Rev® Media Management Platform

vbrick rev v7.37

Admin Guide

Copyright

About Vbrick Systems

Founded in 1998, Vbrick Systems is a privately held company that has enjoyed rapid growth by helping our customers successfully introduce mission critical video applications across their enterprise networks. Since our founding, Vbrick has been setting the standard for quality, performance and innovation in the delivery of live and stored video over IP networks—LANs, WANs and the Internet. With thousands of video appliances installed world-wide, Vbrick is the recognized leader in reliable, high-performance, easy-to-use networked video solutions.

Vbrick is an active participant in the development of industry standards and continues to play an influential role in the Internet Streaming Media Alliance (ISMA), the MPEG Industry Forum, and Internet2. In 1998 Vbrick invented and shipped the world's first MPEG Video Network Appliance designed to provide affordable DVD-quality video across the network. Since then, Vbrick's video solutions have grown to include Video on Demand, Management, Security and Access Control, Scheduling, and Rich Media Integration. Vbrick solutions are successfully supporting a broad variety of applications including distance learning and training, conferencing and remote office communications, security, process monitoring, traffic monitoring, business and news feeds to the desktop, Webcasting, corporate communications, collaboration, command and control, and telemedicine. Vbrick serves customers in education, government, healthcare, and financial services markets among others. Vbrick products are manufactured in an ISO certified manufacturing facility.

Contents

Devices

Media Settings

Integrations

System Settings

Accounts

LDAP

Rev Technical Requirements

Rev Admin Guide

Admin Guide Preface

This guide is written for anyone who will be using or evaluating the Vbrick Rev® media management platform with administrative access. This includes system administrators, software developers, network technicians, and others.

Rev Admin Interface Overview	Describes how to log in and out of the application, access Admin functions, and explains the Admin GUI.
Account Reports	Details the Admin **Home Page** and reporting metrics of Vbrick Rev.
Users	Details the **Users** menu options and how to create, activate, and manage Users, Groups, Channels, and Roles.
Devices	Details how to manage **Devices**, **Presentation Profiles**, and **Zones**.
Media Settings	Covers how to configure **Media Settings** for content in Rev including **Categories**, **Player Settings**, **Recording Settings**, **Transcoding Presets**, **Features**, and creating **Approval Processes**.
System Settings	Understand how to configure detailed system information such as **User Password Parameters**, **API Keys** and your system's email **Environment**.
Accounts	Explains the **Accounts** menu and modules in detail including the **Contact & Billing** module and **Child Accounts** module.
LDAP	Step-by-step instructions for importing and using LDAP groups with Vbrick Rev.

Getting Help

If you can't find the information you need from the online help system, or from your certified Vbrick reseller, you can contact Vbrick Support Services on the Web. Support Services can usually answer your technical questions in 24 business hours or less. Also note that our publications team is committed to accurate and reliable documentation and we appreciate your feedback. If you find errors or omissions in any of our documents, please send e-mail to documentation@vbrick.com and let us know. You may also send feedback about a specific topic using the e-mail icon in the upper right corner.

> **Additional Information**: Vbrick has made every effort to ensure that the information in this document is accurate at the time of publication. Vbrick reserves the right to make changes without notice. To see the latest documentation for all products go to https://portal.vbrick.com.

Tip: All versions of help may be viewed in PDF format for easy portability but are optimized for the Web and are best viewed Online.

Chapter 1

Rev Admin Interface Overview

Access Admin Menu Functions

The Admin **Reports** page is automatically displayed when you log in with a valid **Username** and **Password** and access the Admin menu bar. All Rev functionality and menu bar commands are available from this page but users may not have access to all depending upon the user permissions that you have been granted.

Click the **Gear** icon in the upper right corner of the user menu bar to access Admin menu bar features and functions. Note: Only specific Admin roles have access to the Admin menu bar.

Admin menu bar functions will appear under the user account menu bar functions.

Admin Header Navigation Options

The options available on the menu bar will vary depending upon your user permissions and account access. For example, when you first log in, the menu will display the options for a non-admin user. However, if you log in as an Account Admin, the menu bar will display the Admin menu functions that are seen below. (Note: Media Admin options include only the **Media Settings** menu.)
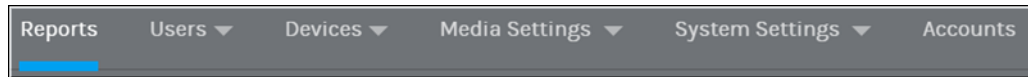
Option	Description
Parent and Child Menu	Provides the ability to navigate between any parent and child accounts that have been created in Rev. Organization/Account names will be displayed with the Parent account defaulted. The image above uses a sample parent account titled "Rev Global Solutions" as an example.
Account Reports	Explains the Admin **Reports** page and various report data available to Admins in Vbrick Rev.
Users	Details on creating, activating, and managing user accounts. Also nests the **Groups**, **Channels**, and **Roles** menus.
Devices	How to manage **Devices**, **Presentation Profiles**, and **Zones**.
Media Settings	Covers how to configure **Media Settings** for content in Rev including **Categories**, **Player Settings**, **Recording Settings**, **Transcoding Presets**, **Features**, and creating **Approval Processes**.
System Settings	Explains detailed system information such as **User Password Parameters**, **API Keys**, and your system **Environment**.
Accounts	Explains the **Accounts** menu and user modules in detail including the **Contact & Billing** and **Child Accounts** modules.

Role(s): Access: Account Admin (all), Media Admin (restricted)

Interface Overview

User Menu Bar

Account Reports

The Admin Report Dashboard

The Admin **Report** dashboard consists of data related to video views, user accounts, and Rev usage created to assist you in monitoring how your Rev media management system is being utilized in sum. The dashboard is displayed when you first access account Admin features through the **Gear** icon and when you click on the **Reports** menu bar option and may be viewed by account and media Admin roles. Each tab of the dashboard and its corresponding data break down is detailed below.

Admin Report Videos Tab

The **Videos** tab of the Admin report details viewing and completion rate trends for all of the videos in Rev.

This tab will include the following data:

• Total number of videos added to Rev

• Total views in the last 30 days

• Completion rate when viewing videos

• Video views in the last 30 days by day

• Top 20 videos viewed. Rolling the mouse over a video in this list will also show its **Total Views**. **Total Views** for a video may also be seen in the **Video Player**.
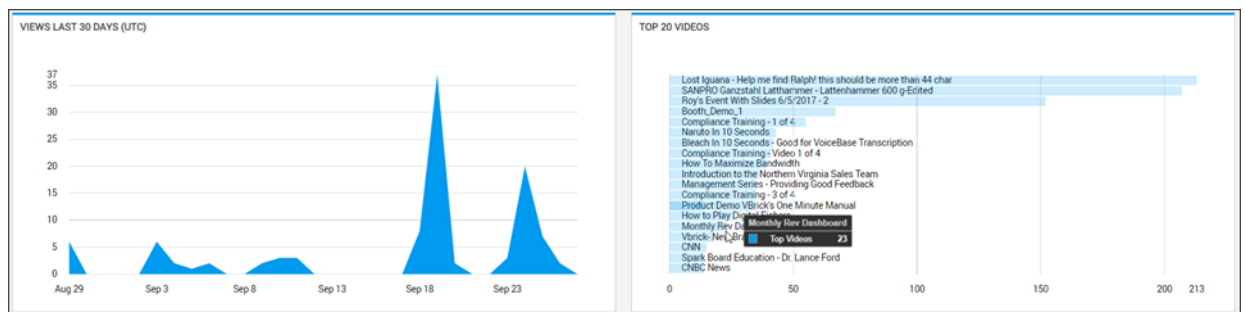
Admin Report Users Tab

The **Users** tab of the Admin report details user account stats and device usage in Rev.

This tab will include the following data:

• Average number of daily log-ins

• Total number of licensed users

AVERAGE DAILY LOGINS	TOTAL LICENSED USERS
11	79

- User account login totals by day (rolling over a specific day includes the daily total)
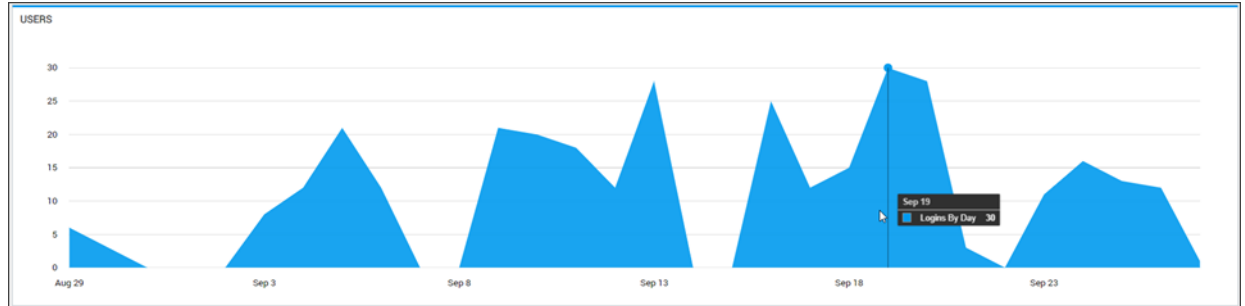
- Device stats such as logins by browser and logins by device
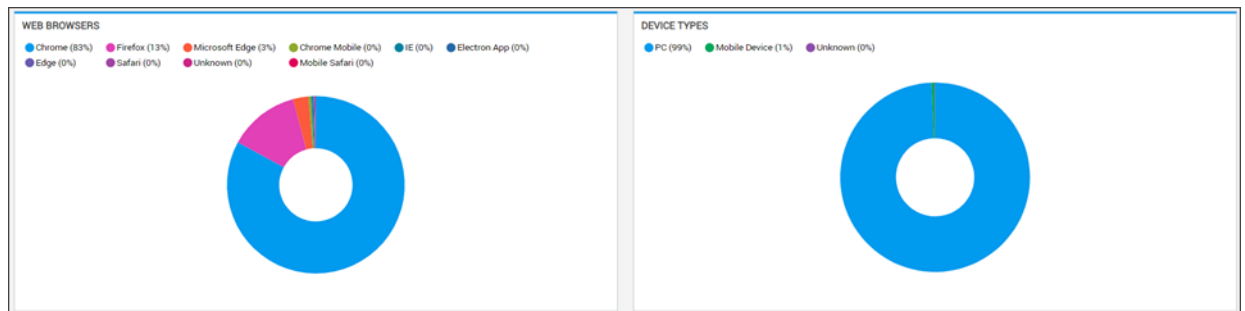
Admin Report Usage Tab

The **Usage** tab of the Admin report details Rev back-end statistics regarding licensing and disk space.

This tab will include the following data:

- Viewing hours buckets that have been configured are displayed and include the total number of hours in each bucket along with the expiration date. The number of hours remaining in each bucket is also displayed.
- More than one viewing hours bucket, with varying expiration dates, may be configured. The usage will always be deducted from the viewing hour bucket with the earliest expiration date.
- Total Webcast hours remaining including internal versus public Webcasts and recording hours remaining.
- Rev IQ credits allocated and remaining and the expiration date, if licensed.
- The total amount of disk space in MB or GB that is currently in use.

TOTAL VIEWING HOURS	VIEWING HOURS USAGE	TOTAL AMOUNT OF DISK SPACE USED
1162	998 Hours Left Licensed: 1,000 Expires: Jul 3, 2020	34.505GB

TOTAL WEBCAST HOURS		TOTAL VOD HOURS		TOTAL RECORDING HOURS	REV IQ CREDITS
1129		30		4	99,000 Credits Left Licensed: 100,000 Expires: Dec 31, 2024
Internal 1108	Public 20	Internal 28	Public 1		

Apply a License Type or Add-On Component to a Child Account

Export Video Viewership and Inventory Reports

The Admin report dashboard may be exported into two separate CSV Excel spreadsheets to save and review. Further, the spreadsheet has more details that may be desirable to you than simply viewing them on the dashboard in Rev. You may export a viewership report or an inventory report. Both are described below.

> **Note**: The **Video Inventory** report is generated asynchronously and you are notified when your download is complete to better support larger video libraries.

Video Viewership Report Export

▼ To export a viewership report:

1. Access the account report dashboard by clicking the **Gear** icon or the **Reports** menu option once in Admin view.
2. Click the **Videos** tab.
3. Select **Viewership Reports** in the **Video Reports CSV** dropdown
4. Select the date range you want to export. Note that this range only applies toward the csv export and is not applied to the report dashboard. Further, you may not use a date range on mobile devices though you may use your tablet. You may choose:
   - Today
   - Yesterday
   - Last 7 Days
   - Last 30 Days
   - Custom (A range you specify with a maximum 12 month period able to be defined)
5. Click the **Download** button in the upper right corner.
6. The **AccountVideoSessions.csv** file will be placed in your **Downloads** folder with the following data collected:
   - Date [each video] is viewed
   - Video ID
   - Title of each video
   - Description of each video

- Duration of each video - This is the viewing time of the user watching the video during that session.
- Username of person who viewed the video - This will be blank if the user was external (public video).
- First name of person who viewed the video - This will be blank if the user was external (public video).
- Last name of person who viewed the video - This will be blank if the user was external (public video).
- Email address of person who viewed the video - This will be blank if the user was external (public video).
- IP address of person who viewed the video
- Whether or not the video was completed - This will be true or false. Note that a viewing sessions is considered "complete" when viewing time is at least 90% of the video's duration.
- Zone the video was viewed from - Rev indicates if playback is not through a Zone. This could be because the video was not served by a DME or because the user's IP address does not fall into one of the defined Zones and the Default Zone is not configured to serve this video. In this case, the user is served the video directly from the Rev server or Cloudfront, depending on account configuration.
- Device that was used to view the video - See notes for Zone.
- Playback URL

Video Inventory Report Export

> **Note**: The **Video Inventory** report is generated asynchronously and you are notified when your download is complete to better support larger video libraries.

▼ To export a video inventory report:

1. Access the account report dashboard by clicking the **Gear** icon or the **Reports** menu option once in Admin view.
2. Click the **Videos** tab.
3. Select **Inventory Reports** in the **Video Reports CSV** dropdown.
4. Click the **Download** button in the upper right corner.
5. The **VideoInventory.csv** will be placed in your **Downloads** folder with the following data collected (Note: Report translated to user's language if applicable):
   - Video ID
   - Title
   - Upload Date (account time zone)
   - Uploaded By (Uploader User Account)
   - Duration of video in format hh:mm:ss
   - Status (Active or Inactive)
   - Last Viewed (account time zone)
   - Completion Rate (percentage) - This is the percentage of viewers who completed the video. Note: A viewing sessions is considered "complete" when the viewing duration is at least 90% of the video's duration.

- Content Type ("Live" or "VOD")
- Publish Date - This is the date the video was initially activated or a custom date set by the video owner.
- Expiration Date; only for specific date, expiration rules are not specified here.
- Access Control (private, public, channels, or all users)
- Enabled Downloads: Yes or 'blank' for No
- Enabled Comments: Yes or 'blank' for No
- Enabled Ratings: Yes or 'blank' for No
- Categories assigned
- Tags assigned
- Custom Fields assigned
- Number of comments received
- Average Rating
- Total Views - This is the total number of times the video was played. Views are aggregated until a viewer has completed watching the video and then restarted. This means you can have multiple views of a video for one user.
- Downloads (Total) - Number of times the video has been downloaded. This includes downloads that have occurred both through Rev and the API.
- Source of the Video (upload, scheduled event, Webex, upload360, scheduled recording, or link)
- Source Type of the Video (Rev, API, Video Conference, Webex)

Chapter 3

Users

Users Menu Overview

The **Users** menu is an Admin only feature and enables you to add and manage the user accounts in Vbrick Rev as well as groups, channels, and roles. After a new account has been added, it is an unlicensed account and must be activated or confirmed so that its status becomes active.
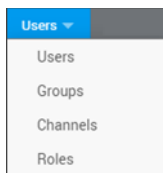
Once the user account is active in the system, you may then assign the account a **Role** that has certain permissions defined such as the ability to view content, edit content, and upload content. You may also add the user to a **Group**. Groups are formed of users that often need to perform similar functions or tasks. Further, groups may be granted view or edit access to specific videos in addition to user accounts.

Finally, **Channels** are another means to bundle user accounts and groups together that may need to share function, content, or video access.

The Users Module

The Groups Module

The Channels Module

The Roles Module

The Users Module

The **Users** module is displayed when you click the **Users** menu bar. Use it to add, configure, and manage the user accounts in your system.

The **Users** module displays:

Column	Description
Name	The first name and last name of the user account.
User Name	Used to log in to the system.
Status	The status of the user account; The status may be unlicensed, active, inactive, awaiting password reset, locked out, or suspended.
Email	The active email address for the user account.
Actions	The actions you may perform on a user account. • **Delete** — Deletes a user account. • **Suspend** — When an account is suspended, the user may not log in. • **Activate** — Click to activate a previously suspended account. The **Activate** button will not be present unless a user account is suspended.

Additional functionality:

Function	Description
Add User	Creates a new user account.
Find User	Filters specific user accounts when you have several created.
Download	Download a list (csv file) of user accounts in the system.
View User Status Summary	A summary of user account statuses is provided above the Find User dialogue box for each Rev account. It includes: • Licensed user accounts • Unlicensed user accounts • Total users See: View a Summary of User Account Licensing Statuses for Rev

The Groups Module

The Channels Module

The Roles Module

Add or Edit a User Account

You must have the Account Admin role to add or edit a user account. This topic discusses how to add a user from Rev. Many user accounts will be imported and managed with LDAP groups. You may also add users or groups through the upload process.

> **Note**: If you have imported your user from an LDAP group, you will only be able to edit the **Preferred Language**, **Assigned Role**, and Rev **Assigned Group** of the user. All other attributes must edited from LDAP.

