This is handled via DNS entries. The IP addresses of both Accellion Controllers can be entered into DNS, but use the same Fully Qualified Domain Name (FQDN). This FQDN must be set on both Accellion Controllers under Administration → Application → Application Hostname. This way, when DNS for the Controllers is queried, it returns two IP addresses for the same FQDN, and the connection is made for either Controller.

Load Balancer/Firewall – A third-party load balancer, or load balancing firewall, can be used to send packets to either Accellion Controller. Check with the instructions for your specific load balancer or firewall for setup details.

Redundancy

One method for ensuring up-time on the Accellion system is to have two Controllers: one actively used, the other in standby. The standby Controller keeps a connection with the primary Controller. All data is replicated to the standby Controller, including files, user accounts, and server settings.

If the primary Controller is no longer available, activation of the standby Controller can be done one of two ways:

1. Change the IP address of the standby Controller to that of the primary Controller. This is done via the Administrative web interface under Appliance → Configure → IP Address. In this method, DNS doesn't have to propagate, so the change-over is faster. You have to switch the IP addresses back when the primary Controller is brought back online.
2. Change the DNS entry to point to the IP of the standby Controller. In this method, you have to wait for DNS to propagate.

Connect Active Directory/LDAP

The Accellion system has the ability to integrate with existing LDAP or Microsoft Active Directory (MSAD) systems. This section walks you through the basic steps of setting up an LDAP/MSAD connection. In these instructions, the term LDAP refers to both LDAP and Microsoft Active Directory.

Follow these steps to setup an LDAP connection on your Accellion Controller:

Log in to the administrative web interface and navigate to Administration → LDAP.

1. Click **Edit** at the bottom of the page.
2. Enter the IP address or hostname of the LDAP server.
3. Enter the correct port to communicate to the LDAP server. We recommend testing the port by using the **Connectivity Check** tool available under Appliance → Status → Tools.
4. Set the User Attribute. This is what the Accellion Controller uses to lookup the user account, and is typically this is set to "Email".
5. Enter the Associate Login ID. This allows users to log in using their "Friendly Name" instead of their email address, and is typically sAMAccountName.

Note: The Accellion server uses the Associate Login ID to find the user's email address, and then uses the email address to login. So, even though the user is typing in their user name, the Accellion server is still using their email address for authentication.

6. Enter the “Base DN” under both User Identification and Authorization. It must be set to the domain used by the LDAP server. For instance, if the LDAP server resides in a private domain, the Base DN is like: DC=company, DC=private.
7. Fill out the “Bind DN”. This is the account the Accellion server uses to access the LDAP server. This should be a service account with *read only* access to the entire LDAP tree. It can be set two different ways:
    a. user@company.private (same as the Base DN)
    b. CN=user, CN=container, OU=organizational unit, DC=company, DC=private

Note: If using the second method you need to know the exact location of the user account, and whether or not the layers are “organizational units” or “containers”. If you’re not sure, a third-party LDAP mapping tool needs to be used.

8. Test the LDAP connection by clicking the **Test LDAP Settings** button at the bottom of the page. This opens a new page where you can enter an email address and test the connection. If you make any changes, click the **Copy to LDAP Settings** and **Copy to Authorization Settings** buttons to save changes to the LDAP setup page.
9. Click **Submit** to write changes.
10. Enable LDAP by clicking **Edit** next to LDAP Enable.

After LDAP is enabled, any user with a valid LDAP account can log in with their email address and LDAP password. Further details of the other settings within LDAP can be found in the *Accellion Administrative Guide*.

Enable Anti-Virus

By default, Anti-Virus is disabled. If your Accellion system is licensed for Anti-Virus, navigate to Administration → Anti-Virus, and click **Enable**.

Connecting Accellion Servers

This section guides you through adding an Accellion Satellite to the Controller. Before following these steps, use the appropriate *Quick-Start Guide* to activate the Accellion Controller and the Accellion Satellite, and make them accessible on the network.

This section applies to all Satellite types, as well as adding a Controller to another Controller.

Note: Only two Controllers may be linked in an Accellion deployment.

Below are the instructions to add Accellion servers to the Controller.

Step 1 – Set Firewall Rules

Open the ports specified in *Satellite Types* for the type of Satellite being added.

Step 2 – Update Software

Both the Controller and the server to be added must be at the same software version. To do this:

1. Log in to the Controller's administrative web interface.
2. Navigate to Administration → Software Update.
3. Click **Check for Update**. The Update page displays.
4. Click **Update Now**. The server updates.

Repeat these steps on the server to be added to the Controller.

Step 3 – Create the Security Token

1. Log in to the Administrative web interface on the server that is being added to the Controller.
2. Navigate to Administration → Locations.

3. Click "**Generate Token**". A new page opens displaying the token.
4. Copy and paste the token into a text editor to save it for later use.

Step 4 – Add the Location

1. Log in to the Administrative web interface on the Controller to which the new server is being added.
2. Navigate to Administration → Locations.

3. Click **Add Location to Network**. A new page displays prompting for information about the server being added.

- *IP Address* – This is the IP address of the new Satellite. Since this address may be translated via NAT, be sure you enter the IP address as it would accessible from the Controller.
- *Token* – This is the token obtained in Step 2 above.
- *Location Host Name* – The hostname that is used for the new Satellite.
- *Location City Name* – Identifier for the Satellite's location. Used by the user when setting download locations.
- *Location Country Code* – Country location of the Satellite server.
- *IP Address of the current location* –The current IP address of the Accellion Controller will be displayed.

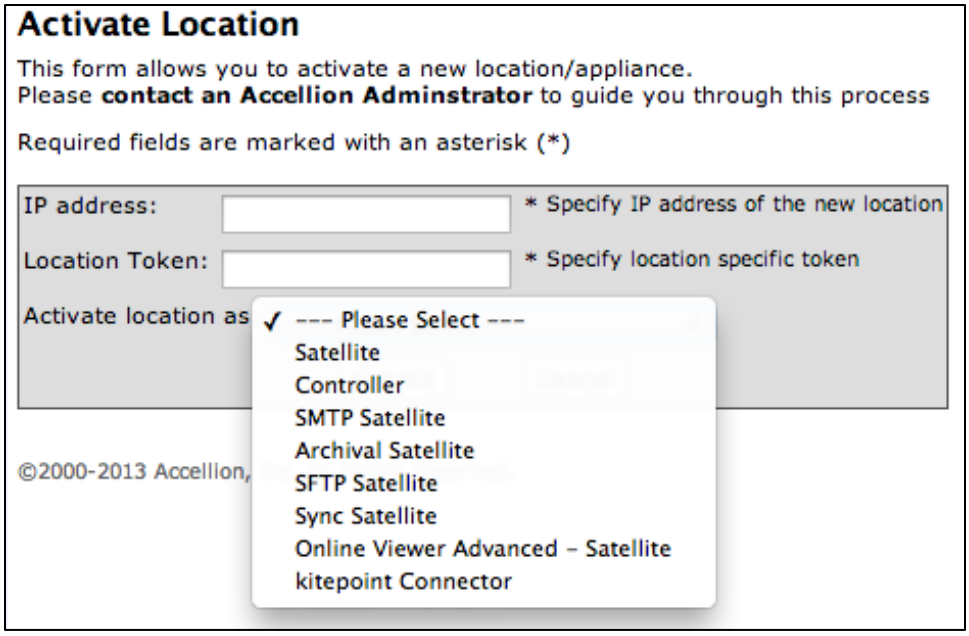
Caution: This address may be translated via NAT; ensure you enter the IP address as it would accessible from this server.

4. Click **Submit**. You are returned to the Administration → Locations page that lists the new Accellion server.

Step 5 – Activate the New Server

Before the new Accellion server can be used, it must be activated and assigned a role. To activate the server:

1. On the Administration → Locations page, click **Activate** next to the server that was added.
2. Enter the token from Step 2.