▼ To add or edit a user account:

1. Navigate to **Admin** > **Users** > **Add User** button.

2. Complete the **New User** section and click **Create User**.

> **Tip**: Click a **User Name** to edit the account. The **Username**, once saved, may not be edited.

Field Name	Required	Description
First Name		First name of the account holder. Text only.
Last Name	Yes	Last name of the account holder. Text only.
Contact Email		Email of the account holder. Must be a valid email address.
Title		Preferred title of the account holder. Text and numerical input accepted.
Phone Number		Phone number of the account holder.
Preferred Language		Preferred language of the account holder.
Username	Yes	Used to log in to the system. Email address is also accepted. Field *must* be unique in the system. This is not case sensitive. This field name may not be edited once saved.

You do not have to add groups or roles when you initially create a user account (a default role is assigned).

As soon as you click the **Create User** button, the user account is set to "unlicensed" status until the user logs in for the first time. At that point, it will be set to "active" status.

An email will be generated by the system and sent to the user so that they may create their own password and security question and log in. Upon logging in, the account status will be updated to "Active".

> **Note:** As mentioned, an email notification is generated to the user with instructions for setting up a password if an email server has been put in place. If you do not have this server set up, you will have to manually confirm and activate each account that is created. This is not recommended.
>
> You should also keep in mind that if your Rev environment is not ready for launch, you should delay setting up user accounts.
>
> For more information, view Rev Supplementary Documentation > Devices & Technical References > Root User Functions Guide > "Email Server Information".

> **Note**: If a user account is created on a Rev system with SSO enabled, the account will be created with no user confirmation required and, further, no email will be generated to the user. However, the account status will remain "unlicensed" until the user logs in for the first time and becomes "active". See: Configure Single Sign On (SSO).

> **Note**: If user accounts are being managed by LDAP, these options will not be available. Instead, user accounts are imported with Groups and LDAP. See: Import an LDAP Group.

View License Usage Summary

Create or Edit an Approval Process

Upload and Edit User Accounts and Groups Using a CSV File

Add or Remove a Group from a User Account

You must have the Account Admin role to add or remove groups from a user account.

▼ To add or remove a group:

1. Navigate to **Admin** > **Users** > **User Account.**
2. Use the **Group Assignment** section to add and remove groups.
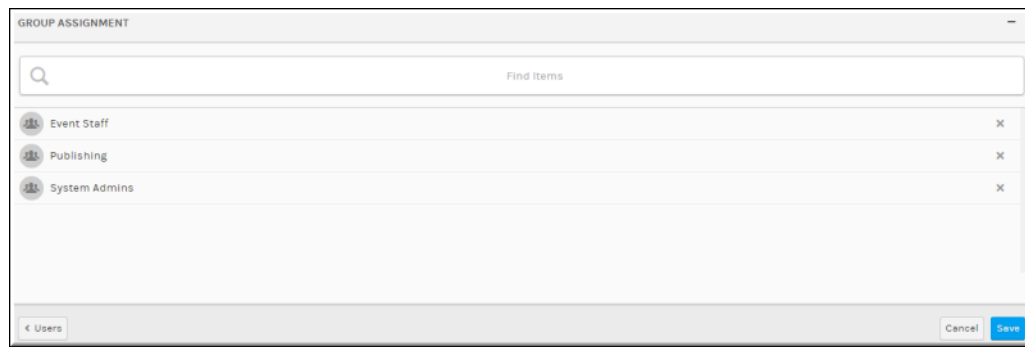
Field/Function	Description

Find Items	Begin typing the name of the group in the **Find Items** box and Rev will suggest possible existing entries for you. Select the entry you want to add and click **Done**. Click the **X** if you want to remove the group from the user account.
Save	Click to save the user account once you have completed all entries.

> **Note**: It is not a requirement that a group be assigned when creating or editing a user account. You may also add a user account to several groups at once using the upload functionality.

Add or Remove a User from a Group

Add or Edit a Group

Upload and Edit User Accounts and Groups Using a CSV File

Add or Remove a Role from a User Account

You must have the Account Admin role to add or remove roles from a user account.

▼ To add or remove a role:

1. Navigate to **Admin** > **Users** > **User Account.**
2. Use the **Role Assignment** section to add and remove roles.
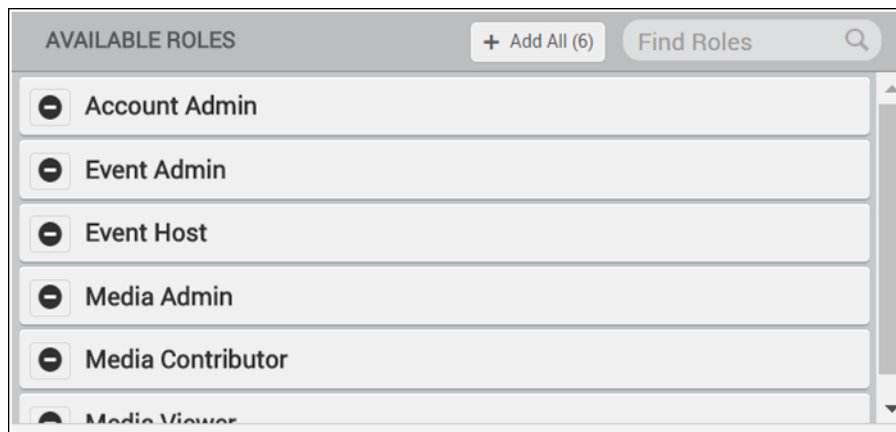
Field/Function	Description
Available Roles	Click on a role in this column to move it to the **Assigned Roles** column.
Add All	Click the **Add All** button to add *all* roles in the **Available Roles** column at once to the user account at once.
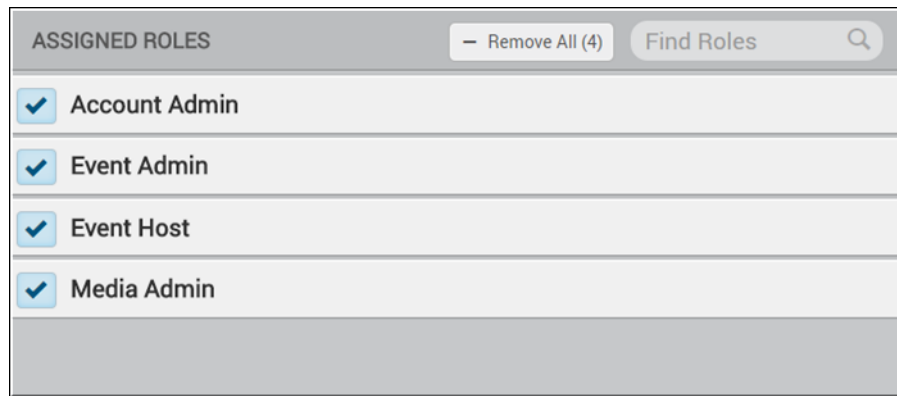
Field/Function	Description
Assigned Roles	Click on a role in this column to remove it from the user. It will appear back in the **Available Roles** column once again.
Remove All	Click the **Remove All** button to remove *all* roles in the **Assigned Roles** columns from the user at once.

Add or Remove a Role from a Group

User Roles and Permissions by Function

Obtain a URL for a Lost or Blocked Registration Email for a New User Account

When a new user is created, the account status is automatically set to "Unlicensed". An email notification is generated to the user with instructions for setting up a password and security question if an email server has been put in place. See the "Email Server Information" topic in the Rev Root Account User Guide on the Documentation Site for more information.

At that point, the new user needs to simply complete their registration and log in. The status of the account will then be set to "Active". See: Create a Rev User Account.

However, if you do not have this server set up, you will need to manually send a registration URL for each account that is created. This is not recommended.

Manually obtaining a registration URL for each account entails editing each account that is in "Active" status. This step may also be performed should the user misplace the system generated email or if it is blocked by the user's spam filter for example.

> **Note**: If user accounts are being managed by LDAP, passwords and security options are not managed through the Vbrick Rev interface.

▼ To obtain a user confirmation URL:

1. Navigate to **Admin** > **Users** > **User Account.**

2. Under **Administrative Actions** > click the **Show** button. This button is only available if the user's status is "Unlicensed".

3. The **User Confirmation URL** will appear.

4. You may send this URL to the user in a new email to complete the registration and activation process.

> **Tip**: The button functions available in **Administrative Actions** vary based on the account's status. Example: "Unlicensed" and you are able to obtain the **User Confirmation URL** to complete the registration process; "Locked Out" and you are able to **Unlock** the account, and so forth.

Add or Edit a User Account

View License Usage Summary

Reset a User's Password

There may be times when you need to manually reset a user's password.

> **Note**: If user accounts are being managed by LDAP, passwords and security options are not managed through the Vbrick Rev interface.

▼ To reset a user's password:

1. Navigate to **Admin** > **Users** > **User Account.**

2. Under **Administrative Actions** > click the **Reset Password** button. This button is only available (by itself) if the user's status is "Active" and *not* in locked out status.

3. A reset password email will be sent to the user with a link to reset their password.

4. Just as with the initial registration email, the email server must be configured before this email may be sent. See: "Email Server Information" in the Rev Root Account User Guide on the Documentation Site for more information.

5. The user account's status will be set to "Awaiting Password Reset".

6. The user must answer his/her security question to reset their password. The password complexity rules set for the system still apply.

7. The password reset link will be in effect for 72 hours.
8. If you need to manually send the password URL, you may do so from the user account **Administrative Actions** section by clicking the **Show** button (similar to obtaining the confirmation URL manually). See: <u>Obtain a URL for a Lost or Blocked Registration Email for a New User Account</u>.

> **Tip**: The button functions available in **Administrative Actions** vary based on the account's status. Example: "Unlicensed" and you are able to obtain the **User Confirmation URL** to complete the registration process; "Locked Out" and you are able to **Unlock** the account, and so forth.

<u>Reset Your Rev User Account Password or Security Question</u>

<u>View License Usage Summary</u>

Unlock a User's Account

If a user has been locked out of his/her user account and is unable to reset the password through the **Forgot Password** link, you have the ability to either unlock the account or reset the password as the case may be.

See: <u>Configure User Lockout Settings</u> for more information on configuring lockout settings.

> **Note**: If user accounts are being managed by LDAP, passwords and security options are not managed through the Vbrick Rev interface.

▼ To unlock a user's account:

1. Navigate to **Admin** > **Users** > **User Account.**
2. Under **Administrative Actions** > click the **Reset Password** button to generate an entirely new password for the user. See: Reset a User's Password.
3. Click **Unlock** to unlock the user's account. The previous password will still be in place.
4. The user's account status must be either "Active" or in "Locked Out" status for these two buttons to be present at the same time.
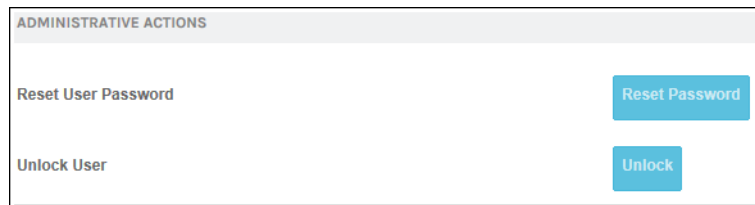
> **Tip**: The button functions available in **Administrative Actions** vary based on the account's status. Example: "Unlicensed" and you are able to obtain the **User Confirmation URL** to complete the registration process; "Locked Out" and you are able to **Unlock** the account, and so forth.

Reset Your Rev User Account Password or Security Question

View License Usage Summary

Reset a User's Security Question

If a user has been locked out of their account and incorrectly answers the **Security Question** needed when attempting to reset it through the **Forgot Password** link, you have the ability to reset the question for the account. **Security Question** maximum attempts are dictated by the same rules as password and lockout settings.
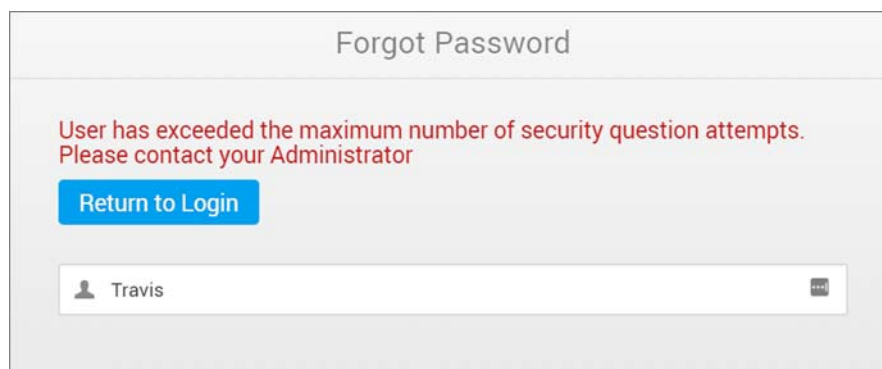
See: <u>Configure User Lockout Settings</u> for more information on configuring lockout settings.

> **Note**: If user accounts are being managed by LDAP, passwords and security options are not managed through the Vbrick Rev interface.

▼   To reset a user's security question:

1. Navigate to **Admin** > **Users** > **User Account.**
2. Under **Administrative Actions** > click the **Reset Security Question** button to generate an email to the user that will prompt the creation of a new password and security question.
3. This button is only available if the user has incorrectly answered his/her security question when clicking the (**Forgot Password?**) hyperlink on the login screen. The amount of times he/she must answer incorrectly is set under Rev Security Settings.

4. The reset link will be in effect for 72 hours.
5. If you need to manually send the reset URL, you may do so from the user account **Administrative Actions** section by clicking the **Show** button (similar to obtaining the confirmation URL manually). See: <u>Obtain a URL for a Lost or Blocked Registration Email for a New User Account</u>

> **Tip**: The button functions available in Administrative Actions vary based on the account's status. Example: "Unlicensed" and you are able to obtain the User Confirmation URL to complete the registration process; "Locked Out" and you are able to Unlock the account, and so forth.

<u>Reset Your Rev User Account Password or Security Question</u>

<u>View License Usage Summary</u>

Suspend a User Account

Only an Account Admin may suspend a user account. When a user account is suspended, the user may not log-in and, if the user is logged in at the time the account is suspended, they will be logged from the system immediately. If a user attempts to log in when the user account is suspended, an error message will result, "<User Account> is Suspended. Please contact your Administrator.".

Keep in mind:

- You may not suspend your own account.
- You may consider suspending accounts as opposed to deleting them.
- Suspended accounts are noted in the **Status** column of the **Users** module.
- An LDAP user account may be suspended if the source of the account is removed (the LDAP group). See: <u>Delete or Suspend an LDAP Group or User</u> for information on how to remove this status.
- Users that are suspended manually through this drop-down will *not* be deleted when an LDAP sync is run again if the **Delete Suspended Users** checkbox is enabled. (See: <u>LDAP</u>

Server Synchronization Settings for details on how to delete users that have never logged in to Rev and are suspended.)
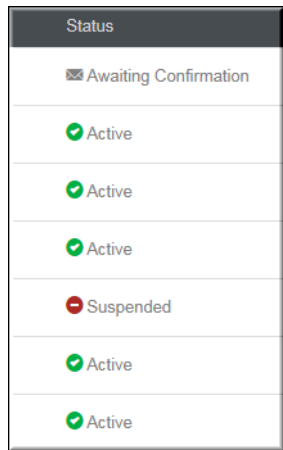
▼   To suspend a user account:

1.   Navigate to **Admin** > **Users.**

2.   In the **Actions** column, click the **Suspend User** button.
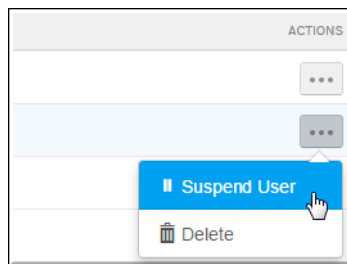
3.   Click the **Activate User** button on a suspended account to reactivate the account.

Delete a User Account

Only an Account Admin may delete a user account. When a user account is deleted, it may not be recovered so use with extreme caution.

Keep in mind:

•   You may not delete your own account.

•   You may delete user accounts imported through LDAP, however, if a sync occurs again, they will be re-imported. It is better to manage the deletions through LDAP. Only suspended users that have never logged in will be automatically deleted forever when synced. (See: LDAP Server Synchronization Settings for details on how to delete users that have never logged in to Rev and are suspended.)

•   You may consider suspending accounts as opposed to deleting them. (See: Suspend a User Account)

•   Users that are suspended manually through this drop-down will *not* be deleted when an LDAP sync is run again if the **Delete Suspended Users** checkbox is enabled. (See: LDAP

Server Synchronization Settings for details on how to delete users that have never logged in to Rev and are suspended.)
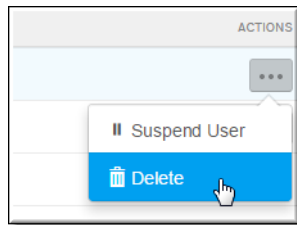
▼ To delete a user account:

1. Navigate to **Admin** > **Users**.
2. Click the **Actions** dropdown > **Delete** button of the **Account Name** you want to delete.

Delete or Suspend an LDAP Group or User

View License Usage Summary

View License Usage Summary

You can easily view how many users are in your system, as well as how many licenses you have consumed for an account, on the **Users** module main page.

▼ To view a summary of license usage on your system:

1. Navigate to **Admin** > **Users**.
2. Licensing status is displayed in the upper left corner of the module page above the **Add User** and **Upload Users** button(s).
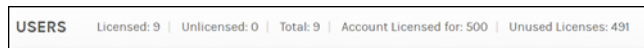
Keep in mind:

- Users are not counted as licensed users until they log in.
- Unlicensed and Suspended status states do not count toward the number of licensed users displayed.
- Active, Locked Out, Awaiting Password Reset, and Awaiting Security Question Reset do count toward the number of licensed users for a Rev account.
- If a user attempts to log in to a Rev account that does not have any licenses available, the user will not be able to log in and a message will be displayed to contact the Rev Administrator.

The Users Module

Add or Edit a User Account

Upload and Edit User Accounts and Groups Using a CSV

File

You may quickly upload and edit multiple user accounts and groups at once using a .csv file if you need to do so without an LDAP import. Further, you may also add and remove the user accounts to multiple groups at once as well using the group association feature. If the groups do not exist in Rev, you may create them during the process.

> **Caution**: You *must* save the CSV file encoded in the UTF-8 format. Otherwise certain characters may not be displayed correctly.

Keep in mind:
- Only .csv files are accepted
- Field names must be in the first row of the file (see sample below).
- Certain fields must be unique and are also required (noted below).
- User accounts are unlicensed when created and do not count toward your licenses until logged in.
- Uploaded user accounts are assigned to the Media Viewer role only.

User Account CSV File Format and Values

Only .csv files are accepted and you must make sure they are formatted correctly. The sample .csv file here is described below.

Download a sample CSV file here.

	A	B	C	D	E	F	G	H	I
1	UniqueId	Username	Lastname	Firstname	Title	PhoneNumber	Email	GroupNames	Action
2	EmployeeID001	randy.omid	Omid	Randy	Title 001	703-123-0001	randy.omid@vbrickTEST.com	Project Managers; Live Stream Events	
3	EmployeeID002	edward.barrett	Barrett	Edward	Title 002	703-123-0002	edward.barrett@vbrickTEST.com	Project Managers; Live Stream Events	
4	EmployeeID003	kathryn.gent	Gent	Kathryn	Title 003	703-123-0003	kathryn.gent@vbrickTEST.com	Project Managers; Live Stream Events	
5	EmployeeID004	mildred.benner	Benner	Mildred	Title 004	703-123-0004	mildred.benner@vbrickTEST.com	Project Managers; Live Stream Events	
6	EmployeeID005	susan.palmer	Palmer	Susan	Title 005	703-123-0005	susan.palmer@vbrickTEST.com	Project Managers; Live Stream Events	
7	EmployeeID006	larry.marble	Marble	Larry	Title 006	703-123-0006	larry.marble@vbrickTEST.com	Project Managers; Live Stream Events	
8	EmployeeID007	calvin.cummings	Cummings	Calvin	Title 007	703-123-0007	calvin.cummings@vbrickTEST.com	Project Managers; Live Stream Events	
9	EmployeeID008	michelle.miller	Miller	Michelle	Title 008	703-123-0008	michelle.miller@vbrickTEST.com	Project Managers; Live Stream Events	
10	EmployeeID009	takisha.hill	Hill	Takisha	Title 009	703-123-0009	takisha.hill@vbrickTEST.com	Project Managers; Live Stream Events	
11	EmployeeID010	arthur.gibson	Gibson	Arthur	Title 010	703-123-0010	arthur.gibson@vbrickTEST.com	Project Managers; Live Stream Events	

Field	Description
Title Row (Row 1)	Field names (UniqueId, Username, Lastname, Firstname, and so forth) must appear in Row 1 (highlighted above) and may not be changed.
Uniqueid	This is a required field and must be unique. You may use employee ID or any unique ID of your choosing.
Username	This is a required field and must be unique. This will be used to log in to Rev.
Lastname	Required field. Last name of the user account.
Firstname	First name of the user account. Not required.
Title	Title of the user account. Not required.
PhoneNumber	Phone number of the user account. Not required.
Email	This field must be unique if used. Not required. Email address of the user account. This field must also be in correct email-format (name@subdomain.top-level-domain)

GroupNames	Optional field. Group(s) to associate the user accounts to. If the groups do not exist they will be created if the **Create Groups** checkbox is selected. More than one group should be separated by a semicolon.
Action	Optional field. Use 'd' to delete the user account. Use 's' to suspend the user account. Leave blank to create the user account with the defaults specified.
	Delete or suspend applies to user accounts already existing in Rev.

For each row:

- If a user row is missing a required field, the user account will not be created.
- If a user account with the same email address already exists in Rev, the new user account will not be created.
- If a user account with the same username already exists in Rev, the new user account will not be created.

Upload a CSV File to Create User Accounts and Groups

Once you have your .csv file formatted and filled out correctly, you are ready to upload.

▼   To upload user accounts and groups:

1. Navigate to **Admin** > **Users** > **Upload Users** button.
2. Click the **Add File** button to select the .csv file to use. (Note: When a .csv file is attached, the **Submit** button becomes active.)

3. If you have groups you want created, click the **Create Groups** checkbox.
4. If your user accounts should be added to the groups you specified in the .csv file GroupNames column in addition to any *currently* existing groups they may belong to (if you are editing user accounts) then select the **Append** radial.
5. If your user accounts should *only* be added to the groups you specified in your .csv file, select the **Replace** radial. This means that any current group associations in Rev will be removed and only those groups in the .csv file will be associated to the user accounts going forward.
6. Click the **Submit** button to upload your file and create (or edit) your user accounts. User accounts will receive an email notification to log in and create their accounts through the usual verification process unless you are using SSO.

7. You will receive a notification in Rev and through email once your upload is complete stating how many accounts and groups have been created or if there were any errors.

> ✔ **Users Upload Completed.**
> You have successfully created 10 new users.
>
> You have successfully created 2 new groups.
>
> Nov 29, 2016 2:17 PM
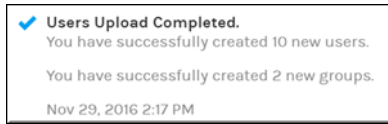
> **Tip**: If you plan on adding or editing several accounts, the upload feature will let you perform a test on one row. A test upload is recommended before creating several groups or deleting/suspending several accounts to make sure your settings and .csv file accomplish what you intend.

> **Note**: Customer accounts with child accounts are not permitted to modify account users by using the upload .csv feature from the parent account.
>
> If there is a need to modify users in a child account via the .csv upload method, then those changes should be made directly in that child account.

The Users Module

Add or Edit a User Account

Add or Remove a Group from a User Account

Download a List of All User Accounts

Account Admins may use the Download button to export a csv file of all user accounts in the system. This button is not present if you do not have Account Admin access. For those Rev clients that have large amounts of users, the download process will prepare in the background. A notification and email will be sent to the Admin Account that prompted the download when it is ready for downloading.

▼ To download a list of user accounts in Rev:

1. Navigate to Admin > Users.
2. Click the **Download** button.
3. As noted, if the download is large, you will be notified by email and Rev notification when it is ready to download.

> INITIATE DOWNLOAD   ✕
>
> Your file download is being processed. We will notify you when the file is ready.
>
>   Cancel   Save
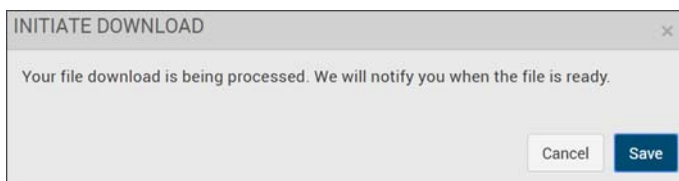
4. Once ready, access the **Notification** menu and click the **Download** notification link to begin csv download. See: Viewing Your Notifications

> **Today**
>
> ✔ Your user file is ready for download
>   DownloadUsers_636fl46586201888793.csv
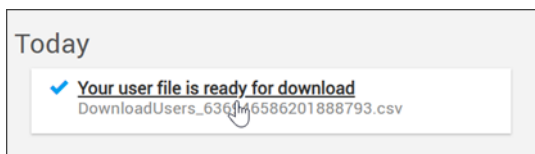
The following fields are contained in the csv download:

- Username
- First Name
- Last Name
- Email Address
- Title
- Phone Number
- Status (Active, Unlicensed, Awaiting Password Reset, Awaiting Security Question Reset)
- Licensed (T or F)
- Preferred Language
- Roles
- Group Assignments
- LDAP Group Assignment
- Channel Names
- Source (System, LDAP)

The Groups Module

Use the **Groups** module to add, configure, and manage the groups in your system. You must have the Account Admin role to manage groups.

The **Groups** module contains:

Column	Description
Name	A descriptive name is helpful if you want to understand what the group's function is at a glance.
Users	The number of users currently assigned to the group; note that this may differ from the number of users that may be available [to assign] to the group.
Source	Details the source of the group's creation; via an add through Vbrick Rev (System Group) or an import from LDAP.
Actions	The actions you may perform on a **Group**: • **Delete** — Deletes a group.

Additional functionality:

Function	Description
Add Group	Creates a new group on the **New Group** page with the ability to add roles and user accounts available.
Quick Add	Quickly creates a group without the ability to add attributes to it immediately available.
Import Group From LDAP	Imports a group from LDAP; LDAP must be configured and an **LDAP Connector** must be set up first. Further, the **Specify Groups to Import** checkbox must be deselected for this button to be visible. See: Add an LDAP Connector Device.
Find Group	Filters to find a specific group if several have been imported or created.

Configure and Import LDAP Groups in Vbrick Rev

Add or Edit a Group

When creating a new group, you may add it from the Vbrick Rev interface or import it from LDAP. This topic discusses adding or editing a group from Vbrick Rev. You must have the Account Admin role to use this functionality.

▼ To add or edit a group:

1. Navigate to **Admin** > **Users** > **Groups.**
2. Enter **Group Name** > Click **Quick Add**.
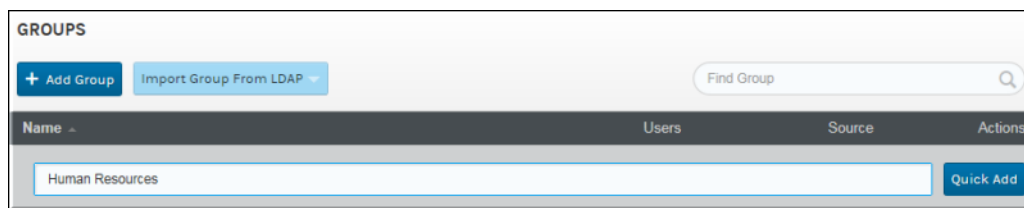
This will create the group without adding any users or roles. You must then edit the group to add users and roles.

If you want to add users and roles during group creation, click the **Add Group** button instead to navigate to the **New Group** page where you will be able to add the group's attributes.

> **Tip**: Clicking a **Group Name** edits an existing group where you may begin adding users and roles if you do not do so when creating the group.

Configure and Import LDAP Groups in Vbrick Rev

Create or Edit an Approval Process

Upload and Edit User Accounts and Groups Using a CSV File

Add or Remove a User from a Group

The **User Assignment** section on the group form provides the ability to add or remove users to a group. You must have the Account Admin role to use this functionality.
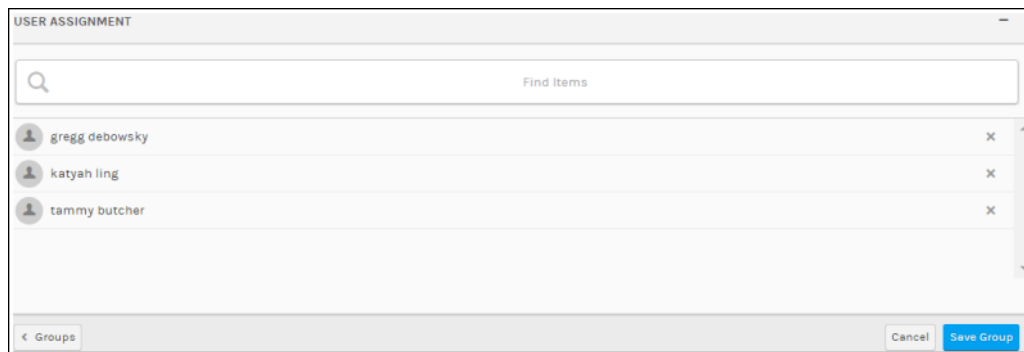
▼   To add or remove a User:

1. Navigate to **Admin** > **Users** > **Groups** > **Group Name.** (or click the **Add Group** button to begin creating a new group)

2. Use the **User Assignment** section to add or remove a user.

> **Note**: The Rev search engine works similar to popular Web search engines in that using double quotes around your search will narrow it and result in more accurate results if you are looking for a specific user or item.
>
> For example, if you are searching *only* for one specific video, user account, event, etc., enclosing the search in double quotes avoids returns of similar terms or derived words in your search results.
>
> Note that this is also true when using **Find Items** search within the Rev user interface to search for user accounts.

Field/Function	Description
Find Items	Begin typing the name of the user account in the **Find Items** box and Rev will suggest possible existing entries for you. Select the entry you want to add and click **Done**. Click the **X** if you want to remove the user account from the group.
Save Group	Click to save the group once you have completed all entries.

> **Note**: If you have imported your group from LDAP, you may not add users to it from Rev. You must edit it from LDAP to add or remove users.

> **Additional Information**: Most groups are imported and managed through LDAP and Active Directory. However, before you may do this there is a series of configuration steps that must be followed. View the topic on Configure and Import LDAP Groups in Vbrick Rev for complete step-by-step instructions on how to use LDAP to import your groups.

Add or Remove a Group from a User Account

Add or Edit a User Account

Upload and Edit User Accounts and Groups Using a CSV File

Add or Remove a Role from a Group

Roles define what actions a user may take within the system based on the permissions that are set for the role. Roles are assigned to a group so that certain permissions are enabled for several users at once (all users assigned to the group). You must have the Account Admin role to use this functionality.

▼   To add or remove a Role:

1.   Navigate to **Admin** > **Users** > **Groups** > **Group Name.** (or click the **Add Group** button to begin creating a new group)

2.   Use the **Role Assignment** section to add or remove a role.

Field/Function	Description
Available Roles	Click on a role in this column to assign it to the group. It will appear in the **Assigned Roles** column indicating it is now assigned to the group.
Add All	Click the **Add All** button to add *all* roles in the **Available Roles** column to the group at once.

Field/Function	Description
Assigned Roles	Click on a role in this column to remove it from the group. It will appear back in the **Available Roles** column and no longer be assigned to the group.
Remove All	Click the **Remove All** button to remove *all* roles in the **Assigned Roles** column from the group at once.
Find Roles	Use the **Find Roles** field to search and filter for a specific role to add or remove if needed.

Add or Remove a Role from a User Account

User Roles and Permissions by Function

Import an LDAP Group

Once you have configured LDAP and set up an LDAP Connector, you may import LDAP groups. Once imported, LDAP groups may be managed directly from the Rev user interface in limited fashion.

If you have not configured Rev for LDAP import or if your LDAP Connector is not running on your host or through a direct connection, you will not be able to import. See: Configure and Import LDAP Groups in Vbrick Rev.

> **Note**: The import method described in this topic retrieves and displays several LDAP groups associated with the Active Directory server. If you only want to import a few specific groups, you may set up your LDAP Connector device to only import the groups that you specify to save time. See: LDAP Groups Specification.

▼ To import an LDAP group:

1. Navigate to **Admin** > **Users** > **Groups** > **Import Group From LDAP** button. This button will not be visible if your connector is set up to only import specific groups.
2. Select an **LDAP Connector** you have previously set up from the dropdown.
3. You will be presented with a list of groups available for import.
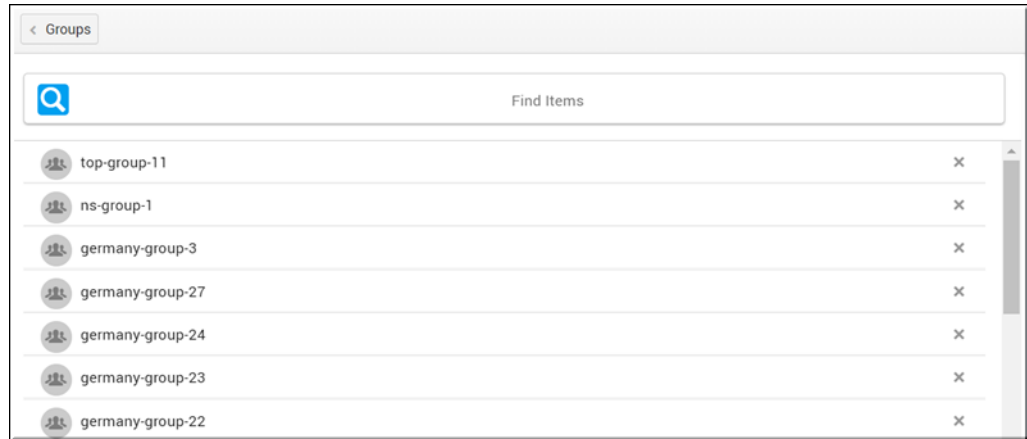
Function	Description
Groups	Click to return to the **Groups** module and cancel the import.
Group Name	Click to display any child groups associated to the group. Click the **X** next to each name to remove the group from the Import.
Import	Imports the displayed groups to Rev.

4. Remove the group and child groups you want do not want to import by clicking the **X** next to their names and then click the **Import** button. All remaining groups will be imported. Note that you must click the group name and remove each child group you do not want to import.

5. After a few minutes (depending upon how large the import/group is), each imported group will appear under the **LDAP Connector** name in the **Groups** module. The user accounts associated to each group will also be imported to the **Users** module.

6. The group will now be regularly synchronized based on the setting you defined when creating your LDAP Connector (and assuming your LDAP Connector Runtime exe is running on your host if you do not have a direct connection enabled). You may manually sync your group again if needed by re-importing it at any time with any updates.

> **Tip**: Similar to manually adding a user account, the status of user accounts imported with LDAP groups will be "Unlicensed" until the account logs in for the first time. It will then be set to "Active" status.

Configure and Import LDAP Groups in Vbrick Rev

The Presentation Profiles Module

Edit an LDAP Group

Once you have imported an LDAP group into Rev, it is edited by clicking on its name in the **Groups** module like any other Rev group. However, the attributes you may edit are very limited since LDAP groups should be managed, for the most part, from LDAP itself.