3. From the pull-down menu, choose which Satellite type this Satellite becomes.

Caution: Choose the Satellite type carefully, as this process cannot be reversed. All information on the Satellite will be overwritten.

Note: The Satellite choices displayed will vary depending on the license purchased.

Note: There can be only two Controllers in a single Accellion deployment.

4. A confirmation window appears with the IP address, and the type of location you are adding. Verify the information is correct, and click **OK**.

Note: If you try to access the Satellite at this point, the following error message displays:

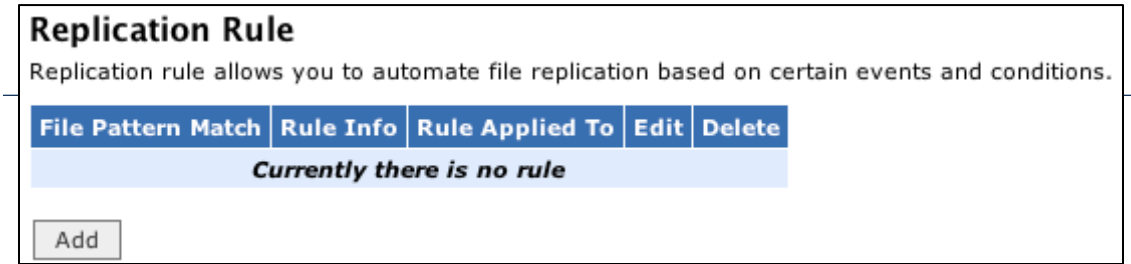
> Sorry, an error occured while processing your request.
>
> Please report this error to support@accellion.com and include the appliance hostname and the diagnostic dump in the mail. Diagnostic dump can be generated from Appliance →Status page.

When the Satellite has been successfully added, the Locations page looks as follows:

Locations	Features	Application	IP Restriction	Port Redirection
multi-1(US) Edit	Controller	Suspend	-	-
multi-2(US) Edit Manage	Controller	Suspend	-	-

Step 6 – Set File Replication Rules (Optional)

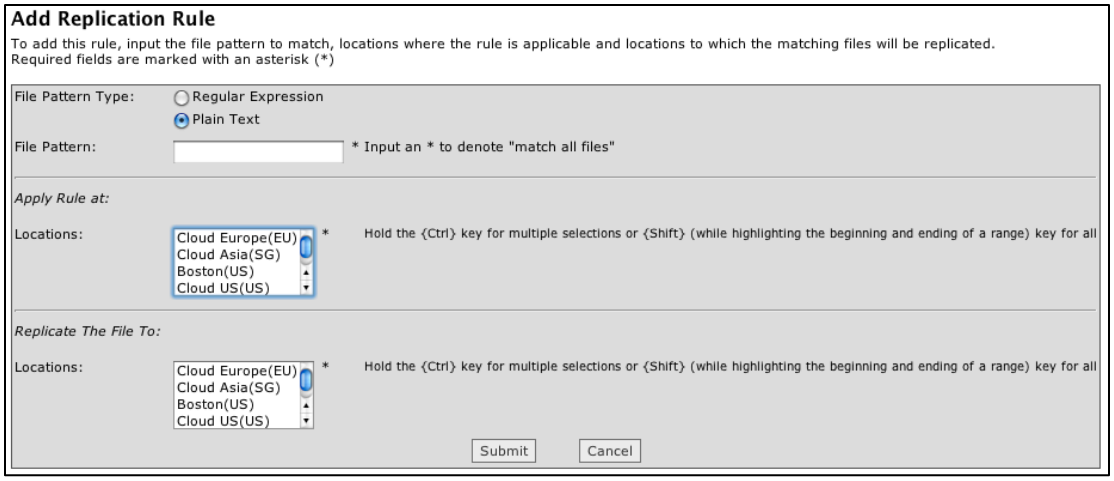
File replication determines which files are replicated from the Controller to Satellite servers.



Replication rules are explicit rules created by the administrator that govern file replication across multiple Accellion servers. If no rules are created, files are replicated based on how users are mapped in Location Maps. For details about mapping users to specific servers, refer to the *Location Maps* section in this guide.

To add a Replication Rule:

1. Log in to the Administrative web interface on the Accellion Controller.
2. Navigate to Settings → Rules
3. Click **Add**. A new page displays.



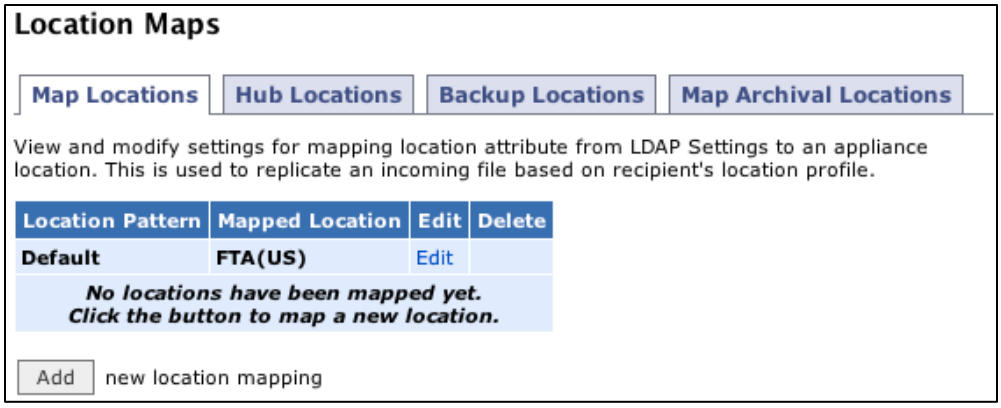
4. Use these fields to create the new rule.
   - *File Pattern Type* – The pattern can be entered as plain text, or as a regular expression.
   - *File Pattern* – To select specific files for replication, put the desired string into the **File Pattern** textbox. That exact pattern is used to determine which files will be replicated. To replicate all files, insert an asterisk (*****) in the textbox.
   - *Apply Rule at: Locations* – Select locations where the new replication rule will be applied. Multiple locations can be selected.
   - *Replicate The File To: Locations* – Select locations where matching files need to be copied to. Multiple locations can be selected.
5. When the parameters of the rule have been set, click **Submit** to create the rule.

To delete a rule, click the **Delete** link of the rule to be deleted. Click the **Delete** button in the popup window to confirm deletion.

Step 7 – Set Location Maps (Optional)

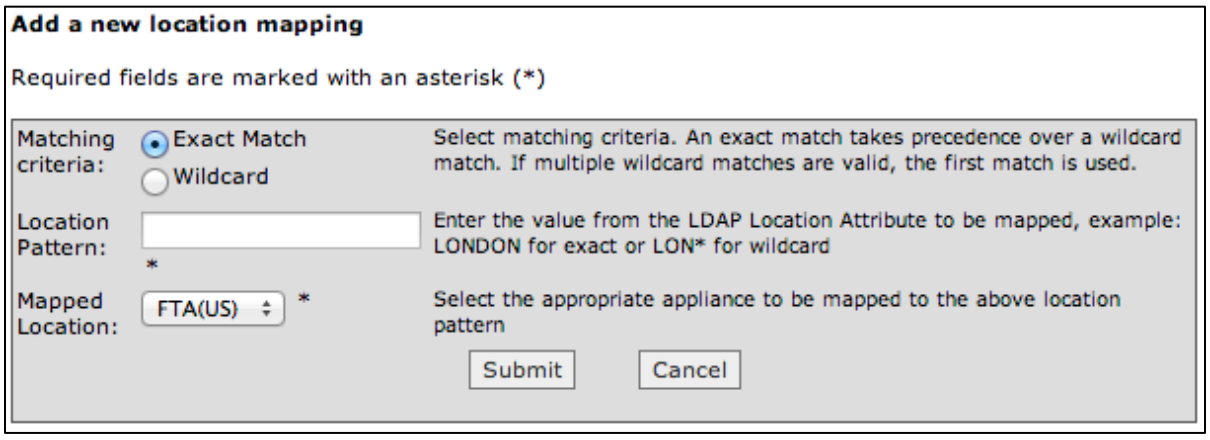
Location Maps are used to map users to different Accellion Controllers and Satellites. This mapping is done according to attributes set in the LDAP section to optimize upload and download speeds.