▼ To edit an LDAP group:

1. Navigate to the LDAP group you want to edit.

2. You will be presented with the **Group Name** and **User Assignment** sections to the LDAP group. However, you may not edit these sections. You must return to LDAP to edit these group attributes and then re-import the group to Rev.

3. LDAP groups also contain a **Role Assignment** section which may be edited within Rev. Note that if the group is updated through LDAP (re-imported) that this assignment will not change. In other words, you may only edit role assignment through Rev.

Add or Remove a Role from a User Account

User Roles and Permissions by Function

Delete or Suspend an LDAP Group or User

You may not delete an LDAP group or user from Rev as you would a Rev created group (from the **Group** or **User** module, **Actions** column).

There are two methods to removing an LDAP group from Rev:
- Remove the group from Rev by deselecting it from the group import screen and perform an import again.
- Remove the group from LDAP itself and perform an import again.

See: Import an LDAP Group

When you delete a group, whether through Rev or LDAP, user data and accounts are preserved (not deleted). However, they *may* be placed in a suspended state.

Suspended LDAP user accounts will be removed from a suspended state when:
- The group is re-imported again to Rev
- The user account is added to another group in LDAP and the new group is imported to Rev.
- The only time that imported user accounts are deleted from Rev is if the LDAP Connector itself is deleted.

You may manually suspend an LDAP user account as you would a Rev created user account. To activate it, you simply press the **Activate** button in the **Actions** column on the **User** module as you would a Rev user account.

LDAP user accounts that are not manually suspended (through the **Actions** drop-down UI) and that may be automatically suspended (and then deleted as a result in some cases) include:

• Those accounts that are created and imported but then never log-in. An example of this may be a user account that leaves the company before logging-in.

• These accounts may be permanently deleted upon an LDAP sync by selecting **Delete Suspended Users Who have never logged in** checkbox under the **LDAP Server Synchronizations Setting** section on the **LDAP Connector** device. Please keep in mind that if this checkbox is enabled, the Suspended account deletions *will* be permanent and will only include those accounts that have never been logged in; not the manually suspended accounts through the Users module UI and described above.

• Those accounts that are suspended as a result of removal from an LDAP group or an LDAP group is removed during an LDAP sync. You have the option to disable this suspension setting by selecting **Do not suspend users when removed from all LDAP groups or LDAP group is removed**. See: LDAP Server Synchronization Settings

Delete a User Account

Suspend a User Account

The Channels Module

A Channel contains users or groups that are very often similar in function or location. Use the **Channels** module to set up expanded permission structures for organizations focused on groups, users, content permissions and approval processes as needed.

For example, you may decide that only certain groups or users that are assigned to a specific Channel may view, edit, or upload videos to the Channel page based on their Channel role assigned.

Caution: *Only* certain roles in Rev may *create* a Channel and include Account Admin/Media Roles or the Channel Creator role. Once created, you should designate a **Channel Admin** in charge of editing its settings and members.

It is important to note that the *Channel* role governs what you can and cannot do within the structure of the Channels module and Channel pages rather than the Rev role. This means that Rev Account Admins will be somewhat limited in actions and view options if they are not also a member of the Channel.

In general, if you are unable to perform an action you need to accomplish in relation to Channel functionality, double-check the Channel role you have been assigned; not the Rev role.
See: Channel Role Definitions and Permissions for details between Channel roles and Rev roles with regard to Channel actions and permissions.

The **Channels** module displays:

Column	Description
Name	The **Channel Name**. Click to edit channel attributes.
Actions	The actions you may perform on a channel. • **Delete** — When a channel is deleted, the users and groups associated to it are not deleted.

Additional functionality:

Function	Description
Create Channel	Creates a new channel by taking you to the **New Channel** page where you may add groups and users to the channel. This includes Account Admins, Media Admins, and Channel Creators.
Quick Add	Quickly creates the channel you type in the channel name text box but does not add any content. Account Admins only.
Find Channels	Search for a specific channel.

The Users Module

The Groups Module

The Roles Module

Create and Edit a Channel

Channels allow you to create media pages and permissions specific to only the user accounts that are members of the channel.

For example, you may decide to set up an approval process based on the groups and user accounts in a channel. Or, you may base video access to different channels by location.

> **Caution**: *Only* certain roles in Rev may *create* a Channel and include Account Admin/Media Roles or the Channel Creator role. Once created, you should designate a **Channel Admin** in charge of editing its settings and members.
>
> It is important to note that the *Channel* role governs what you can and cannot do within the structure of the Channels module and Channel pages rather than the Rev role. This means that Rev Account Admins will be somewhat limited in actions and view options if they are not also a member of the Channel.
>
> In general, if you are unable to perform an action you need to accomplish in relation to Channel functionality, double-check the Channel role you have been assigned; not the Rev role.
> **See**: Channel Role Definitions and Permissions for details between Channel roles and Rev roles with regard to Channel actions and permissions.

▼ To add or edit a Channel:

1. Navigate to **Admin** > **Users** > **Channels**.

2. Enter a **Name** for a new channel or click the Channel name to edit the channel if it has already been created.

3. Click **Quick Add**. This does not add any assets to the channel such as Channel Members.

▼ To create a Channel and add assets:

1. Click the **Create Channel** button. The **New Channel** form is displayed. Enter the various attributes described below to create the Channel Landing Page. As noted above, only Account or Media Admins may create new Channels.

• **Channel Name**: Create or edit the name as needed.

• **Channel Description:** Create or edit text on the purpose of the channel.

• **Channel Logo Image:** Upload a logo for the Channel. Use a size of 480x360 for best results. If no image is uploaded, the background color only will be used for the Channel tile and header.
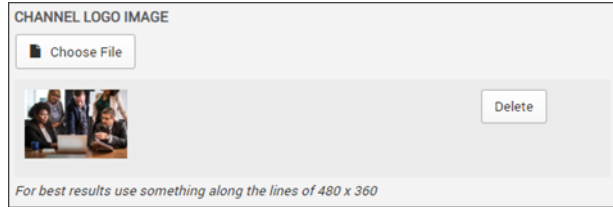
- **Colors:** Assign a background color for the Channel tile and header. You may click on the current color to use the color wheel or enter a hexadecimal color value in the **Header Background** field. Select either a **Light** or **Dark** font for the **Header Font Color** based on the background color you select.

- **Assign Users and Groups**— Used to add user accounts and groups to the channel. Begin typing the name of the user account or group in the **Find Items** box and Rev will suggest possible existing entries for you. Select the entry you want to add and click **Done**.
- Assign the **Channel Role** that is required for the user or group. You should begin by assigning a **Channel Admin** in charge of managing the Channel. See: <u>Assign or Modify Channel Roles and Permissions</u>.
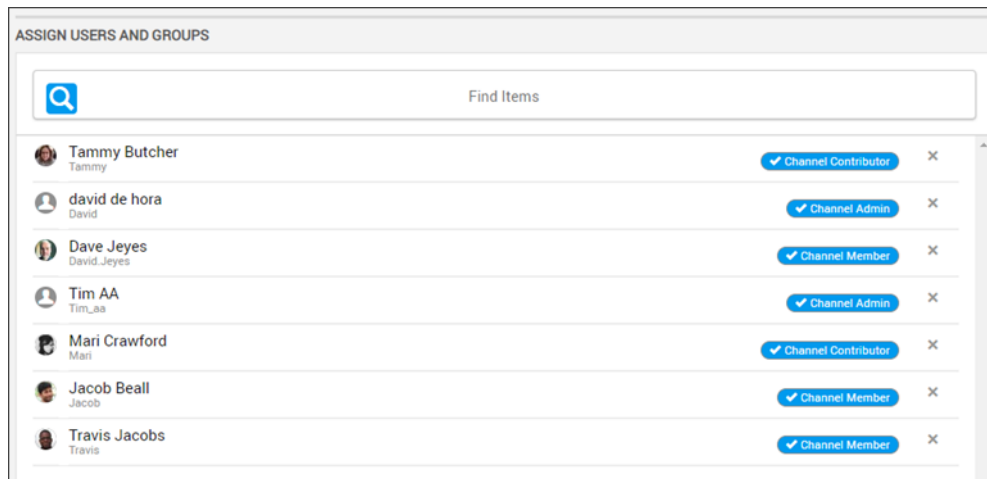
- Click the **Save Channel** button when you have finished completing your Channel set up.
- Keep in mind that all permissions and processes assigned to this channel, including videos, will now be granted to the user accounts and groups saved in the channel.

<u>Understanding the My Channels Menu</u>

<u>Set Video Access to Channels</u>

<u>Channel Role Definitions and Permissions</u>

<u>Assign or Modify Channel Roles and Permissions</u>

<u>Create or Edit an Approval Process</u>

The Roles Module

Add or Remove a User Account or Group from a Channel

The **Assign Users and Groups** box on the **New Channel** page provides the ability to add a user account or group (or both) to a Channel. When a user accounts or groups are added to a Channel, they will have access to permissions granted to that Channel such as video access or content approvals.

Only Channel Admins are able to edit previously created Channels within the Channel interface. Rev Account or Media Admins are able to edit a Channel through the Admin > Users > Channel interface only.

Caution: *Only* certain roles in Rev may *create* a Channel and include Account Admin/Media Roles or the Channel Creator role. Once created, you should designate a **Channel Admin** in charge of editing its settings and members.

It is important to note that the *Channel* role governs what you can and cannot do within the structure of the Channels module and Channel pages rather than the Rev role. This means that Rev Account Admins will be somewhat limited in actions and view options if they are not also a member of the Channel.

In general, if you are unable to perform an action you need to accomplish in relation to Channel functionality, double-check the Channel role you have been assigned; not the Rev role.
See: Channel Role Definitions and Permissions for details between Channel roles and Rev roles with regard to Channel actions and permissions.

Field/Function	Description
Find Items	Begin typing the name of the user account or group in the **Find Items** box and Rev will suggest possible existing entries for you. Select the entry you want to add and click **Done**. Click the **X** to remove the entry from the channel.

Save Channel	Click to save the channel once you have added all entries.

> **Note**: The Rev search engine works similar to popular Web search engines in that using double quotes around your search will narrow it and result in more accurate results if you are looking for a specific user or item.
>
> For example, if you are searching *only* for one specific video, user account, event, etc., enclosing the search in double quotes avoids returns of similar terms or derived words in your search results.
>
> Note that this is also true when using **Find Items** search within the Rev user interface to search for user accounts.

Delete a Channel or Channel Member

Account Admins and Channel Admins will have a delete icon under the **Actions** column on the **Channels** module. This allows deletion of channels in order to maintain accurate content structures for organizations.
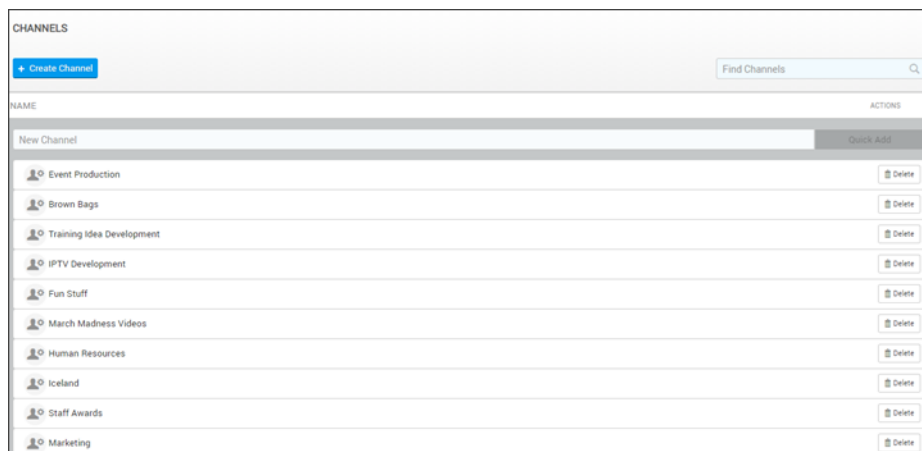
Only Channel Admins may delete Channel Members by clicking the X control next to the Channel Member on the Channel page.

Understanding the My Channels Menu

Set Video Access to Channels

Create or Edit an Approval Process

Assign or Modify Channel Roles and Permissions

You should make sure that your Channels have at least one **Channel Admin** assigned when you create them so that you have someone in charge of managing the Channel settings and members.

Note that you may designate non-Admin accounts in Rev the ability to manage channels by assigning them Channel Admin access. Channel Roles are separate from Rev Roles (though similar in function).

> **Caution**: *Only* certain roles in Rev may *create* a Channel and include Account Admin/Media Roles or the Channel Creator role. Once created, you should designate a **Channel Admin** in charge of editing its settings and members.
>
> It is important to note that the *Channel* role governs what you can and cannot do within the structure of the Channels module and Channel pages rather than the Rev role. This means that Rev Account Admins will be somewhat limited in actions and view options if they are not also a member of the Channel.
>
> In general, if you are unable to perform an action you need to accomplish in relation to Channel functionality, double-check the Channel role you have been assigned; not the Rev role.
> **See**: Channel Role Definitions and Permissions for details between Channel roles and Rev roles with regard to Channel actions and permissions.


▼ To assign or edit a Channel Role:

1. Navigate to a Channel. For new channels, you must be an Account or Media Admin (or Channel Creator) to create the Channel and assign Roles. For existing Channels, you must be the Channel Admin to create or edit a Channel Role.

2. Next to the user and/or group, click the Role control drop-down and assign the Channel Role as required.

Channel Admins have the same rights as an Account Admin but only for videos assigned to that specific Channel. This includes:

- Ability to edit channel settings
- Ability to bulk edit videos in the channel
- Ability to approve or reject videos in the channel that are part of an approval process

Understanding the My Channels Menu

Set Video Access to Channels

Channel Role Definitions and Permissions

Assign or Modify Channel Roles and Permissions

Create or Edit an Approval Process

The Roles Module

Roles are groups of permissions to system features that you may then assign to **Groups** and **Users**. For example, a *Media Viewer* role may be able to view content but not edit or approve it whereas an *Account Admin* role may have permission to manipulate virtually every setting in the system. The roles and permission features of Vbrick Rev ensures that each user has access to only the features that are needed.

Keep in mind that Rev also has Channel roles and permissions that are separate from the Rev roles described in this section of help though they are similar in function and relate *only* to the management of a Rev channel.

Use the **Roles** module to view the roles and permissions in your system. Only Account Admins will have access to this module.

The **Roles** module displays:

Columns	Description
Role	The role name. This is a descriptive name that provides indication of what permissions the role contains.
Permissions	What permissions the role contains and what functions (as a result) the user or group may access when assigned to this role.
Description (not shown)	A complete description of the role's permissions.

Add or Remove a Role from a Group

Add or Remove a Role from a User Account

View a Role

The predefined roles in Rev may be accessed through the **Roles** menu bar if you have the Account Admin role assigned to your account.

▼ To view a role:

1. Navigate to **Admin** > **Roles.**
2. **Role Name**, **Permissions** and **Description** (not shown) are displayed.

User Roles and Permissions by Function

The table below illustrates Rev's main functions along with which roles have permission to access them.

Function		Roles						
		Account Admin	Media Admin	Media Contributor	Media Viewer	Channel Creator	Event Admin	Event Host
Account Admin Home	Edit account details	x						
	Add sub-account	x						
	Edit sub-account	x						
	Delete sub-account	x						
Groups	Add user groups	x						
	Edit user groups	x						
	Delete user groups	x						
User	Add users	x						
	Edit users	x						
	Delete users	x						
	Suspend/un-suspend users	x						
	Add channels	x	x			x		
	Edit channels	x	x					
	Delete channels	x	x					
Roles	View roles	x						
Devices	Add devices	x						
	Edit devices	x						
	Delete devices	x						
	Add zones	x						
	Edit zones	x						
	Delete zones	x						
	Add presentation profiles	x						
	Edit presentation profiles	x						
	Delete presentation profiles	x						
	Manage Set Top Boxes	x						
	Manage display devices	x						

Function		Roles						
		Account Admin	Media Admin	Media Contributor	Media Viewer	Channel Creator	Event Admin	Event Host
Media Settings	Add categories	x	x					
	Edit categories	x	x					
	Delete categories	x	x					
	Add transcode presets	x	x					
	Edit transcode presets	x	x					
	Delete transcode presets	x	x					
	Edit transcode settings	x	x					
	Edit Media Feature settings	x	x					
	Edit Integration settings	x	x					
	Add Approval Processes	x	x					
	Edit Approval Processes	x	x					
	Delete Approval Processes	x	x					
	Edit Recording settings	x	x					
	Add Expiration rules	x	x					
	Edit Expiration rules	x	x					
	Delete Expiration rules	x	x					
	Add VOD templates	x	x					
	Manage VOD template settings	x	x					
	Delete VOD templates	x	x					
	Add Webcast templates	x	x					
	Manage Webcast template settings	x	x					
	Delete Webcast templates	x	x					

Function		Roles						
		Account Admin	Media Admin	Media Contributor	Media Viewer	Channel Creator	Event Admin	Event Host
System Settings	Edit Security settings	x						
	Add API Key	x						
	Edit API Key	x						
	Delete API Key	x						
	Edit Environment settings (Root Account only)	x						
	Edit UI branding settings	x						
	Add custom fields	x						
	Edit custom fields	x						
	Delete custom fields	x						
	Add Webcast registration fields	x						
	Edit Webcast registration fields	x						
	Delete Webcast registration fields	x						
Reports	Admin reports	x	x					
	Video reports	x	x					
	Event reports	x	x				x	
Media	Add media	x	x	x				
	Record media	x	x	x				
	Manage Featured Videos	x	x					
	Manage all videos	x	x					
	Approve media	x	x					
Events	Add event	x	x				x	x
	Edit event	x	x				x	x*
	View event	x	x	x	x	x	x	x
	Delete event	x	x				x	x*

* Event Hosts may only edit and delete events that they create.