Map Locations



To add a new Location Map:

1. Log in to the Administrative web interface on the Accellion Controller.
2. Navigate to Settings → Location Maps.
3. Click **Add**. A new page displays.
    - *Matching criteria* – "Exact Match" means only location patterns that fit the criteria are mapped. Exact Match takes precedence over wildcard matches.
    - *Location Pattern* – The Location Pattern is the LDAP attribute used to determine a user's location.



    The LDAP/MSAD administrator sets this. The LDAP Location Attribute is configured under Administration → LDAP → Location Attribute. Different LDAP servers can have a different Location Attribute.
    - *Mapped Location* – Select which server the users matching this Location Pattern should use. This becomes their default location when using the Outlook Plugin and Web Client.
4. Click **Submit** to process the changes.

To edit an existing Location Mapping, Click the **Edit** link in the row of the location to be edited.

To delete a location click the **Delete** link in the row of the location to be deleted.

Hub Locations

In a multiple-site server, hub locations can be set to direct where users can upload their files. If one or more hubs are set, users are able to upload files to the hubs as well as to where the locations they are mapped. If no hub location is set, every user is able to upload to every location.

To set the hub, click the **Edit** link, and then select the location(s) to be hubs.

Backup Locations

The Outlook plugin can have two locations for uploading files to the server: Default Location, and Backup Location. For Outlook accounts created by the administrator, both locations can be specified. For Outlook accounts created automatically using the Zero-Input Agent Install, the Default Location is set according to the user's LDAP mapped location (as determined by the rules in Settings → Location Maps → Map Locations). The Backup Location is set according Backup Locations (this page).

To set the Backup Location, click **Edit** in the row of the Backup Location to be edited. Select the desired Backup Location from the dropdown menu.

Note: The **Backup Location** default setting is the same as the **Location** parameter. Changing the **Backup Location** to another server is recommended so the Outlook Plugin can still upload files should the Default location become unavailable.

Satellite Types

This section of the guide is divided into sections pertaining to specific Satellite installations. The information is organized as follows:

Description – Describes this Satellite's function.

Firewall Ports – Details what firewall ports are required for that specific Satellite type.

Deployment – Shows any specific recommendations on setting up this Satellite (example: should it be in the DMZ).

Satellite Administrative Settings – Shows what settings are available via that Satellite's Administrative interface.

Managing the Satellite – Gives instructions on how to manage aspects of this Satellite, typical usage, tips, and other best practices information

Troubleshooting – Presents common issues and their solutions for each Satellite.

Administrative Interface

Each Satellite has its own administrative web interface. The exact options available vary based on the Satellite's type, but some menu items are the same across all Satellites.

Home

From here, the contact email address and password of the logged in administrative account can be changed.

Appliance

Contains all the settings for that specific Accellion server. These menu headings are described in detail in the *Accellion Administrative Guide*.

Appliance → Communication – Shows the current connection status between the Kitepoint Satellite and the Accellion Controller.

Note: If the IP address of the Accellion Controller changes, it must be edited here as well. Click **Edit** next to the appropriate Controller, and enter the correct IP address.

Accellion File Satellite

Also called “Replication Satellite”, the Accellion Satellite is an additional full service Accellion server that is linked to the main Accellion Controller. The Controller replicates files and user data to this Satellite to provide quicker access to information in geographically diverse installs.

Firewall Ports

Service	Type	Port	Direction	Notes
HTTPS	TCP	443	Inbound/Outbound	–
SSH	TCP	22	Inbound/Outbound	–
DNS	UDP	53	Inbound/Outbound	–
SMTP	TCP	25	Outbound	–
AUDP	UDP	8812	Inbound/Outbound	To the Accellion Controller
RSYNC	TCP	873	Inbound/Outbound	To the Accellion Controller
NTP	UDP	123	Outbound	–

Deploying

This Satellite deploys the same as the Controller, though typically in a different data center.

Satellite Server Settings

The Accellion File Satellite is similar to the Controller, but the administrative web interface has only the Appliance menu available. For details on Appliance menu settings, see the *Accellion Administrative Guide.*

Managing

Because the Satellite receives file and user information from the Controller, there is nothing to manage on the Accellion Satellite directly.

SFTP Satellite

The Accellion SFTP Satellite is used to store and deliver files over SFTP by using any available client that supports SFTP. Scripted SFTP transfers can work transparently with the SFTP Satellite as well. Uploaded files are stored using the secure Accellion file system.

Firewall Ports

The following are the firewall settings required by the SFTP Satellite:

Service	Type	Port	Direction	Notes
HTTPS	TCP	443	Inbound/Outbound	–
SFTP(SSH)	TCP	22	Inbound/	For SFTP
DNS	UDP	53	Inbound/Outbound	–
SMTP	TCP	25	Outbound	–
AUDP	UDP	8812	Inbound/Outbound	To all Accellion servers
RSYNC	TCP	873	Inbound/Outbound	To all Accellion servers
NTP	UDP	123	Outbound	–

Deploying

Since internal and external users typically access the SFTP Satellite, Accellion recommends the SFTP Satellite be deployed in the DMZ with a valid internal and external DNS hostname. It needs either a public IP address, or a NAT'd IP address.

SFTP Server Settings

The SFTP Administrative web interface will change showing only the Home and Appliance menus.

The only change specific to SFTP is under Appliance → Status SSH (SFTP).

From here, you can:

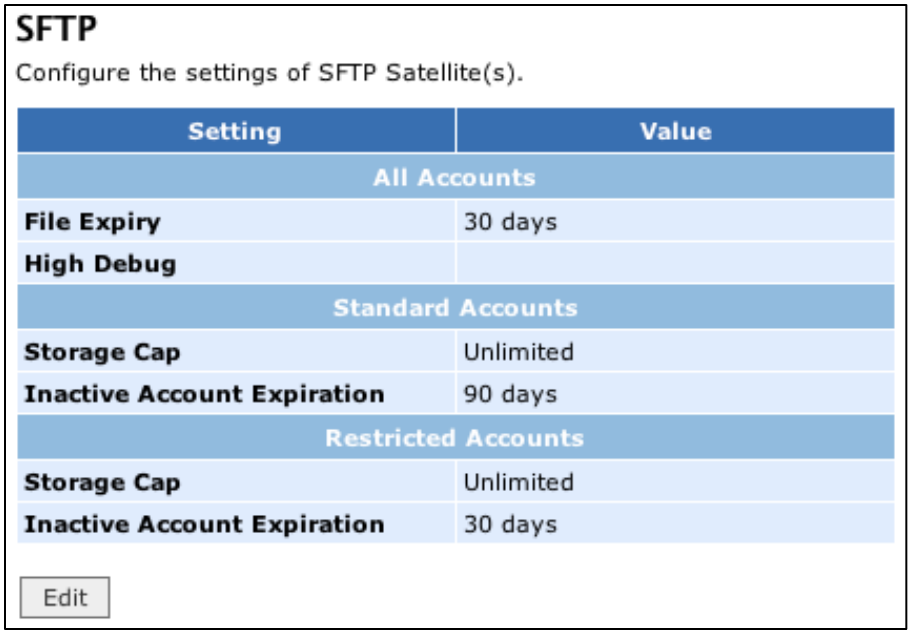
- Restart the SSH (SFTP) service
- Change the remote management password used by Accellion tech support.
- Display the SSH Public Key that is used during SFTP transactions.

Managing the SFTP Satellite

After activation of the Satellite, additional setup is required on the Controller's administrative web interface under Settings → SFTP before users can use the Accellion SFTP Satellite.

All Accounts

The settings in this section affect both Standard and Restricted SFTP accounts.



File Expiry – This setting determines the number of days the uploaded files remain on the server after being uploaded. Expired files are purged.

High Debug – When high debug is enabled, more debug information is recorded in log files, so that errors can be recorded for detailed analysis.

Standard and Restricted Accounts

Settings only affect the account type under which it is listed.

Storage Cap – The total file size uploaded by an account user cannot exceed the storage cap (set in Megabytes). The storage cap can be set to 0 for a specific account type for unlimited storage.

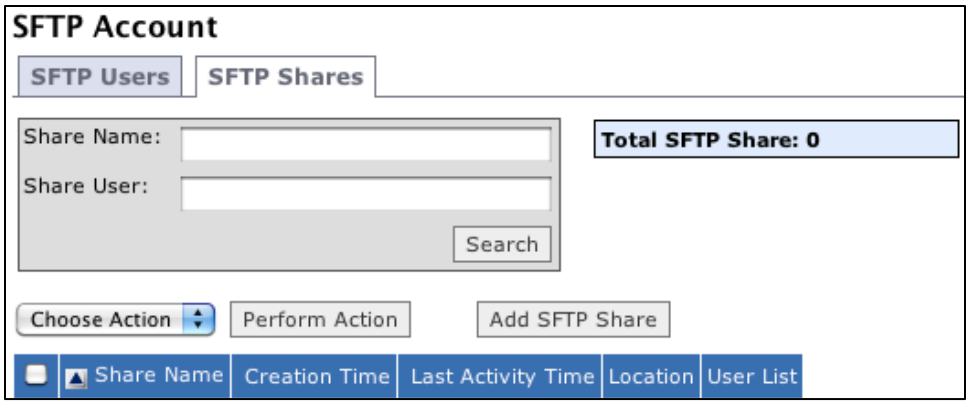
Inactive Account Expiration – An SFTP account that is not used in the number of days specified by this setting are treated as inactive. Inactive accounts are deleted, along with all files uploaded by that account.

The following steps show the creation of an SFTP account, creating an SFTP share, and adding an SFTP share to workspaces.

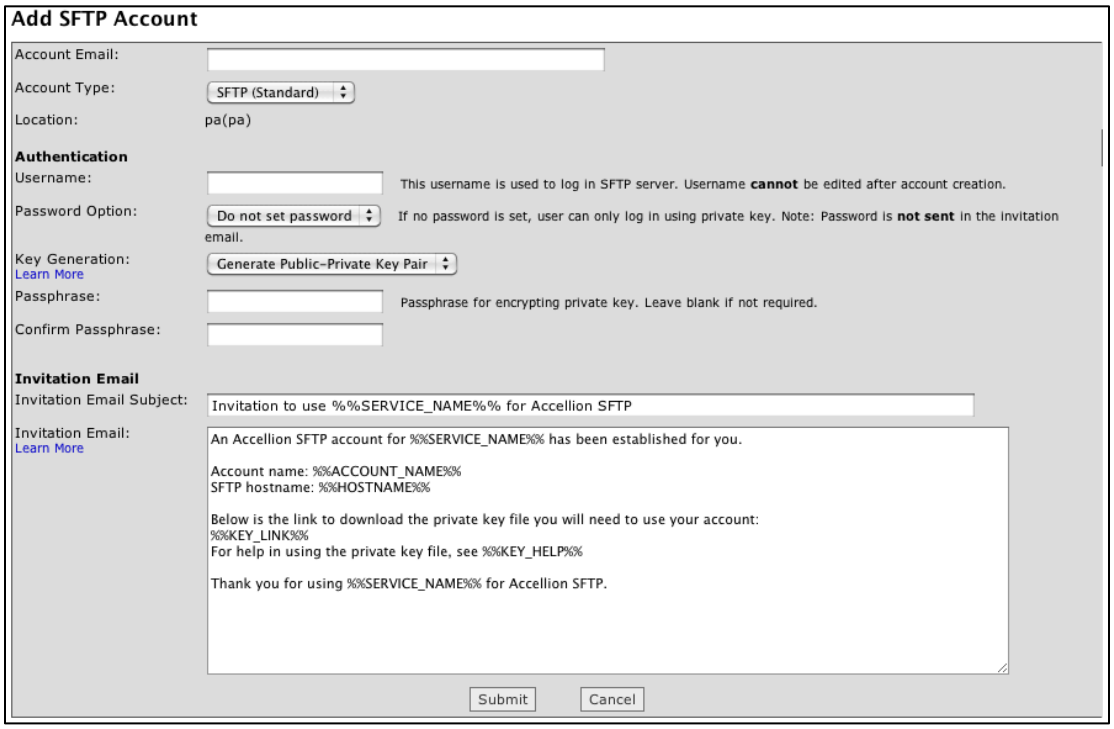
Creating SFTP Accounts

The following steps will guide you through creating SFTP accounts.

1. Log into the Controller's Administrative web interface and navigate to **Manage → SFTP Account**.



2. Click Add SFTP User.



3. Fill out the Add SFTP Account using the information below.

Account Email – Enter the email address of the user to be created.

Account Type – Select the account type: SFTP (Standard), or SFTP (Restricted).

Location – Select the appropriate location if there are multiple SFTP servers.

Username – Enter the name with which the user logs in.

Password Option – Select one of two options for authenticating the user:

- *Do not set password* – Users are given a private key they can use to authenticate. A link to this key is sent in the invitation email.

OR

- *Set Password* – Sets a password the user uses to authenticate to SFTP shares. The password is not sent in the invitation email, so must be given separately.

Password – Sets the password for the account.

Key Generation – The SFTP service is designed to work with public-private key pairs. The SFTP Satellite stores public keys for specific users. The user uses the corresponding private key in the SFTP client to authenticate against it. There are two ways to set up the key pair authentication for a user:

- *Generate Public-Private Key Pair* – The server generates a 2048-bit RSA public-private key pair. The public key is uploaded to the SFTP Satellite, and the matching private keys are sent to the user via invitation email.

OR

- *Upload Public Key* – The public key is uploaded during account creation. Both OpenSSH and ssh.com public key formats are accepted.

Tip: The minimum length for an RSA key to provide sufficient security is 1024-bit, but RSA Security recommends using 2048-bit.

Passphrase – The Passphrase is optional, but recommended to encrypt the generated private key for additional security. The Passphrase must be at least five characters long. Passphrases are sent to the user in a separate email.

Private keys are in OpenSSH format that works with most Unix clients. If required, these keys can be converted into PPK format for MS Windows clients using external utilities such as PuTTYgen.

Invitation Email – Shows the invitation email as it is sent. To see what %%fields are supported in the email, click the **Learn More** link.

4. Click **Submit** to create the user account and send the invitation email.

Note: The content of the email can be edited under Settings → Notification → Plugins and Agents.

Now the user's account is set up. The invitation email contains important information needed for the user to login in to the SFTP service.

To edit an SFTP account, go to Manage → SFTP Account, and click the wrench icon to the left of the account you wish to edit.

To upgrade or downgrade account types, or delete multiple accounts, you can use the **Choose Action** drop down on Manage → SFTP Account. Check the accounts you want to edit, select the appropriate action from the drop down, and click **Perform Action**.

Creating SFTP Shares

Now that the user account is set up, the next step is to create SFTP shares. SFTP shares are a virtual directory used to share files among SFTP accounts. The administrator creates a share and adds SFTP accounts to it. SFTP accounts that have been added to the share are able to see the share folder and upload files to it.

Note: .....An SFTP share does not consume a license.

The following instructions will walk through creating an SFTP share.