Add or Remove a Role from a Group

Add or Remove a Role from a User Account

Channel Role Definitions and Permissions

Keep in mind that Rev also has Channel roles and permissions that are separate from Rev roles though they are similar in function. Channel roles and permissions relate *only* to the management of a Rev channel. Further, Rev roles do *not* have permissions within the scope or context of a Channel, and this includes a Rev Account Admin. Instead, Admins will need to access the Channel through the Users menu if needed.

Because of this, you should make sure that your Channels have at least one Channel Admin assigned when you create a Channel so that you have someone in charge of managing the Channel settings and members. This also means that you may designate a non-admin account in Rev a Channel Admin for a Channel if you so choose since the roles and permissions are entirely separate.

Role	Permissions	Description
Channel Admin	• Access to All Channel Features • Manage All Channel Content • Manage All Channel Users and Groups • Ability to Edit All Channel Content	Similar to the Rev Account Admin role within the context of the Channel module and page in that this role has all the abilities of the Channel Member and Channel Contributor in addition to being able to edit new Channel members and Channel settings (of the specific Channels they administer). As a result, you may *not* edit the settings of any Channels where you do not have the Channel Admin role assigned even if you are an Account Admin in Rev (on a Channel page). As previously stated, within the context of a Channel, the Channel role governs *not* the Rev role.
Channel Contributor	All permissions granted to Channel Members, plus permissions to: • Upload video assets (anything available under the Add Content + icon) including recording live streams • View/edit content based on permissions	Similar to the Media Contributor role in Rev. This role has view and upload permissions to the Channel, along with sort and filter abilities. However, Channel Contributors have *no* ability to edit Channel settings and members. Only the Channel Admin may do this.
Channel Member	• View, sort, and filter video assets to which Channel has been granted access • Attend events to which Channel has been granted access • This user cannot add content to the Channel	The default role that is assigned when you first add a user or group to a Channel. This role is similar to the Media Viewer role in Rev and only has view, sort, and filter access. It may not upload or edit Channel video assets.

Add or Remove a User Account or Group from a Channel

Assign or Modify Channel Roles and Permissions

Devices

Devices Overview

Devices are external components that "talk" to Vbrick Rev and may include Vbrick Encoders/Decoders, Distributed Media Engines (DMEs), LDAP servers, and Set Top Boxes.
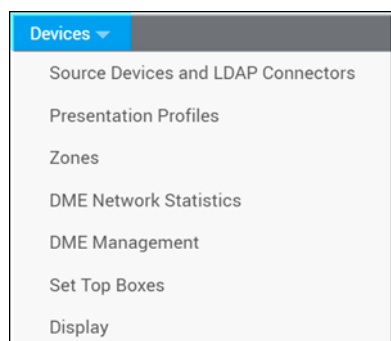
Through the **Devices** menu bar, you are also able to create **Presentation Profiles** that are predefined video source inputs and destination outputs for devices that your event creators may use for the Webcasts they create. The **DME** modules allows you to manage and monitor the health and network traffic on all DMEs assigned to your network.

Finally, **Zones** are used to create a series of IP Address ranges that you assign to each device in your system that maintain strict control of your network, bandwidth, and content ingestion.

This makes device control in Vbrick Rev for both admins and users alike more intuitive and easy to use than any system on the market.

Device Initial Configuration and Set Up

Before you are able to add a device to your system, you must make sure it is configured correctly with an API key first.

> **Note**: The steps in this section *must* be completed first before you begin adding devices from any of the **Devices** modules or menu options.

▼   To set up device configuration in Rev:

1. Create an API key for the system devices (DME and/or Encoder) you plan to add and use with Rev. You may add a key for each device or one that is used for all devices that communicate with Rev. You will also need to create an API key for your LDAP connector which must be a separate key from your system device key.

    •   See: Add an API Key.

    •   See: Configure and Import LDAP Groups in Vbrick Rev

2. For each device:

- Add the API key created to each device you plan to link to Rev.
- Add the host URL to your Rev installation to each device. May be obtained from the **Account Host Name** field on the **Contact** module or from your browser bar URL on the Log in screen minus the "#/login" text. See: <u>View Contact and Billing Information for an Account</u>.
- Example: To configure and link an Encoder, enter this information in the **API Key** and **Host** fields under the **System Configuration** > **General** section of the Encoder.
- Example: To configure and link a DME, enter this information in the **System Configuration** > **Rev Interface** section of the DME.
- See the corresponding device's Admin technical manual for more information if needed.

3. You are now ready to add your devices in Rev through the **All Devices** module.

<u>Supported Vbrick Devices</u>

<u>Add an API Key</u>

The Source Devices and LDAP Connectors Module

Use the **Source Devices and LDAP Connectors** module to add, configure, and manage encoders, LDAP connectors, custom devices, and Akamai devices you want connected to your system. Keep in mind that you will often need to have devices added and configured before using them elsewhere in Rev, such as with a **Presentation Profile** which will use devices that are added in this module.

The **Source Devices and LDAP Connectors** module displays:

Column	Description
Name	Name or Hostname of the device that has been added.
Type	The type of device that has been added.
Network Address	The MAC address of the device.
Status	The status of the device; Online, Offline, or Inactive. If inactive, your device will not be able to be accessed by Rev.
Actions	The actions you may perform on the device. • **Edit** — Edit the device. • **View Log** — View a log of recent actions that have occurred on the device. This is good for troubleshooting if your device is not performing as expected. • **Delete** — When a device is deleted, the content stored on the device is not deleted. However, you may not access it because the association to the device is removed.

Additional functionality:

Function	Description
Add a Device	Adds a new device association in Rev.

Add an Encoder

To optimize the viewing of your content across your enterprise network, Vbrick Rev easily facilitates adding an Encoder to your environment. Encoders are designated as the video streaming sources of your network or, in other words, where your video is input from.

> **Tip**: Make sure you configure your Vbrick devices before you begin adding them. See: Device Initial Configuration and Set Up

▼ To add an Encoder device:

1. Navigate to **Admin** > **Devices** > **Source Devices and LDAP Connectors** > **Add a Device** button.
2. Select **Add an Encoder** from the dropdown.

Field Name	Required	Description
Device Name	Yes	This can be a name of your choosing. This is a required field. Descriptive location or host name is recommended.
Status		The status of your device may be set to **Active** or **Inactive** upon adding it to your system.
MAC Address	Yes	The MAC Address is required. Copy the MAC Address for an Encoder from the **Monitor** > **Network** page of VBAdmin in the Encoder.

Field Name	Required	Description
Video Streams	Yes	**Name**, **URL**, **Encoding Type**, and **Multicast** are all designated [through the **Add URL** button] and are required fields if the Encoder is intended to be utilized as a streaming device for live events and Webcasts. These streams will later be selected on **Presentation Profiles** as viewing destinations. **Note**: The exception to this scenario is if you are using the DME as a video destination. In this case, you will not need to add a URL for the Encoder because the DME is providing the video destination URLs. View the Vbrick Device Integration guide for more information.

3. Click the **Create** button.
4. After a few seconds, the Encoder status should flip from **Uninitialized** to **Active**. If it does not, check your **MAC Address** field to ensure it is correct and the Encoder configuration steps such as the **API key** and **Host** fields. See: Device Initial Configuration and Set Up topic.
5. Your device is now ready to use with Rev.
6. Account admins will be sent an email notification if any DME or Encoder goes into Warning or Offline status so that they may pro-actively troubleshoot the device. The email will include when the device went into warning or offline status (date/time), the device name, and a link to the device.

Supported Vbrick Devices

Add a Distributed Media Engine (DME)

View the Status of a Device

View and Request Device Logs

Add a Presentation Profile

Add a Zone

Zone Logic and Hierarchy

Add an LDAP Connector

Before you are able to import an LDAP group, you must first create a means for Vbrick Rev to communicate with Active Directory and LDAP groups; This is accomplished by creating an LDAP Connector and then running that connector on a host.

View the topic on Configure and Import LDAP Groups in Vbrick Rev for complete step-by-step instructions on how to use LDAP.

Tip: Make sure you configure your Vbrick devices before you begin adding them. See: Device Initial Configuration and Set Up

Add a Custom Device

You may also add a custom device that you may define as either a source or a destination (or both) in addition to using Vbrick's Encoders and DMEs.

> **Tip**: Make sure you configure your Vbrick devices before you begin adding them. See: Device Initial Configuration and Set Up

▼ To add a custom device:

1. Navigate to **Admin** > **Devices** > **Source Devices and LDAP Connectors** > **Add a Device** button.
2. Select **Add Custom Device** from the dropdown.

Field Name	Required	Description
Name	Yes	This can be a name of your choosing. This is a required field. Descriptive location or host name is recommended.
Status		The status of your device may be set to **Active** or **Inactive** upon adding it to your system.
IP Address	Yes	The IP address of where your device is located.
Capabilities	Yes	At least one capability is required. You must designate that the device be at least a stream source or a viewing destination source. If you designate the device as a viewing destination source, then you must also input Video Streams.
Video Streams	Yes	**Name**, **URL**, **Encoding Type**, and **Multicast** are all designated [through the **Add URL** button] and are required fields if the device is intended to be utilized as a viewing device for your users. These streams will later be selected on **Presentation Profiles** as viewing destinations or can also be used for automatic multicast viewing.

3. Click the **Create** button.

HLS Stream Preparation for Automatic Multicast and Reflection

To optimize the use of Custom Devices features, the HLS stream should meet certain specifications.

Please review the DME help documentation on stream specifications in the Rev Initiated Multicast and Reflection topic.

Supported Vbrick Devices

Add a Distributed Media Engine (DME)

View the Status of a Device

View and Request Device Logs

Add a Presentation Profile

Add a Zone

Add an Akamai Device

Vbrick Rev integrates seamlessly with the Akamai Content Delivery Network. Keep in mind that video playback will be from either Rev's devices or Akamai once the integration is complete depending upon how you set up your zone logic.

> **Tip**: If you plan to use Akamai and are a Rev cloud customer, Akamai will be configured for you by Vbrick automatically. Contact Vbrick Support Services if Akamai playback is not activated for you when you access Rev for the first time. This topic is only for Rev On-Premise customers.

You must make sure you have your Akamai CDN set up correctly to integrate with Rev before you add your Akamai device so speak with your Akamai Representative to ensure your properties are set up first.

Make sure the Akamai device is added to a zone upon completion. This can be default zone or a new zone/child zone depending on how you want your zone logic to be configured.

If you want to set up the integration yourself, view the "Akamai Integration Application Note" under the **Vbrick Integrations** section on the Vbrick Documentation site for configuration details on how to do so.

Supported Vbrick Devices

Add a Distributed Media Engine (DME)

View the Status of a Device

View and Request Device Logs

Add a Presentation Profile

Add a Zone

Add an Akamai Secure Streaming Custom Device

If you are using an Akamai integration with Vbrick Rev, you can create a secure streaming custom device for specific use with Akamai that will prevent URL sharing. Similar to other custom devices, you may define the Akamai device as either a source or a destination (or both) in addition to using Vbrick's Encoders and DMEs.

> **Tip**: Make sure you configure your Vbrick devices before you begin adding them. See: Device Initial Configuration and Set Up

▼   To add an Akamai secure streaming custom device:

1. Contact Vbrick Support Services and request an Akamai secure streaming URL and token key for your device. You will not be able to move forward until you have this URL with the key appended to the end of the URL.

2. Once you receive the URL from support, navigate to **Admin** > **Devices** > **Source Devices and LDAP Connectors** > **Add a Device** button.

3. Select **Add Custom Device** from the dropdown and complete the fields below.

Field Name	Required	Description
Name	Yes	This can be a name of your choosing. This is a required field. Descriptive location or host name is recommended along with the fact this is your Akamai Secure Streaming device.
Status		The status of your device may be set to **Active** or **Inactive** upon adding it to your system.
IP Address	Yes	The IP address of where your device is located.

Field Name	Required	Description
Capabilities	Yes	You must designate that the device be at least a viewing destination source so that you may enter the URL given to you by Vbrick Support. You may also designate the device as a stream source if desired.
Video Streams	Yes	**Name**, **URL**, **Encoding Type**, and **Multicast** are all designated [through the **Add URL** button] and are required fields. • Name: May be the name you choose • URL: Enter the URL provided to you by Vbrick Support • Encoding Type: Must be HLS in this scenario. • Is Multicast: Not valid with HLS in this case; leave unselected. These streams will later be selected on **Presentation Profiles** as viewing destinations.

4. Click the **Create** button.

Supported Vbrick Devices

Add a Distributed Media Engine (DME)

View the Status of a Device

View and Request Device Logs

Add a Presentation Profile

Add a Zone

Add an Akamai Live Device

You will need to add an Akamai Live device if you plan to utilize Video Conference (VC) Live Webcast events. VC Live events are a cloud-only feature and are enabled by Vbrick. Once enabled, you must add your Akamai Live device. At that point, you may create and host your events using live video conferences as your video source while taking advantage of Rev's Webcast event features.

> **Tip**: Currently supported are Webex, Cisco DX and Cisco SX video conference devices. Contact Vbrick Support Services to obtain the required field values.

Most fields will be provided to you by Vbrick Support Services.

Keep in mind that all VC Live Webcast events will automatically use Akamai Live devices (once added) for distribution. Rev allows a maximum of four concurrent VC Live events active on each Akamai Live device. Further, each device uses DME v3.15 or higher for reflecting VC Live Webcast events. Shared API authorization keys are not currently supported for this functionality.

Supported Vbrick Devices

Add a Distributed Media Engine (DME)

View the Status of a Device

View and Request Device Logs

Add a Presentation Profile

Add a Zone

The Presentation Profiles Module

Presentation Profiles are used to define device profiles for your event creators. Use them to specify the device video source inputs and destination outputs, so that your event creators have an easy to use and intuitive system already in place when they begin to design and deliver their Webcast events in Vbrick Rev.

The **Presentation Profiles** module displays:

Column	Description
Name	A descriptive name that describes the profile you have created.
Video Source	The video input source of your profile such as Encoder slot and channel input or a custom device name.

Status	The status of your profile; active or inactive. If inactive, your profile will not be able to be selected by an event creator for using during presentations.
Actions	The actions you may perform on the presentation profile. • **Delete** — Deletes a presentation profile.

Additional functionality:

Function	Description
Add a Presentation Profile	Creates a new profile.

Add a Presentation Profile

Account Admins create Presentation Profiles to control devices for a Webcast Event. Once created, Event Admins may then assign them to the Webcast during event setup. Event Hosts can also do this but *only* on those events where they have also been assigned.

> **Tip**: Make sure you configure your Vbrick devices before you begin adding them. See: Device Initial Configuration and Set Up

▼   To create a Presentation Profile:

1. Navigate to **Admin** > **Devices** > **Presentation Profiles** > **Add a Presentation Profile** button.
2. Complete each section of the **Presentation Profile** form and click **Create**.

Presentation Profile Name and Description

Field Name	Required	Description
Name	Yes	Enter a profile **Name**. This is a required field and must be unique.
Description		Enter a description that details what the profile will be used for.
Status		The status of the profile. When inactive, it will not be functional for use in events.

Source

Field Name	Required	Description
Video Source	Yes	A streaming video source *must* be specified for each profile. The source may be specified by selecting a predefined Encoder or custom device (See: <u>Device Initial Configuration and Set Up</u> topic) in the **Video Source** dropdown.

> **Note**: If an Encoder is selected in the **Video Source** dropdown, the following conditions must be true:
> - The Encoder must be configured in Rev under the **All Devices** module
> - All slots and channels associated with the Encoder have been configured correctly
> - The available slots and channels are displayed in the following format: `<device name>:<slot #>:<channel #>`.
>
> This is seen in the image above.

Destinations

At least one viewing destination must be defined for each profile. Multiple viewing destinations may also be defined if needed or desired.

Any of the following devices may be defined as a viewing destination:
- An Encoder if that Encoder has also been set as the source in the **Video Source** section.
- A DME that has been previously configured in the system on the **All Devices** module.
- A manually (custom) specified destination.

Field Name	Required	Description
Select a Destination	Yes	Selects a predefined device as your viewing destination. At least one viewing destination is required.
Add Another Destination		Adds additional viewing destinations.
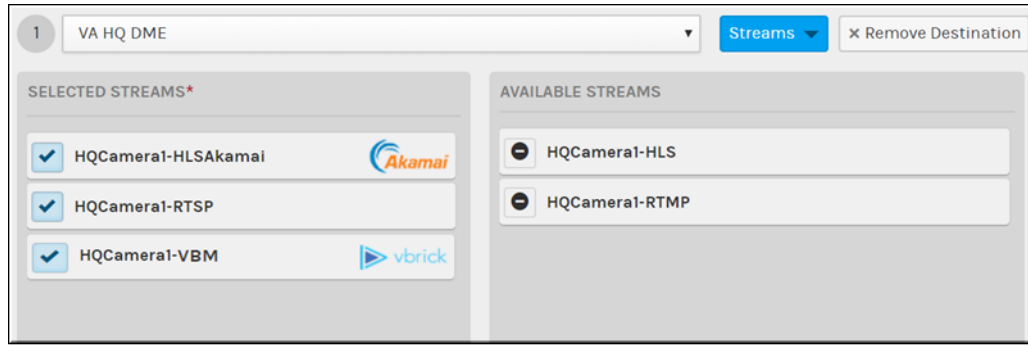
Field Name	Required	Description
Available Streams		Available streams on the selected device that are available to be designated as viewing streams. Click the stream to add it to the **Selected Streams** column. It will then be used on the profile as a viewing stream.
Selected Streams		Streams that have been selected as viewing streams on the profile. Click a stream to remove it. It will be placed back in the **Available Streams** column and no longer available for use as a viewing stream.

Note: An RTSP unicast stream is required for recording live Webcasts in Rev. Make sure that your stream has a keyframe interval between 2 to 5 seconds and do not use B-frames. Please see your individual Encoder (stream source) documentation for setting information.

Akamai streams are denoted by the Akamai logo.

Caution: Presentation Profiles may contain multiple Destinations/ DMEs. Rev Connect Peer Meshes may use any HLS in the Destination/DMEs for content retrieval. In order to correctly leverage the Mesh and multiple Destinations, It is important that each Destination has the same named and sourced Live WebCast HLS stream for use with Rev Connect.

Tip: Streams are configured on the device when you add it from the **All Devices** module.

Role(s):

- **Create**: Account Admin
- **Assign to Webcast Event**: Event Admin, Event Host (if also assigned to event)

Select a Presentation Profile for a Webcast Event

Add a Distributed Media Engine (DME)

View the Status of a Device

The Zones Module

The **Zones** module may be selected to create a series of IP address ranges that you may then assign specific devices to such as DMEs, Encoders and so forth. This, in turn, allows you to maintain strict control of your network, bandwidth, and content ingestion by deciding which content is ingested and streamed where on your network. Zones may also be configured into Rev Connect zones and form peer-assisted, browser-based peer meshes that optimize video retrieval for live HLS events.

The **Zones** module displays:

Column	Description
Zone Name	A descriptive name for the zone.
Number of Devices	The number of devices that are assigned to the zone.
Actions	The actions you may perform on the zone. • **Add Child**: Add a Sub-Zone to the currently selected Zone. • **Delete Zone**: Deletes the currently selected zone or sub-zone.

Note: The Zones module is optimized for efficient load times for large customers that have several devices and streams per zone. When you view the Zone details of a specific Zone, only the Devices are listed. To view the Streams for that Device, click the **Customize** button or click a Device itself.

Add a Zone

When adding a new zone or sub-zone, it is important to consider where users and devices are located so that you can efficiently direct content and viewers on your network and manage your bandwidth effectively.

Also, by understanding zone logic and how to configure zone hierarchies, you also provide a fail-over for your content distribution if your devices in a specific zone fail for whatever reason.

> **Note**: The Zones module is optimized for efficient load times for large customers that have several devices and streams per zone. When you view the Zone details of a specific Zone, only the Devices are listed. To view the Streams for that Device, click the **Customize** button or click a Device itself.

For more information on how to manage this, view the topic on <u>Zone Logic and Hierarchy</u>.

▼ To add a new Zone:

1. Navigate to **Admin** > **Devices** > **Zones** > **Add Zone** button.
2. Complete all sections described below and click **Create**.

Zone Details

Field Name	Required	Description
Zone Name	Yes	A descriptive name for the zone; normally indicative of where the zone will cover or what types of devices it will house.
Supports Multicast		Enable to indicate whether or not the zone will support multicast.

IP Addresses	Yes	Both IPv4 and IPv6 zones are accepted. **Note**: IPv6 shorthand notation not accepted. IP addresses should be separated by carriage returns. IP ranges are divided by a dash. Example: 168.222.108.1-168.222.108.254
		If a user's IP address falls into the range specified, the zone will be used for that user and content will be served from that zone and device. This is important when setting up <u>Zone Logic and Hierarchy</u>.
Supports Rev Connect		Enable Rev Connect for this Zone. This will enact peer-sharing between browsers in this zone for HLS Webcasts and video conferences. This feature requires additional licensing to be available and displayed, please see your Sales representative for more information.
		Additional configuration options will become visible once this is enabled.
		This is disabled by default.
		See: <u>Rev Connect Enabled Zones</u>

Slide Delay for HLS Live Video

Field Name	Required	Description
Override Account Slide Delay Setting		This checkbox allows you to override the Rev account slide delay settings that have been defined under the **Media Settings** > **Slide Delay** section. If an account slide delay has not been set manually and has been turned off, this checkbox will not appear.
		See: <u>Recording</u>
Delay in Seconds		Specify the delay in seconds. If this setting is not used, the account level settings are used.

Devices Section

Field Name	Required	Description
Live Only		Select this checkbox if you want to configure the DME as a Live Only DME. This option is disabled by default. **Note**: This is a Rev restriction only. This means that Rev will not direct players to retrieve VOD directly from this DME. However, please note that the DMEs will continue to operate and share within the DME Mesh as currently designed.
Available Streams		Available streams on the selected device that are available to be designated as viewing streams in the zone. Click the stream to add it to the **Selected Streams** column. It will then be used in the zone as a viewing stream. **Note**: Streams will only be loaded or created when you click the **Customize** button. This is to support efficient loading for those devices several streams.
Selected Streams		Streams that have been selected as viewing streams on the profile. Click a stream to remove it. It will be placed back in the **Available Streams** column and no longer available for use as a viewing stream. **Note**: When using a Custom Device based on Automatic Multicast, only select one to be used **PER DME**. You can include multiple DMEs (as destinations) each with a single associated Custom Device for any load balancing or multicast network bifurcation needs.

Caution: Be aware of what zone you are placing devices and streams. For example, in the image above, Akamai HLS streams should only be zoned for outside remote users.

Add a Distributed Media Engine (DME)

View the Status of a Device

The DME User Location Service

Rev Connect Enabled Zones

Rev Connect is a separately licensed, peer-assisted, browser-based software solution created by Vbrick for Live Webcasts. This feature is limited to cloud only Rev instances and addresses the problem of distributing Live Webcasts to reduced bandwidth/reduced viewer locations (such as remote offices).

Rev Connect optimizes distribution within a Zone by creating a cooperating set of viewers' browsers. These browsers (using WebRTC data channels) form a Peer Mesh. The peer mesh browsers work together to retrieve content and share it in a peer-to-peer manner. The Rev Player downloads the WebRTC controls and there is no additional download or install necessary. This feature only works with browsers that support WebRTC data channels.

When used, one of the peer mesh browsers retrieves the HLS segments from "origin" (for example, a DME or Akamai) and shares that content to the other peer mesh browsers. Those other browsers, depending upon timing, can then also share that content with other browsers within the peer mesh with an overall goal of limiting the number of origin retrievals/segment to as few (e.g., 1) as possible. In this way, a peer mesh that supports 25 browsers/viewers retrieves 1 HLS segment for up to 25 viewers.

Rev Connect utilizes WebRTC technology. See the <u>Supported Player and Stream Compatibility</u> table for supported browsers.

Rev Connect is a separately licensed product available through Vbrick and controlled/configured within Rev Zones (see: <u>Rev License Types and Add-On Components</u>).

Add Rev Connect to a Zone

Before you enable a Zone to use Rev Connect, consider if the Zone should be enabled. Rev Connect is designed to provide Live Webcasts to remote offices with reduced (ingress) bandwidth. Do *not* enable Rev Connect for Zones that include DMEs – using the DMEs for distribution is recommended.

> **Caution**: This is a rule that *must* be followed. Presentation Profiles may contain multiple Destinations/DMEs. Peer meshes may use any HLS in the Destination/DMEs for content retrieval.
>
> In order to correctly leverage the Mesh and multiple Destinations, it is important that each Destination has the **same named and sourced** Live WebCast HLS stream for use with Rev Connect.

▼   To configure a Zone to use Rev Connect:

1.   Navigate to **Admin** > **Devices** > **Zones** > **Add Zone** button.

2.   Select an existing zone or add a new zone as you normally would. See: <u>Add a Zone</u>.

3.   In the **Zone Details** section, click the **Supports Rev Connect** checkbox and configure a Rev Connect Zone.

Field Name	Required	Description
Supports Rev Connect		Disabled by default. If it is not present, then check that your account has purchased Rev Connect licenses. (See: Rev License Types and Add-On Components)
		Once enabled, it allows the current zone to use Rev Connect and displays additional controls in the Zone form.
		Reminder: The default order of available streams is the following: • Vbrick Multicast • Flash Multicast • Rev Connect • Unicast Streams
Restrict Peer Meshes Within IP/IP Ranges		Disabled by default.
		If disabled (unrestricted), viewers selected for this zone are eligible to be put into the *same* Peer Meshes.
		If enabled (restricted), viewers selected for this zone are eligible to be put into Peer Meshes that *align* to the IP Ranges.
		Note: If you previously used a Rev Connect enabled zone and the **Use Rev Connect IP Groupings for Peers** checkbox (now deprecated), this setting is set to true/false based on that prior setting as of Rev v7.31. You may modify this at any time.
Disable Unicast Fallback		Visible when Rev Connect is enabled.
		This feature controls the ability for the player to fallback to a unicast stream (if available). If enabled, then the Zone will only support Multicast or Rev Connect. This is useful if you are trying to optimize the ingress bandwidth to a Zone location.
Maximum Number of Peer Meshes	Yes	Visible when Rev Connect is enabled.
		This allows Administrators to define the maximum number of peer meshes to be created for the zone. This is not a reservation, but an upper limit on what can be used within the zone based on licensing restrictions for the Rev account.
		Zones enabled for Rev Connect will be able to concurrently use up to the Account licensed amount of peer meshes. These may be split across several Zones. Once at capacity, new viewers/players will fallback to Unicast in accordance to the Zone settings.

Keep in mind:

• If a Rev Connect Zone is used during a Webcast, it will be noted in the Webcast Attendees Report once the event has ended.

- If you use a Rev Connect Zone during a Webcast Event, a Rev Connect Zone report may be downloaded once the event concludes.

> **Note**: If you add a Rev Connect enabled zone, you should make sure you list your outbound connections. **See**: Allowed Lists and Required Rev URLs

Download the Webcast Event Attendees Report

Download the Rev Connect Zone Report

Zone Logic and Hierarchy

As noted, when adding a new zone or sub-zone, consider where your users and devices are located and/or how you want your content to be ingested and viewed on your network.

When you configure zone hierarchies, you provide a fail-over for your content distribution if your devices in a specific zone fail for whatever reason.

For example, in the image below, the **Washington, DC** zone is nested under the **East Coast** zone, which is nested under the **United States** zone (which in turn is nested under **North America**).

Users should be directed to zones based on their IP addresses. Recall that IP address ranges for a zone may be specified when you Add a Zone.

▼ Using an example where a user is directed to the Washington, DC zone:

1. If Rev detects that the DME associated to the **Washington, DC** zone is available, then the user will be served the video off of that DME.

    However, if Rev detects that the DME is unavailable in **Washington, DC**, it will direct the user up the zone hierarchy to the **East Coast** zone.

2. If Rev detects that the DME associated to the **East Coast** zone is available, the user will be served the video off of that DME.

However, if Rev detects that the **East Coast** DME is unavailable, it will direct the user up the hierarchy to the **United States** zone.

This will continue for as many levels of the zone hierarchy that have been configured. If the user cannot be served video off a device in the highest level of configured zones, the system will direct the user to the default zone as a last resort.

> **Additional Information**: When using Rev in the cloud, users behind a corporate firewall will appear as if they are coming from the same external IP address. To prevent this and utilize Rev's zone logic and hierarchy to maximum effect, Rev allows you to obtain an internal IP address. See: The DME User Location Service.

For VOD files, Rev will fail up to the Rev File Store as a last resort if all the DMEs in your configured hierarchy are offline.

> **Tip**: If multiple DMEs are assigned to a zone, all DMEs will be tried before the next zone in the hierarchy will be attempted.

> **Caution:** If zone logic is disabled by an Account Admin, zone logic will only return the playback URL of the DMEs in the user's matched zone and zone logic will *not* return a playback URL from Rev.
>
> Further, if there is no matching URL, then the user will be displayed the following message: "Playback of this video is not available at this time. Please try again later."

Add a Distributed Media Engine (DME)

View the Status of a Device

The DME User Location Service

Enable Zone Fallback for VOD Streams

DME Network Statistics

Use the **DME Network Statistics** menu to monitor your DME overall health, activity, and video usage statistics of each DME in your network.

▼ To view DME network statistics:

1. Navigate to **Admin** > **Devices** > **DME Network Statistics**.
2. Immediately displayed is health information for each DME including percentages used for CPU, memory (including swap space), disk space, and throughput. The bar colors associated with health information are described in the table below.
3. If DME Stream Authorization is enabled, the Used For Streaming column will display either Authorized or Error depending upon if content is being sent to the DME. See: DME Stream Authorization Lockdown Management for details.

4. Clicking the DME name displays a dropdown of more information about that specific appliance including IP address, MAC address, and version (some data will not be available for older DMEs prior to v3.6)

5. You are also presented four buttons that provide more information and the ability to edit DME settings. The buttons provide the following abilities:

   • **DME Administration**: Links to the DME Admin interface so you may edit settings as needed in the DME. You must know your DME Admin login information. Note: DME v3.14 has implemented preventions that thwart Cross-Site Request Forgery (CSRF) prevention. Customers that select the DME Administration button may see a 500 error. If this occurs, click the reload the browser page and gain direct access.

   • **Rev Configuration**: Links to DME settings in Rev for editing. See: Add a Distributed Media Engine (DME) if you are not sure how to configure a DME for Rev.

   • **View Log**: Server logs for this DME. You are able to view specific actions that occur with the Show Details button on the log.

   • **Reboot**: Reboots the DME device.

6. Admins can also view the following point in time server stream usage information for each DME:

   a. Percentage of total available streams used by incoming versus outgoing streams

7. Admins can view the following point in time Multi-Protocol Server (MPS) server stream usage information for each DME:

   a. Percentage of total available streams used by incoming versus outgoing streams.

8. Admins can view a breakdown of stream information for each streaming server:

   a. Number of incoming streams

   b. Number of outgoing unicast streams

   c. Number of outgoing multicast streams

9. Admins can view the percentage of usage of transrating for each DME (N/A is displayed if transrating is not licensed on the DME).

10. Admins can view the number of recordings occurring on each DME.

TRANSRATING STREAMS	RECORDINGS	STREAMS		
			Unicast	Multicast
0 (0 %)	0			
		RTP	0	0
		MPS	0	0

11. DME versions prior to v3.6 will not display throughput or MPS server stream usage. If data cannot be retrieved from a DME because it is an older version, an indicator will be displayed.

The table below illustrates the threshold values that are used for the health data that is reported for the DME. Data change is indicated by color and corresponds to the following values: Normal (no color change), Caution (yellow), Alert (red).

Health Data Reported	Normal	Caution	Alert
Throughput (reported in Mbps and percentage against license)	< 60%	60 - 90%	> 90%
CPU Usage (reported in percentage across cores)	< 70%	70 - 80%	> 80%
Memory Usage (reported as aggregate total and percentage)	< 50%	50 - 85%	> 85%
Disk Space (reported as total and percentage)	< 75%	75 - 85%	> 85% or < 32GB whichever is smaller
Current Pulls	1 - N		
Current Pushes	1 - N		
Current VOD Retrievals (reported as number, with total allowance, and percentage of total)	< 70%	70 - 85%	> 85%
Current Live Retrievals (reported as number, with total allowance, and percentage as total)	< 70%	70 - 80%	> 80%
Overall DME Health (calculated status = max status; CPU, memory, total of all streams)			
DME Mesh Status (count of reachable peers, total peers, percentage reachable) status based on percentage reachable	> 50%	20 - 50%	< 20%

DME Management

Use the **DME Management** module to add, configure, and perform bulk schedule, reboot, and software update actions on DMEs that you use with Rev.

The **DME Management** module displays:

Column	Description
Name	Name or Hostname of the DME.
Version	The current version/build of the DME.
Mac Address	The MAC address of the device.
Scheduled Download	If the DME has scheduled download times.
Status	The status of the device; Online, Offline, or Inactive. If inactive, your device will not be able to be accessed by Rev. While updating the software of the DME, the progress of the update will also be displayed here.
Used for Streaming	Specifies if the DME is authorized for streaming and not in lockdown status. See: DME Stream Authorization Lockdown Management and Enable DME Stream Authorization Lockdown
MFSTB	Specifies if the DME has been designated as a STB Connector DME. See: Designate a DME as a MF-STB Connector DME
Actions	The actions you may perform on the DME. • **Sync Now**: Perform an immediate synchronization. See: Synchronize DME Content. • **Reboot**: Reboot the selected DMEs. This bulk reboots all selected DMEs or a single DME if only one is selected. See: Reboot a Device • **View Log**: View a log of recent actions that have occurred on the device. This is good for troubleshooting if your device is not performing as expected. See: View and Request Device Logs • **Request Logs**: Gathers necessary logs from the DME and sends them securely to Vbrick Support. (Requires DME v3.24+. This can also be completed in Bulk Actions with one ore more DMEs selected. Do not complete this action during events as it can be labor intensive. An email and notification is generated when the logs are complete and support is able to view them. See: View and Request Device Logs • **Delete**: When a device is deleted, the content stored on the device is not deleted. However, you may not access it because the association to the device is removed. See: Delete a Device

Additional functionality:

Function	Description
Add DME	Adds a new DME association in Rev.
Bulk Actions	**Reboot:** Reboots the selected DMEs. You must have at least one DME selected.
	Scheduled Download: Set up an identical download schedule for several DMEs at once. See: Create a Bulk Scheduled Content Synchronization for DMEs
	Update: Update the software version for one or more DMEs. See: Update the Software Version of DMEs
	Request Logs: Request the logs of one or more DMEs be sent to Vbrick Support. Must have v3.24+ of the DME software installed. See: View and Request Device Logs

Add a Distributed Media Engine (DME)

To optimize delivery of your content across your enterprise network, Vbrick Rev easily facilitates adding a DME to your environment. DMEs are designated as the viewing destinations of your video content on the network where content may be distributed and viewed.