1. Log into the Controller's administrative web interface and navigate to Manage → SFTP Account → SFTP Shares.

2. Click **Add SFTP Share**. The following window opens.

3. Create the share using the information below.

Share Name – This is the name shown inside the Share directory in the user's home directory. The share name should be unique.

Caution: All characters are permitted as a share name, except that it cannot be <*number*> - <*number*>, since that format is used for account IDs.

User Lists – List of users that were created under Creating SFTP Accounts.

4. Add users to the share by selecting the user account, then clicking **Add** →. The account appears in the right side column.

Permission – Determines if the user can upload files to the share, or read/download only.

Map to Workspace – SFTP shares can be mapped to workspaces. Files uploaded to a mapped share will be automatically added to the workspace.

To map a workspace:

1. Log in the Controller's Administrative Web interface and navigate to Manage → SFTP Account → SFTP Shares.
2. For existing shares, click the wrench icon on the share you wish to map. To create a new share, click Add SFTP Share.
3. From the pull-down menu, select the name of the Workspace to which this share will be mapped.

4. Click **Submit** and the share is mapped to the selected workspace.

Now files uploaded to this SFTP share are added to the mapped Workspace automatically.

Note: .....This only affects files uploaded after the share has been mapped.

Note: Files put into sub folders of the SFTP share are also added to the mapped but do not create a nested Workspace. Changes made within the Workspace will not show in the SFTP client.

Users must have an SFTP client to upload/download files on the SFTP Satellite. Common SFTP clients include PuTTY, WinSCP, Filezilla, FireFTP, etc.

To use the client, the user must log in with the credentials provided in the invitation email. They'll use the hostname of the Accellion SFTP server (not the Accellion Controller), and connect on port 22 (standard SFTP port).

When authenticated, the user will have access to any files/shares as they would on a standard SFTP server.

SFTP Share Management

Settings for an SFTP share can be edited by clicking the  icon to the left of the share under Manage → SFTP Account → SFTP Shares.

To delete SFTP shares:

1. Select the checkboxes on the left of the SFTP shares to be deleted.
2. From the "Choose Action" drop down list, click **Delete**.
3. Click Perform Action.

SMTP Satellite

SMTP Accounts allow Multi Function Devices (MFDs), such as SMTP enabled copy/scanner/fax machines, to upload files to the Accellion server and send a secure link instead of an attachment. The email is sent from the MFD to the Accellion SMTP Satellite, which strips the attachment from the email, uploads it to the server, and replaces it with a secure download link.

Firewall Ports

Service	Type	Port	Direction	Notes
HTTPS	TCP	443	Inbound/Outbound	–
SSH	TCP	22	Inbound/Outbound	For Support use
DNS	UDP	53	Outbound	–
SMTP	TCP	25	Inbound/Outbound	–
AUDP	UDP	8812	Inbound/Outbound	To all Accellion servers
NTP	UDP	123	Outbound	–

Deploying

The SMTP satellite must be in a place on the network where it can be seen by the MFDs. This is typically in the same area as the mail server.

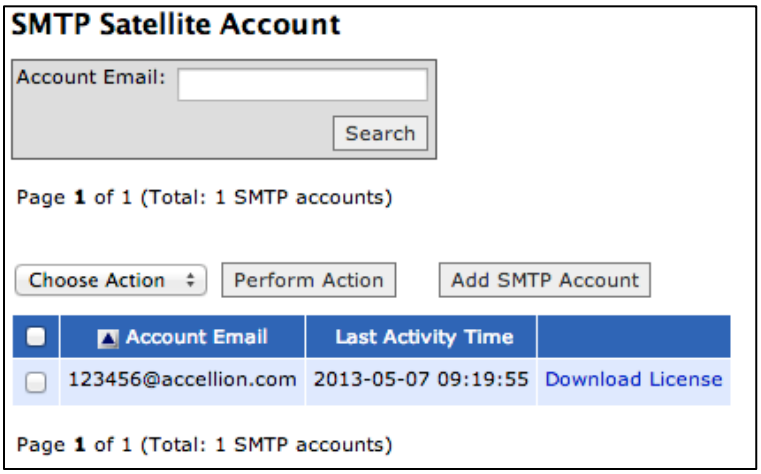
SMTP Satellite Settings

The SMTP Satellite has the Appliance and SMTP Satellite menus. The Appliance menu is where changes are made to the Satellite server's settings. The SMTP Satellite menu is where the SMTP license is uploaded, and any customer parameters are configured.

SMTP License

Before you can use the SMTP Satellite, you must generate a license from the Controller. To do this:

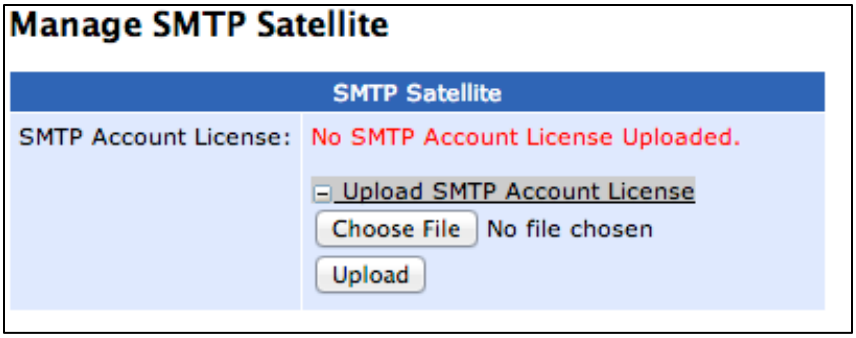
1. On the Controller's Administrative web interface, navigate to Manage → SMTP Account.



2. Click **Download License** and save the file.

When you have the license, it must be applied to the SMTP Satellite. To do this:

3. Log in to the SMTP Satellite and navigate to SMTP Satellite → Manage SMTP.

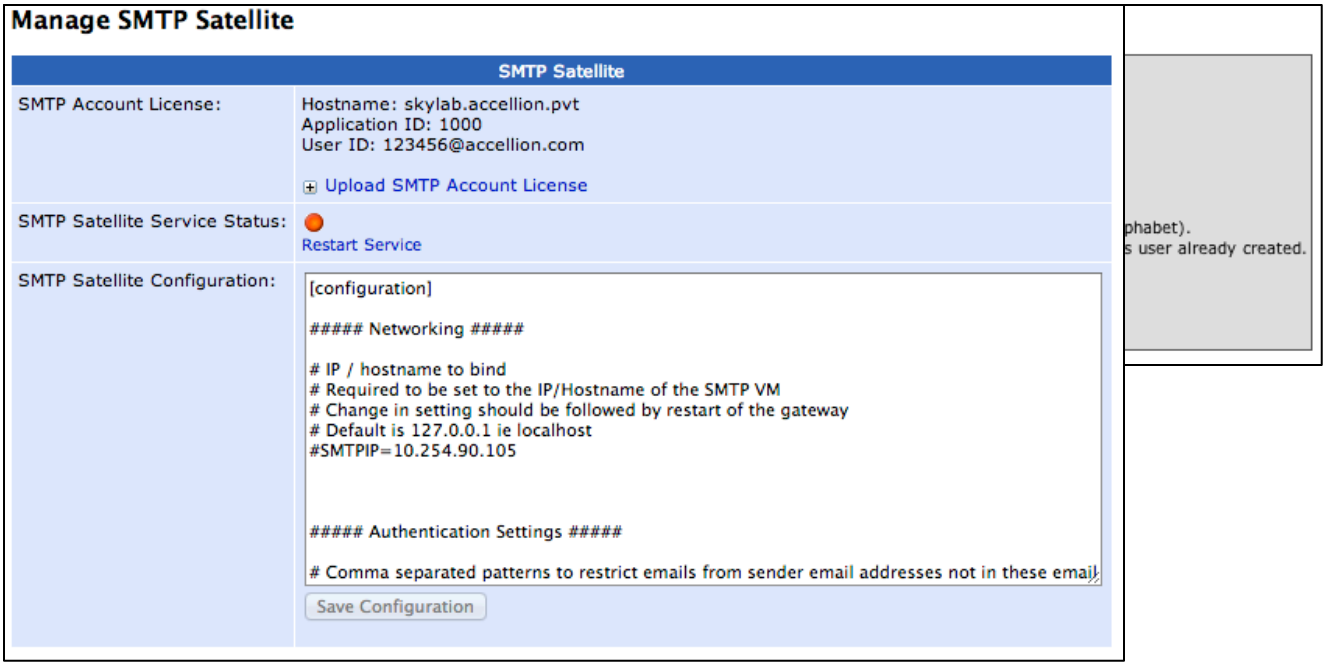


4. Click **Choose File**, and navigate to the license file from step 2 above.
5. Click **Upload**.
6. Change any of the parameters needed in the SMTP Satellite Configuration window. These settings are available from your MFD.
7. Click **Restart Service** to start the SMTP service.