> **Tip**: Make sure you configure your Vbrick devices before you begin adding them. See: Device Initial Configuration and Set Up

▼ To add a DME device:

1. Navigate to **Admin** > **Devices** > **DME Management** > **Add DME** button.
2. Complete the fields as required.

Field Name	Required	Description
Device Name	Yes	This can be a name of your choosing. This is a required field. Descriptive location or host name is recommended.

Field Name	Required	Description
Status		The status of your device may be set to **Active** or **Inactive** upon adding it to your system.
MAC Address	Yes	The MAC Address is required. Refer to your device's documentation for details on how to obtain its MAC Address.

Field Name	Required	Description
VOD Playback Device		Selected if the DME is intended to be used as a Video on Demand (VOD) playback device for serving stored video content. If more than one DME is designated as available for storage, then content will be pushed to all such designated DMEs. This is selected by default.
Preposition Content		Selected by default. Enable this setting to specify which DMEs on the network receive prepositioned video files for playback; should only be used if using MESH. You can also then set your download schedule if you so choose. See: Preposition DME Content

Field Name	Required	Description
Video Streams	Yes	**Name**, **URL**, **Encoding Type**, and **Multicast** are all designated [through the **Advanced** tab > **Add URL** button if adding manually] and are required fields if the DME is intended to be utilized as a streaming device. These streams will later be selected on **Presentation Profiles** and **Zones** as viewing destinations. You may also generate your URLs dynamically through the **Create URLs** tab. Note: DME v3.10 and greater devices are capable of registering fully qualified domain names in order to play HTTPS content to the Rev HTML5 video player. Therefore, DME streaming URLs may or may not contain an IP address Hostname. See DME documentation for set up details. For more information on DME **Video Streams** in Rev, see: Add a Distributed Media Engine (DME) Video Stream.

3. Click the **Create** button.
4. After a few seconds, the DME status should flip from **Uninitialized** to **Active**. If it does not, check your **MAC Address** field to ensure it is correct and the DME configuration steps such as the **API key** and **Host** fields. See: Device Initial Configuration and Set Up.
5. Your device is now ready to use with Rev.
6. Account Admins will be sent an email notification if any DME or Encoder goes into Warning or Offline status so that they may pro-actively troubleshoot the device. The email will include when the device went into warning or offline status (date/time), the device name, and a link to the device.

> **Caution**: If you add more than one DME to your system, be sure to designate your primary DME recording device. A DME is required if you intend to record video in Vbrick Rev.

Supported Vbrick Devices

Add a Distributed Media Engine (DME)

Add a Distributed Media Engine (DME) Video Stream

View the Status of a Device

View and Request Device Logs

Synchronize DME Content

Update the Software Version of DMEs

Set a Primary and Secondary DME

Add a Presentation Profile

Add a Zone

Zone Logic and Hierarchy

Add a Distributed Media Engine (DME) Video Stream

DMEs may be designated as streaming devices on the network where content may be distributed and viewed. Presentation Profiles and Zones may use these defined streams. Video streams on a DME may be set up manually or dynamically by the DME itself. Both methods are described below.

> **Note**: An RTSP unicast stream is required for recording live Webcasts in Rev. Make sure that your stream has a keyframe interval between 2 to 5 seconds and do not use B-frames. Please see your individual Encoder (stream source) documentation for setting information.

Add a DME Video Stream Manually

The **Advanced** tab under **Video Streams** is used to create your own manual stream.

▼ To add a manual DME video stream:

1. Navigate to **Admin** > **Devices** > **DME Management** > **Add DME** button.
2. Add a DME device as you normally would. See Add a Distributed Media Engine (DME).
3. Click the **Advanced** tab in the **Video Streams** section.

Field Name	Required	Description
Name	Yes	A name for your video stream.
URL	Yes	The URL of your video stream. Copy your created URLs to this field.
Encoding Type	Yes	The encoding type that will be used; select from the drop-down menu.
Is Multicast		Select if your video will be multicast.

Add a DME Video Stream Dynamically

The **Create URLs** tab under **Video Streams** is used to create your own dynamic stream playback URLs in Rev so that you do not have to create them manually and then copy them to Rev as described above. Note that creating a dynamic stream works with DME v3.4 and above only. If you do not have v3.4 or above, you must create a manual video stream.

▼ To add a dynamic URL DME video stream:

1. Navigate to **Admin** > **Devices** > **DME Management** > **Add DME** button.
2. Add a DME device as you normally would. See Add a Distributed Media Engine (DME).
3. Click the **Create URLs** tab > **Add URL** button in the **Video Streams** section.

Field Name	Required	Description
Name	Yes	A value representing the stream name. The stream name must be unique within the DME that you are currently adding. If you are setting up several DMEs to distribute the same stream, consider using the same stream name across DMEs so that you can easily trace the stream across multiple DMEs. Stream names must be alphanumeric and contain no spaces. Stream names are not case sensitive.
Enable Vbrick Multicast		Select if you want to enable Vbrick multicast streams. You must have DME software 3.18 or greater before this may be configured. Once selected, enter the following to automatically configure Vbrick multicast streams: • Multicast IP Address: (required) Must between 224.0.0.0 and 239.255.255.255 • Multicast Port: Default is 4444 • Packet Size: (entry 1000 to 8192) in Bytes, default: 4096 • Please note that the IP Address and Port cannot be duplicated across multiple streams • HLS streaming options are independent of Vbrick multicast streams • If the IP Address, Port, or Packet Size values fail, Rev will display a configuration failure message and will request that you edit the values again
Enable HLS		Select if you want to create an HLS stream. This is required for mobile devices. The default is no.

Field Name	Required	Description
Add HLS Akamai Publishing Point		You must have the HLS checkbox enabled before this becomes visible and you must have DME software 3.17 or higher before this can be configured.
		Once selected, enter the following to automatically configure an Akamai HLS Publishing Point (obtained from Vbrick Operations):
		• Akamai Post Host Name (required)
		• Akamai Playback Host Name (required)
		• Akamai Stream ID (required, numeric only)
		• Akamai Shared Auth Key (not required if encryption is not desired)

When the DME is saved or updated, the following will occur:

• An RTMP (Flash) stream will be created and enabled using the provided stream name.

• An RTSP stream will be created and enabled using the provided stream name.

• If Vbrick Multicast was enabled, a Multicast stream with -VBM appended will be created.

• If HLS was enabled, an HLS stream will be created and enabled using the stream name.

• If an Akamai Publishing Point was created, the Akamai HLS stream will be visible and using your stream name.
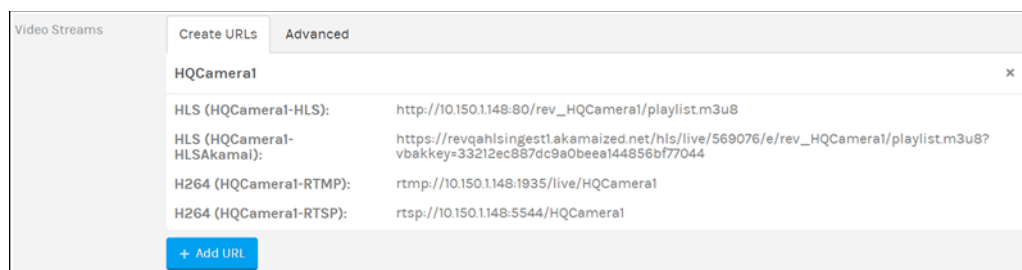
> **Note**: If for any reason one or more of the URLs cannot be created, none of the URLs will be created and an error message will be displayed.
>
> If you have previous publishing points and want to add Akamai publishing points, you will need to delete them and recreate them to add the Akamai streams.

Presentation Profiles and Zones list the different available streams created as well. Including the Akamai streams created with the Akamai logo and Vbrick Multicast streams with the Vbrick logo if applicable.
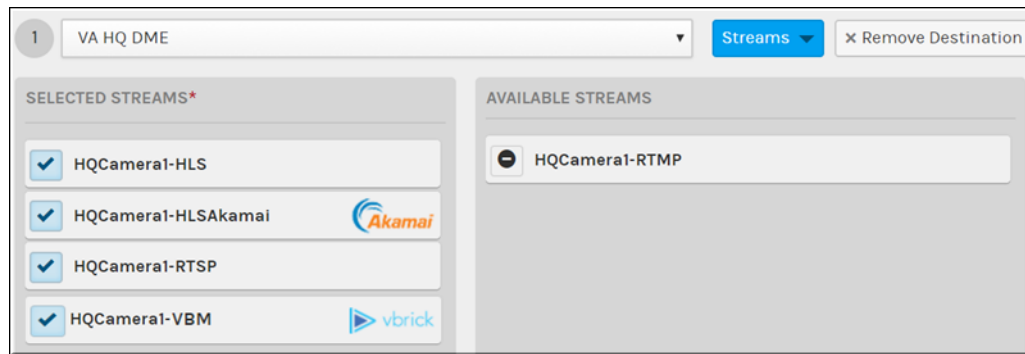
> **Note**: Some set up is required before you may create live streams in Rev. A quick setup guide that steps you through the entire process is located in the Rev Supplementary Documentation section titled: Streaming Live Video to Rev Webcasts.

Add a Distributed Media Engine (DME)

Add a Distributed Media Engine (DME)

View the Status of a Device

View and Request Device Logs

Synchronize DME Content

Update the Software Version of DMEs

Set a Primary and Secondary DME

Add a Presentation Profile

Add a Zone

Zone Logic and Hierarchy

Enable and Configure a DME for Automatic Multicast and Reflection

> **Note**: The new Automatic Multicast and Reflection services requires installation of DME v3.23 and Vbrick Multicast (VBM) Agent v1.2.

DMEs that have been upgraded to v3.23 or higher may be configured to use automatic multicast and reflection for Video Conference sourced Webcasts. In effect, each VC Webcast is automatically transformed into Vbrick multicast and distributed to viewers from specified DMEs. Viewers must be using the Vbrick Multicast Agent v1.2 (or higher) to receive the multicast within their browsers. (See: Vbrick Multicast Installation Quick Reference Guide) Viewers who cannot take advantage of multicast can alternatively receive an automatically reflected stream from the DME (saving corporate bandwidth).

Both of these approaches greatly expand the reach of your Live Video Conference sourced Webcast. This feature includes all Vbrick video conference integrations. (See: Supported Video Conference (VC) System Integrations)

Additionally, DMEs can be configured to automatically multicast and/or reflect third party HLS URLs during a Webcast. Remember that using this service to pull HLS will not provide a RTSP stream for recording. Make sure, if you are to record the event, that you provision an RTSP stream to a recording DME.

Here are the steps and considerations to using automatic multicast and/or reflection in Rev:

1. Make sure all multicast viewers have the VBM Agent v1.2 or higher.
2. Coordinate with your Network Administrators to get a block of Multicast IP addresses (you will need this for the configuration).
3. Enable and configure automatic multicast settings on the DME(s) you want to use.
4. Once the DME is enabled for automatic multicast, you are then able to utilize the feature in two different ways:
    a. Automatically multicast live stream video conference activities.
    b. Create a custom device and automatically multicast 3rd party HLS streams through a presentation profile.
5. Each method is described in more detail below once a DME is enabled for the feature.

As noted, Automatic Multicast is only available for DME devices that have v3.23 (or higher) installed, along with VBM Agent v1.2 (or higher). If you do not see the appropriate sections within your Rev UI described below, contact your Account Admin to upgrade the DME.

▼   To enable and configure automatic multicast settings on a DME device:

1. Navigate to the DME you want to configure.
2. Select the **Enable Automatic Multicast** checkbox and complete the following fields.

Setting	Description
Multicast IP Addresses	Enter the range of IP addresses to be used for automatic multicasting. Keep in mind the best practices that should be followed when assigning a multicast address (described below).
	Also, it should be pointed out, that every DME that has this feature enabled will have a set of multicast addresses. These are the addresses that Rev will assign to each new automatic multicast as they are created. Rev keeps track, and will not hand out duplicate multicast addresses within an account. Best practices is to provide a large number of multicast addresses.
	For example, you could use the range: 239.110.1.0-239.110.1.255 (this is a random range, but still within the 239 space). This range provides for 255 multicast addresses. Of course, this depends on the number of simultaneous multicast streams you will have. Best practices is to provision many multicast addresses – they will not be used until needed, and will be recycled after use. For simplicity of network administration and stream identification, if you have multiple DMEs generating the automatic multicast, you can use the same range and Rev will provision unique addresses (within that range) each time. Again, please work with your Network Administrator to get the block of multicast addresses.
Port/Port Range	You can enter a single port or range of ports.
	Best practice is to enter a single port. This is because if there are two different multicast streams on a given multicast IP with different ports, then each device (think router, switch, or end consumer) will have to receive the two streams. This creates unnecessary overhead. Therefore, while multiple ports are supported, best practice is to use one port and provision many multicast IPs.
	For simplicity, Vbrick recommends the default value: 4444
Packet Size	You can set the packet size for the multicast. This is an advanced feature, and the recommendation is to accept the default.
	The default value: 4096

Setting	Description
Default Rendition Selection	When the DME pulls a remote HLS stream (either for Video Conference streams or 3rd party HLS), it must decide which rendition or specific bitrate to convert to multicast. A multiple bitrate (MBR) stream can have a number of bitrates to choose from. This setting, which applies to all automatic multicast generated from this DME, will define which rendition.
	If the HLS stream has only one rendition, it will be used. Otherwise, it will use either the High Bitrate or Low Bitrate rendition based on setting.
	If you have the need to separate out your HLS into multiple different automatic multicasts based on bitrate, then best practice is to set up different DMEs – one to always generate High Bitrate multicast, and the other will generate Low Bitrate multicast. Please review the use of these DMEs within the appropriate zones, and use the Automatic Multicast stream from each DME accordingly.

Assigning a Multicast Address

Many factors must be considered when designing a multicast address infrastructure since Ethernet switch implementations can significantly vary between vendors. Furthermore, multicast addressing techniques rely on an Ethernet to IP Address mapping rule, which does not guarantee a unique physical address. In fact, it is possible to create multicast addresses that differ from an IP perspective, but overlap when presented to the Ethernet network.Addresses created in this situation can cause significant network and operational problems.

Specifically, multiple IP Addresses are mapped into the same physical layer address. For example, all IP multicast addresses with the same or differing first octet, and the second octet differing by exactly 128, map to the same physical address (226.5.5.4, 227.5.5.4, and 228.133.5.4 all map to the same physical address).

Another factor to keep in mind when assigning multicast addresses is that 224.x.x.x is a range containing reserved addresses, particularly in the range 224.0.0.x. For example, 224.0.0.1 is the 'all hosts' multicast address and 224.0.0.2 is the 'all routers' reserved address. Other 224.0.0.X numbers are reserved for RIP, OSPF, DVMRP, etc. Here are some recommended rules for multicast IP Address assignment:

1. Do not use 224 in the first octet since many of these are reserved. (Vbrick encoders enforce this rule.)
2. Use a digit between (225–239) for the first octet and standardize on it for each network.
3. In the second octet, either use numbers from 1–127, or 129–255, do not mix ranges on a given network.

Use Automatic Multicast with Video Conferences

To use automatic multicast with live Video Conference streaming, configure streams as you normally on the DME by enabling Vbrick Multicast. Now every VCI stream will be automatically multicast from the DME. Each Zone, that has multicast viewers, should include

the DME with multicast as a destination, and the stream title Automatic Multicast. In that way, that Zone will use that DME for multicast.

See: Add a DME Video Stream Dynamically

Use Automatic Multicast with Custom Devices

You can also configure custom HLS URLs to be used for Automatic Multicast and Reflection. This is done by associating a **Custom Device** (which has HLS URLs) with the DME. Then these streams can be utilized within a **Presentation Profile** to enable them for reflection and automatic multicasting during a Webcast. This means you can allow 3rd party HLS streams (and encoders) to utilize the automatic multicast feature.

Note: There are some HLS streams and tags that are not supported as mentioned in the DME Help topic, "Rev Initiated Multicast and Reflection".

▼   To configure automatic multicast streams on a DME:

1.   In the **Video Streams** section of the DME, click the **Custom Devices** tab.
2.   Click the **Add Custom Device** button and complete the selections as follows.

Setting	Description
Select a Custom Device	This is a custom device that you would have already created. Only HLS streams can be used for this feature so the custom device must have one or more HLS streams. See: Add a Custom Device
Select a Stream Name	Each stream has a unique name (when you created the Custom Device). Here you select the appropriate name for the URL stream you wish to use for multicast and/or reflection. Note that you may not use the same name more than once.

Setting	Description
Enable DME Reflection	Select this checkbox if you want the DME to reflect the stream(s). Clicking this will create a new stream within the DME (the name is listed within the user interface.) This stream must be included within the Presentation Profile (with the DME as the Destination) to generate automatic reflection through the DME. Including the Custom Device as a Destination within the Presentation Profile will use the stream(s) as it does today – unicast. **Note**: At least one of the Enable DME Reflection or Enable Automatic Multicast checkboxes must be selected.
Enable Automatic Multicast during webcast	Select this checkbox if you want to enable automatic multicasting during Webcasts. Clicking this will create a new stream within the DME (the name is listed within the user interface.) This stream must be included within the Presentation Profile (with the DME as the Destination) to generate automatic multicast from this DME. Including the Custom Device as a Destination within the Presentation Profile will use the stream(s) as it does today – unicast. **Note**: At least one of the Enable DME Reflection or Enable Automatic Multicast checkboxes must be selected.

Identify Automatic Multicast and Reflection Streams in Rev Zones

After you have set up your Rev devices, make sure the **Supports Multicast** checkbox is selected on your Rev Zone(s) to enable selection of your DME configured for automatic multicast. Those streams that you enabled for automatic multicast and reflection are now available.