SMTP Accounts

Now that the license has been uploaded to the SMTP Satellite, an SMTP account must be created. To do this:

1. On the Controller's Administrative web interface navigate to Manage → SMTP Account.
2. Click **Add SMTP Account**. The following page opens:



3. Fill out the required information.

- **Account Email –** These are the account addresses that will be created, and where the invitations will be sent. Multiple email addresses can be entered, separated by a comma or semi-colon.
- **Password –** A password must also be set for the account to authenticate to the Accellion server. The password must be at least 6 characters long and contain at least one numeral and one upper case letter. The password will be ignored if the account user is an LDAP account, or already exists on the Accellion server.

4. Click **Submit** to create the account.

Set Up the MFD

Next, add the Accellion SMTP account to the MFD.

On the MFD(s) that will be using the Accellion SMTP Satellite, you must add the IP address/hostname of the Accellion SMTP server and the account it will be using. Setup of these will depend on the MFD being used. Consult the manufacture's manual for assistance.

The account is now able to receive requests from the MFD, and replace the email attachment with a secure Accellion link.

Managing the SMTP Satellite

Once setup, the SMTP Satellite requires no management. Additional SMTP accounts can be added via the Controller under Manage → SMTP. Any changes to the account on the Accellion Controller or changes to the SMTP Satellite requires updating of the settings on the MFD.

Archival Satellite

The Accellion Archival Satellite archives emails and attachments for companies that require all emails be kept for later discovery/auditing. The Archival Satellite sends the email on to the company's existing email archive server.

Firewall Ports

Service	Type	Port	Direction	Notes
HTTPS	TCP	443	Inbound/Outbound	–
SSH	TCP	22	Inbound/Outbound	For Support
DNS	UDP	53	Inbound/Outbound	–
AUDP	UDP	8812	Inbound/Outbound	To all Accellion servers
NTP	UDP	123	Outbound	–
SMTP	TCP	25	Outbound	To existing archiving server

Deploying

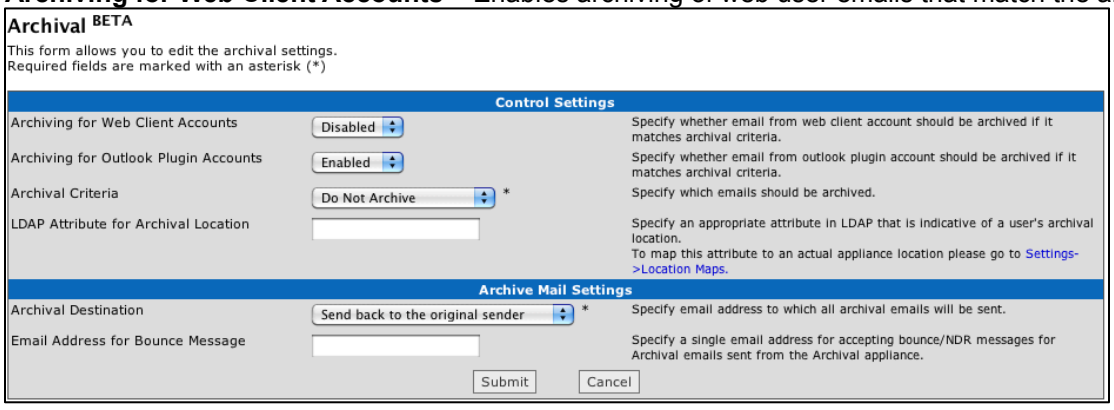
The Archival Satellite requires access to the existing archival solution for your company. For this reason it is typically set up in the same DMZ as the archival solution.

Archival Satellite Settings

There are no Archival specific settings on the Archival Satellite. It has the Appliance menu so changes can be made to the server specific settings, but nothing else. All settings and management for connecting the Accellion Archival Satellite are located on the Controller.

The Archival Satellite needs the IP address/hostname of the archive server filled out under Appliance → Configure → Mail Host Relay.

Archiving for Web Client Accounts – Enables archiving of web user emails that match the archival criteria.



Archiving for Outlook Plugin Accounts – Enables archiving of Outlook Plugin user emails that match the archival criteria.

Archival Criteria – Determines what emails will be archived.

Do Not Archive – Disables the Archival feature. No emails will be archived.

Archive All Emails – Archives all emails sent via the Accellion server.

Archive Selected Emails – When selected, gives two new options:

Only if sender's LDAP attribute – Determines what LDAP attribute is checked.

Matches with – Determines what the LDAP attribute will need to be for the account to be selected for Archival.

LDAP Attribute for Archival Location – Specifies what LDAP attribute is used to determine a user's archival location (when multiple Archival Satellites are available). This attribute can be set under Settings → Location Maps.

Archival Destination – Determines where archival emails are sent.

Send back to the original sender – Sends the archival email back to the originator of the email.

Send to the following email address – When selected, gives a new option to add an email address the archival email is sent to.

Email Address for Bounce Message – The email address for accepting bounce/NDR messages for Archival emails sent from the Accellion Archival Satellite.

Managing the Archiving Satellite

Archive Satellites can take advantage of LDAP mapping to determine what Satellite is used if multiple Archiving Satellites are available. These can be set under Settings → Map Locations → Map Archival Locations.

Kitedrive Sync Satellite

End users install the Kitedrive Sync client and choose a sync location on their local system. Within the sync location, users will see folders corresponding to their Kitedrive as well as other syncable workspaces on the Accellion server. For the Kitedrive workspace, synchronization is continuous as long as the Kitedrive client is running. Sync for other workspaces is on demand. Users can initiate on demand sync by clicking the **SYNC NOW** link in the Kitedrive client or tool-tray menu.

Firewall Ports

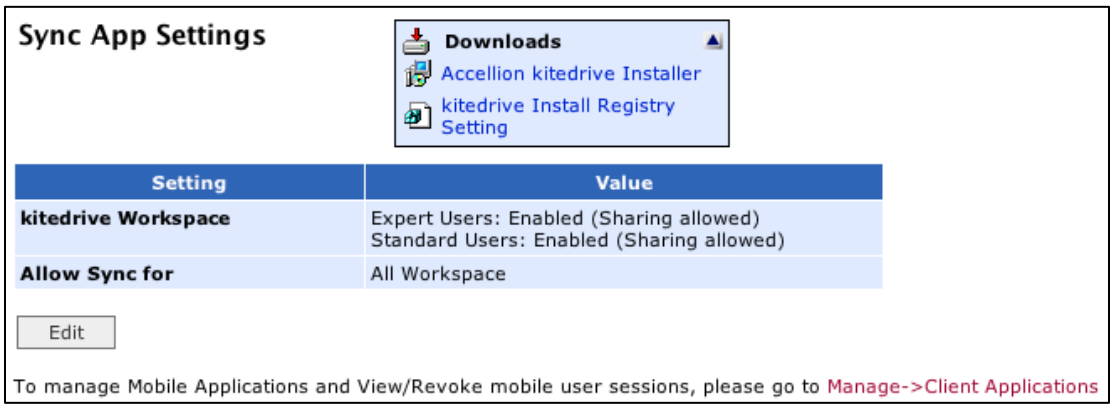
Service	Type	Port	Direction	Notes
HTTPS	TCP	443	Inbound/Outbound	–
DNS	UDP	53	Inbound/Outbound	–
AUDP	UDP	8812	Inbound/Outbound	To all Accellion servers
NTP	UDP	123	Outbound	–
SSH	TCP	22	Inbound/Outbound	For Support

Deploying

The Kitedrive satellite must be deployed where it can access the Accellion Controller.

Kitedrive Sync Satellite Settings

The Kitedrive interface looks exactly like Accellion Satellite interface.

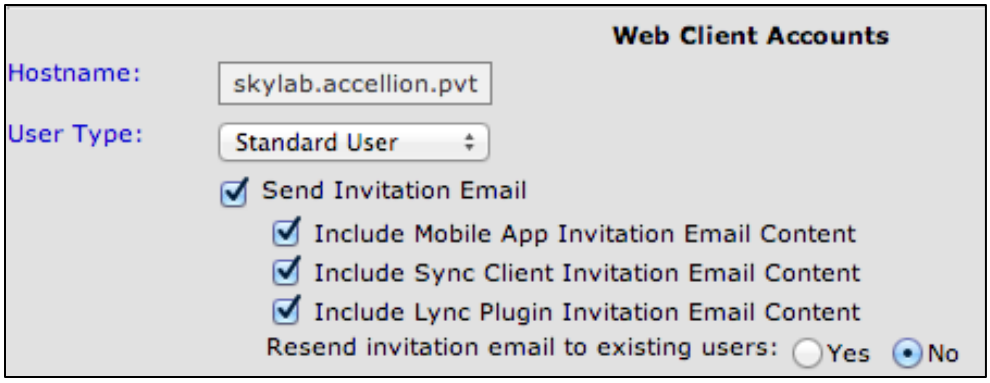


Managing the Kitedrive Sync Satellite

Both the kitedrive workspace and Sync functionality are enabled on the Controller's administrative interface under Settings → Sync App.

To add kitedrive functionality to a user's account:

1. On the Controller's administrative web interface, navigate to Manage → Users



2. Click **Add User** to bring up the Add User page.

3. Under the “Web Client” section, check Include Sync Client Invitation Email Content.

4. Click **Submit**.

The user will receive the invitation email containing a link to download the kitedrive client, and a link to the *Accellion User Guide*.

Further information for installing the Kitedrive Sync client can be found in the *Accellion User Guide*.

Kitepoint Satellite

The Kitepoint Satellite, also referred to as a Kitepoint Connector, allows users to synchronize Accellion workspaces with folders on their local computer. This function can be added to existing workspaces, or newly created ones. Multiple users can use the same workspace, and kitredrive synchronizes documents between them all.

Firewall Ports

Service	Type	Port	Direction	Notes
HTTPS	TCP	443	Inbound/Outbound	–
SMB	TCP	445	Inbound/Outbound	To the CIFS/SMB server
SSH	TCP	22	Inbound/Outbound	For Support
HTTP	TCP	80	Inbound/Outbound	SharePoint Connection
DNS	UDP	53	Inbound/Outbound	–
AUDP	UDP	8812	Inbound/Outbound	To all Accellion servers
Websocket	TCP	8082	Inbound/Outbound	To all Accellion servers
NTP	UDP	123	Outbound	–

Deploying

The Kitepoint Satellite requires access to both the Accellion Controller and the SharePoint resources, typically in the DMZ.

Kitepoint Satellite Settings

After the Kitepoint Satellite has been added to the Controller, it must be configured. To start, log into the administrative web interface on the Kitepoint Satellite.

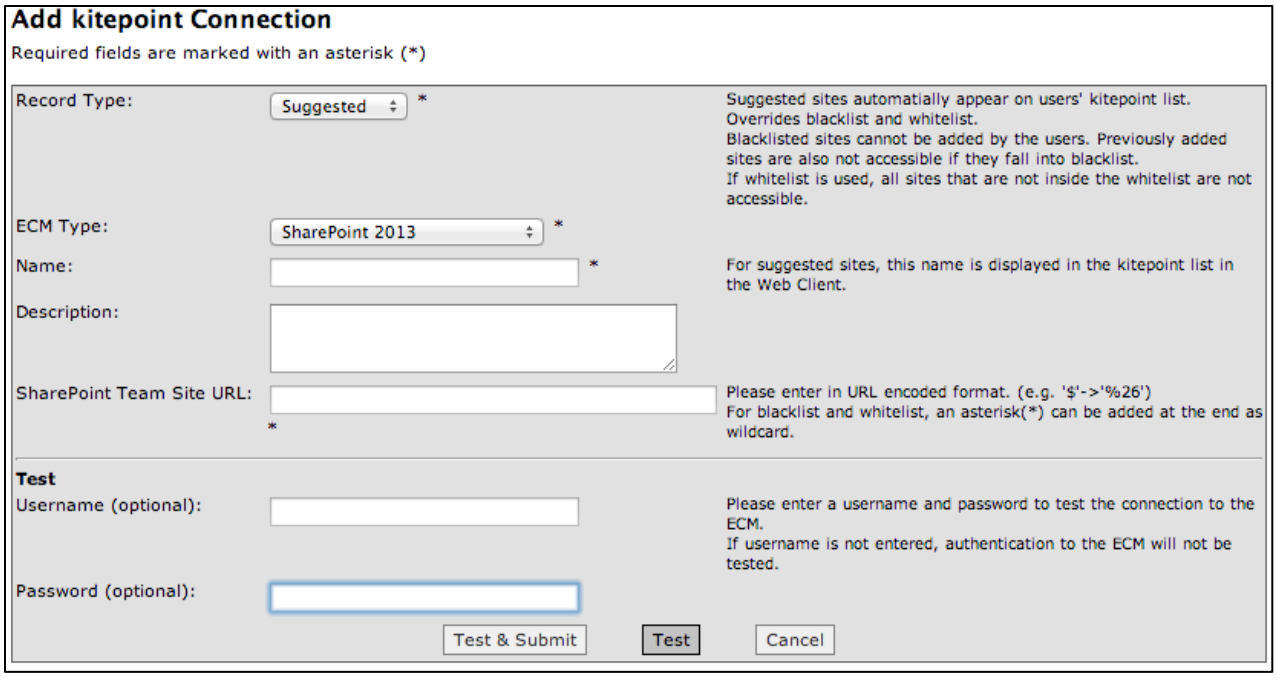
This is the typical menu with settings that control basic functions on the Satellite. Details about these settings are in the *Accellion Administrative Guide*.

Appliance → Kitepoint

On this page all Kitepoint specific settings are accessed.

Follow these steps to add a Kitepoint connection.

1. Click **Add**. The following page displays:



2. Fill in this page with the Kitepoint Connection details as described below.

Record Type – There are three record types available:

- Assigned – These sites automatically appear in the user's kitepoint list.
- Whitelist – This will mask out all sites except the whitelisted sites. &&&
- Blacklist – These sites are not available to the user. &&& Wait... what? Sent message to Singapore

ECM Type – Determines whether the Kitepoint Connection is to a SharePoint 2013, 2010 or 2007 server.

Status – Toggles the Kitepoint service off and on. It can be disabled without deleting if the SharePoint service becomes temporarily unavailable.

Kitepoint Name – This is the name displayed in the Kitepoint list in the Accellion web user interface, as well as the Kitepoint Connection list on the administrative page.

SharePoint Team Site URL – The URL to which this connection maps to when retrieving SharePoint resources.

Description – This will display on the Kitepoint Connection administrative page. It is used only to describe what this connection is.

Username/Password – This is used to test the new Kitepoint Connection. Enter a valid username and password.

Click **Test** to test the username/password, without saving.

Click **Test & Submit** to test the username and password and save any changes.

3. Click **Submit** to creat the Kitepoint Connector.

Another method to test the Kitepoint Connection is to click **Test** in the Actions column**.** The following page displays.

4. Enter a valid SharePoint user name and password and click **Test**.

If it is unable to connect, or if there is invalid information, an error is displayed and the fields with incorrect information are highlighted.

If the Username is incorrect, the following error appears:

Error: Failed to add the connection! Attempting to authenticate as <username>... FAILED.

If this happens, check the username and password, and try again.

Once added the new Kitepoint Connection shows in the table on the Appliance → Kitepoint page. It also displays in the Web Client page of any user whose account has access to those SharePoint resources.

To verify it is active, check the Kitepoint Service on the Administrative web interface on the Satellite under Appliance → Status.

To change any of the settings for an existing Kitepoint Connection, click **Edit**.

To remove a Kitepoint Connection, click **Delete**. You will be asked to confirm the deletion.

To test the connection with alternate user names, click **Test**. This opens a new page. This is used for troubleshooting individual user accounts.

Managing the Kitepoint Satellite

Kitepoint is available via the Accellion web user interface. Any user that authenticates with appropriate MSAD credentials has their available SharePoint resources displayed above the workspaces on the left.

Troubleshooting

Connection Issues – If a user reports an issue connecting, or that SharePoint resources are not available, check the following:

- Verify the account they're using has access to those SharePoint resources. It could be they have multiple accounts, and the account they're logging in with doesn't have access to those resources.
- Check their user account via the Kitepoint Satellite under Appliance → Kitepoint, and click **Test**. Enter that user's credentials in and verify the connection succeeds.

Check Disk Space Error – If the user receives an error such as "Check Disk Space", it could mean the temp directory within the Kitepoint server is full. This directory is cleaned out automatically, with any temporary files older than three days removed several times an hour. To resolve this, wait until the temp directory has been cleaned out, or contact Accellion technical support.

Online Viewer – Advanced Satellite

The Online Viewer – Advanced Satellite handles document rendering for display in the Online Viewer for Web Client and Mobile App users. The Satellite is used in deployments with a heavy usage load where the task of rendering files for display in the viewer must be off-loaded from the Accellion Controller.

Firewall Ports

Service	Type	Port	Direction	Notes
HTTPS	TCP	443	Inbound/Outbound	–
SSH	TCP	22	Inbound/Outbound	–
DNS	UDP	53	Inbound/Outbound	–
AUDP	UDP	8812	Inbound/Outbound	To all Accellion servers
NTP	UDP	123	Inbound/Outbound	–

Deploying

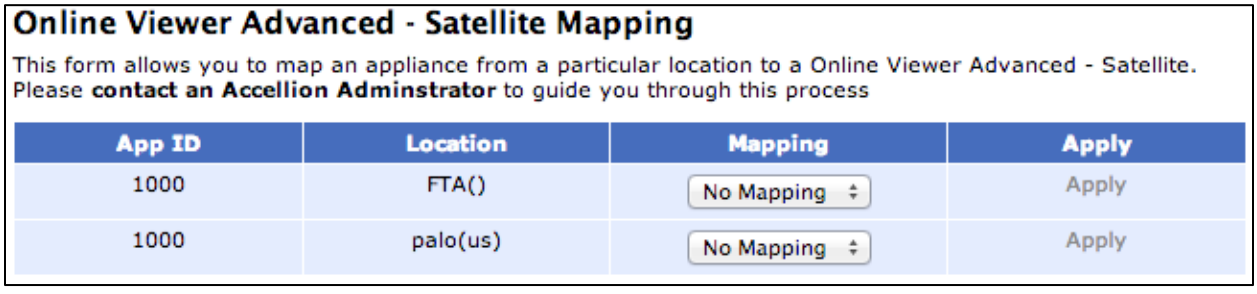
The Online Viewer – Advanced Satellite can be deployed in the same network as the Accellion Controller. It requires a minimum of 4 GB of RAM when used in a virtual environment.

Online Viewer Advanced Satellite Settings

There are no specific settings on the Online Viewer Advanced – Satellite.

Managing the Online Viewer Advanced Satellite

On the Controller, navigate to Administration → Viewer Mappings → Online Viewer Advanced Satellites. From here, you can determine which locations use an existing Online Viewer – Advanced Satellite.



To map an Online Viewer Advanced – Satellite, choose the location under the **Mapping** pull-down menu. All Online Viewer Advanced – Satellites are listed there. Select the new location and the corresponding **Apply** link becomes active. Click **Activate** to save the location change.

When switched, web users who use the Online Viewer function will then be using their designated viewing Satellite. The change is transparent to the users.

Troubleshooting

When adding the Satellite you receive the error:

Error
An error occurred while adding application. Please re-try

This indicates not enough resources are available when setting up the Satellite, or that the Online Viewer – Advanced is disabled on the Controller. It can be enabled under the Settings → Web Client → Features tab. The Online Viewer – Advanced requires 4 GB of RAM and 2 CPUs minimum on both the Controller and Satellite.

All Firewall Ports

Service	Protocol	Source Host	Source Port	Target Host	Target Port	Reason
REQUIRED for all Servers						
HTTP	TCP	Any	–	Server(s)	80	Redirects to port 443.
HTTP	TCP	Server	–	fsbwserver.f-secure.com	80	Allows server to obtain Anti-Virus definition updates (if purchased).
HTTPS	TCP	Any	–	Server(s)	443	Access web interface.
HTTPS	TCP	Server	–	update.accellion.net	443	Allows servers to obtain software updates from Accellion's update server.
DNS	UDP	Server(s)	–	DNS Servers	53	DNS Resolution to allow servers to lookup hostnames.
SMTP	TCP	Server(s)	–	Mail-Gateway server (any)	25	System must send emails and can be configured to deliver email directly or through an SMTP-Gateway.
NTP	TCP	Server(s)	–	NTP Servers	123	Servers must maintain a synchronized time for proper communications and logging.
MPIPE	UDP	Server(s)	1024	Server(s)	8812	Accellion Proprietary UDP communications.
RSYNC	TCP	Server(s)	–	Server (s)	873	RSYNC communication to allow files to replicate between servers.
CONDITIONALLY REQUIRED for all servers – IF IPSEC is not available						
IPSEC	UDP	Server(s)	500	Server(s)	500	IPSEC IKE communication between servers.
OPTIONAL FOR CONTROLLERS						

Service	Protocol	Source Host	Source Port	Target Host	Target Port	Reason
LDAP	TCP	Server(s)	–	Directory Server(s)	389[1]	When purchased user authentication can be integrated with a Directory Server.
OPTIONAL						
SNMP	UDP	SNMP Servers	–	Server	161	Server can be monitored using SNMP polling.
SNMP	TCP	SNMP Servers	–	Server	199	
SFTP	TCP	SFTP Satellites	–	Server	22	Allows communication with SFTP Satellites.
Syslog	UDP	Server	–	Syslog Servers	514	Server can send logging messages to a Syslog Server
SSH	TCP	174.129.220.92	–	Server	22	Allows Accellion to access the system for maintenance and support.
ILO console	TCP	174.129.220.92	–	Server ILO	443 & 23[2]	Allow Accellion to access the ILO console for hardware support and diagnostics.

Note 1: Port 389 for LDAP, Port 636 for LDAPS, Port 3268 for Active Directory Global Catalog.

Note 2: These ports can be changed from ILO interface.

Resources

If you have questions that were not answered by this guide, or technical assistance, visit our support portal at:

https://support.accellion.net/