Distinct graphic visualizations are now associated with each stream type are available as well and are described below.
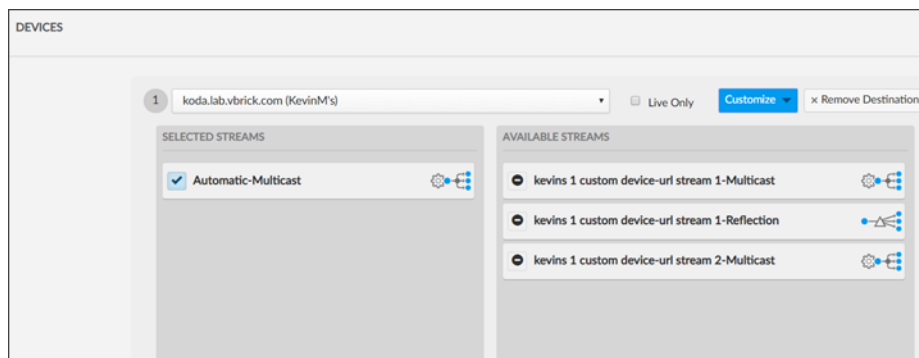
Each icon and its associated meaning is described below:

Icon	Description
	Stream that has been enabled for automatic multicast.
	Stream that has been enabled for cloudstream.
	Stream that has been enabled for flash multicast.
	Stream that has been enabled for multicast.
	Stream that has been enabled for reflection.
	Stream that has been enabled for unicast.

Note: Presentation Profiles have the same visualization icons for streams.

DME Stream Authorization Lockdown Management

Enabling DME Stream Authorization in Rev places all DMEs in a lockdown state where playback of Live or VOD HLS assets requires authorization. When enabling (or disabling) this feature, Rev directs each DME to change its Stream Authorization state.

There are several configuration items that are necessary for a DME to enter this state. Most are automatically handled by the DME and include:

When DMEs are placed into lockdown by enabling this setting in Rev, the following steps are taken within each DME automatically:

- All DME Network Time Protocol (NTP) synchronization fields are enabled and set so that all DMEs can have a consistent time. NTP uses UDP port 123, so please plan accordingly. Customers that restrict traffic through Proxy should consult their network support staff. DMEs that cannot sync time will not be able to participate in content sharing.
- All DMEs are set to distribute content via HTTPS only.
- All DMES are checked to ensure that a valid security cert is in place.

If all three of these properties are met or set successfully, the DME returns a success message to Rev and is placed into a lockdown state.

DMEs that are *not* successfully placed into a lockdown state will not receive playback URLs from Rev. Rev automatically provides authorization encoded into the playback URLs for those DMEs that are in a lockdown state. DMEs receive the request, validate the security token, and subsequently authorize the stream.

Admins may put their entire systems into and out of this lockdown state as needed or required.

Caution: iOS Safari (on iPhones) requires additional playback considerations when utilizing Stream Authorization. This includes:

• Because your DMEs (which are on premises) and Rev (which is in the Cloud) have two different domains, default configuration on iPhones disallows playback. To fix this, disable cross-site tracking. This is done on your iOS device by visiting **Settings** -> **Safari** -> **Prevent Cross Site Tracking**.

• iOS Safari in Private Mode does *not* support playback when DMEs are utilizing Stream Authorization.

The **DME Management** and **DME Network Statistics** page(s) within Rev may be reviewed to check on the status of each DME once this setting is enabled. As noted, DMEs that cannot enter the lockdown state will not be used for content delivery. This feature provides even higher level security than the existing user/video access level currently provided in Rev.

In addition to using the two modules above, DMEs that are used for streaming when this setting is enabled may also be edited and have their authorization viewed as seen below. If the DME is not authorized, an error will be seen instead.

Note: You must have all of your deployed DMEs on Version 3.21 (or later) to use this functionality. DMEs on previous versions will not be used for content distribution. Best Practice is to update all your DMEs before attempting to use this feature.

Enable DME Stream Authorization Lockdown
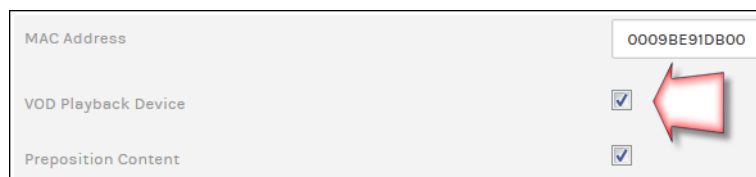
DME Management

DME Network Statistics

Designate a DME Video Playback Device

You have the ability to designate which DMEs in your video ecosystem are used for storage and playback so that you can easily organize and distribute your content positioning. If more than one DME is designated as available for playback, then content will be pushed to all VOD designated DMEs.

▼ To designate a DME video playback device:

1. Navigate to **Admin** > **Devices** > **DME Management** > **DME Name**.

2. Select the **VOD Playback Device** checkbox.

3. If VOD playback is enabled on a DME, individual videos may be prepositioned to it. See: Enable Prepositioning of Individual Videos.

Add a Distributed Media Engine (DME)

View the Status of a Device

View and Request Device Logs

Synchronize DME Content

Synchronize DME Content

Update the Software Version of DMEs

Enable Prepositioning of Individual Videos

Preposition DME Content

This feature is used in conjunction with the DME mesh caching configuration (See the "Mesh with Rev Caching Configuration" topic in DME Online help).

With this configuration, you can designate which DMEs in your video ecosystem will have content prepositioned immediately (downloaded to the DME immediately after upload) or scheduled (by day of the week and time) by selecting the **Preposition Content** checkbox. This option is only available for DMEs that are also selected as a VOD Playback Device.
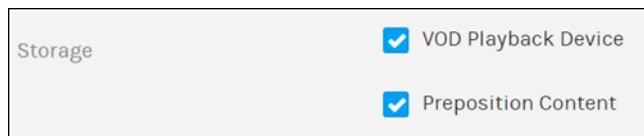
Rev will use zone logic to route content requests by end users to the closest DME. If the DME closest to the user does not have the requested content, that DME will get the content from a "sister" DME that has the content. The content will then be cached on the new DME and will be available for the next person requesting it. Initially, the only "sister" DMEs that will have the content are the prepositioned DMEs. Subsequently, as the content becomes available on more DMEs based on user content requests, any DME that has cached a copy of the content will be a sister DME from which other DMEs can then retrieve the content.

This means that content is only pushed to a handful of DMEs initially, so fewer downloads will be pushed through the cloud and into the network for Rev cloud customers.

> **Caution**: You should make sure that all DMEs in your network are able to communicate with at least one DME that has all prepositioned content.
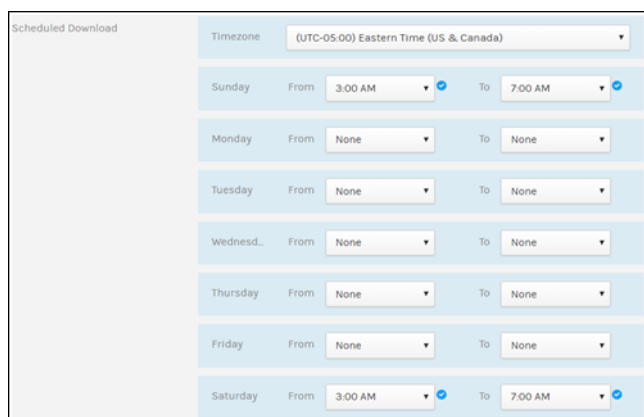
As mentioned, view the "Mesh with Rev Caching Configuration" in DME Online help for details on how to enable mesh caching in DME.

▼   To specify that a DME prepositions content:

1.   Navigate to **Admin** > **Devices** > **DME Management** > **DME Name**.

2.   Select the **VOD Playback Device** checkbox.

3.   Select the **Preposition Content** checkbox.

4.   When the **Preposition Content** checkbox is selected, **Scheduled Download** time frames appear where you may dictate when this DME may receive video files so that network traffic can be managed by timezone, day of the week, and hourly if desired. For example, the image below shows that this DME will <u>only</u> have content pushed to it on Saturday and Sunday between the hours of 3:00 a.m. and 7:00 a.m. eastern time.

5.   If no scheduled download times are set, content will always be pushed to the DME as soon as it is finished transcoding.

There are several instances where a DME will trigger a Rev Mesh update. They are:

•   If any DME reports a new Hostname or IP to Rev

•   If any DME reports a new software version number (including build)

•   If any DME reports a change in http / https serving status to Rev

•   If any DME preposition status is changed (enabled or disabled) on Rev

•   If any DME status (Active or Inactive) is modified

•   If any DME VOD Playback Device setting or status is modified

Enable Prepositioning of Individual Videos

Preposition an Individual Video

Designate a DME Video Playback Device

Synchronize DME Content

Account Admins have the ability to initiate a content sync to a DME so that users may begin obtaining content from that DME. This is useful if the DME is added later to the video ecosystem so that it may obtain all current content in Rev.

▼   To synchronize content to a DME:

1.   Navigate to **Admin** > **Devices** > **DME Management** > **DME Name**.

2.   Click the **Sync Now** button. This button will only be visible if the DME is in **Active** status and the **VOD Playback Device** checkbox is checked.

Upon sync initialization, the following occurs:

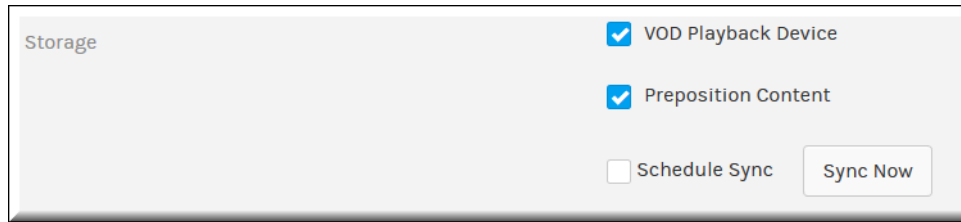•   The DME begins downloading all active videos in Rev in batches of ten.

•   The oldest content will be downloaded first (ascending by upload date/time)

•   During the sync, playback URLs will be updated based on the following:

   a.   If playback URLs already exist for the given DME and video, playback URLs will be overwritten.

   b.   If playback URLs do not exist for the given DME and video, playback URLs will be added.

Keep in mind:

•   If your DMEs support the MESH caching feature, the DME will attempt to get the videos from a meshed DME first before it attempts to retrieve files from Rev. See the "Mesh with Rev Caching Configuration" online help topic in DME help.

•   The DME will only download files that it does not have.

•   The DME will always send back playback URLs, even if it already has the content, to indicate to Rev that the video has been synced.

•   The content sync may be canceled at any time by clicking the **Cancel** button. All videos that have been sent to the DME for download will continue. All videos that have not yet been sent to the DME (queued) will be canceled.

•   You may also sync the device from the **Actions** dropdown on the **All Devices** page.

Add a Distributed Media Engine (DME)

View the Status of a Device

View and Request Device Logs

Designate a DME Video Playback Device

Preposition DME Content

Update the Software Version of DMEs

Schedule an Individual DME Content Synchronization

Account Admins may specify when the system initiates a DME content sync so that it may be conducted during non-business hours.

▼   To schedule a DME content sync:

1.   Navigate to **Admin** > **Devices** > **DME Management** > **DME Name**.

2. You may schedule the sync from either the additional actions dropdown or by editing the DME device to sync and clicking the **Schedule Sync** checkbox.

You may specify the following when scheduling a DME sync:

*   Start date
*   Start time
*   Timezone

Keep in mind:

*   A content sync may only be scheduled in the future.
*   If a pending sync has already been scheduled, it will be noted in the **Status** column of the device on the **All Devices** page.
*   A scheduled sync can be canceled at any time by unchecking the **Schedule Sync** checkbox and saving your changes. If the scheduled sync has already started, you can cancel the sync by clicking the **Cancel** button.
*   As noted, you may also schedule the synchronization from the **Actions** dropdown on the **All Devices** page.

Create a Bulk Scheduled Content Synchronization for DMEs

Add a Distributed Media Engine (DME)

View the Status of a Device

View and Request Device Logs

Designate a DME Video Playback Device

Preposition DME Content

Update the Software Version of DMEs

Create a Bulk Scheduled Content Synchronization for DMEs

If you have several DMEs associated to Rev, you may also create a schedule for all of them at once to synchronize their content so that Rev performs this maintenance at the same time every day and you are easily able to manage this under one intuitive interface.

▼   To create a bulk schedule content sync:

1. Navigate to **Admin** > **Devices** > **DME Management**.
2. Select the checkbox to the left of each DME that you would like to add to your schedule.
3. Click the **Bulk Action** > **Scheduled Download** button.
4. The scheduling window appears.

You may specify the following when scheduling a DME sync:

- Start date
- Start time
- Timezone

Keep in mind:

- A content sync may only be scheduled in the future.
- If a pending sync has already been scheduled, it will be noted in the **Status** column of the device on the **DME Management** page.
- A scheduled sync can be canceled at any time by editing the individual DME's schedule.

> **Note**: All selected DMEs will be set to preposition content as part of scheduling their download windows.

Schedule an Individual DME Content Synchronization

Add a Distributed Media Engine (DME)

View the Status of a Device

View and Request Device Logs

Designate a DME Video Playback Device

Preposition DME Content

Update the Software Version of DMEs

Update the Software Version of DMEs

If you have one or more DMEs associated to Rev, you may install DME software updates directly from Rev to multiple DMEs at once so that you do not have to go to each DME individually to do so.

Note the following:

The version the DME(s) you select to be updated will be identified at the top of the module

- If your Admin has not specified a version update this will also be noted. Contact your Admin to enable this functionality and to provide an update path.
- Once the DME(s) have been updated, the new version will be verified in the Version column.
- Bulk updates are not permitted in mobile view.

• During the update process, DME(s) will not be able to record. The status of the update will be displayed in the Status column.

▼ To update the software version of one or more DMEs:

1. Navigate to **Admin** > **Devices** > **DME Management**.

2. Note the version of the software that you will update to at the top of the module to make sure it is correct. If no version is displayed, contact your Admin.

3. Select the checkbox to the left of each DME that you would like to update.

4. Click the **Bulk Action** > **Update** button.
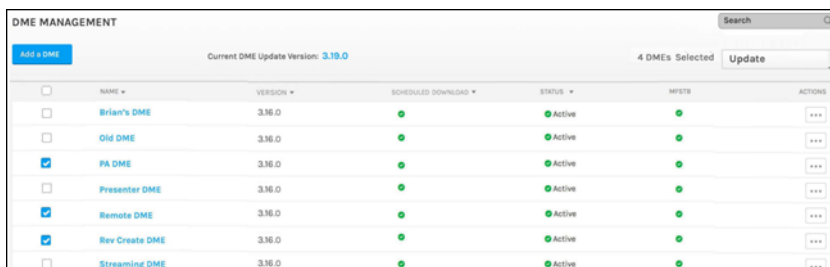
5. A confirmation window appears.
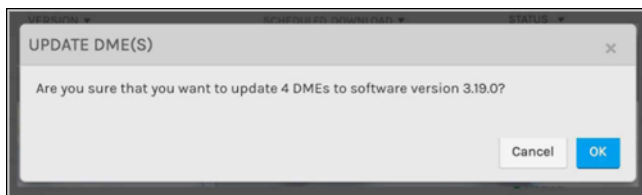
6. Progress of each update will be noted in the DME's **Status** column. The **Version** column will be updated with the new version once complete.
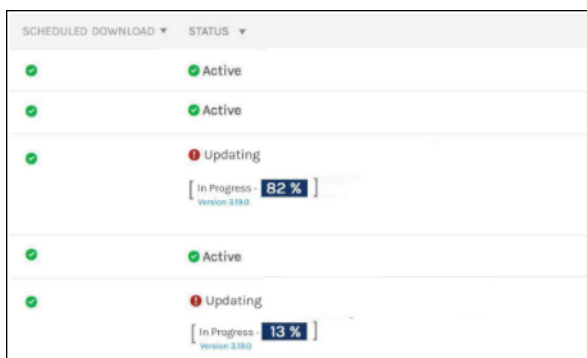
Caution: As noted, you may not use the DME as a recording device during an update.

There are several reasons why a DME may not automatically update. For instance, DMEs do not update if they are within 3.5 hours of a scheduled event including pre-production or Lobby time, are actively recording as the recording DME, or have a sync in progress.

Note that in some cases, it may be up to 15 minutes before the progress percentage of the DME software update is displayed. Be sure to wait until the DME reflects that it is **Active** before administering or using a DME whose software is updated.

Finally, you may not update or "revert" a DME software version to an older version.

Schedule an Individual DME Content Synchronization

Add a Distributed Media Engine (DME)

View the Status of a Device

View and Request Device Logs

Designate a DME Video Playback Device

Preposition DME Content

Designate a DME as a MF-STB Connector DME

If you want to display your video assets from Rev to your Vbrick MF-STB (Multi-format Set Top Box) also referred to as, simply, a STB (set top box), you must do so with a DME which acts as the connector between Rev and the STB.

STBs send out periodic multicast SAP (Session Announcement Protocol) messages and the DME is able to "listen" for them. These messages contain the information necessary for the DME and Rev to connect and communicate with the STB.

Caution: These SAP announcements are multicast and *cannot* go over the general Internet. Therefore, a local DME is necessary to intercept them and send them to Rev. Rev cannot communicate directly to the STB. If your STBs are on a non-multicast network, then a direct connection needs to be made between each STB and DME.

To do so, you will need to SSH/login to each STB and edit the /data/config.txt file. Change the "stb.sap.packet.addr" parameter from the default multicast IP address of 224.2.133.134 to the IP address of your STB Connector DME and reboot each STB(s). You can keep the default 224.2.133.134 **IP Address** setting and the default 9876 **Port** setting in the **Set Top Box Control** section of the STB Connector DME's device settings on Rev as seen in the table below.

This feature only works with the Vbrick MF-STB on Version 2.0.1 or greater.

You must designate which of your DMEs will be the STB Connector so that it will begin "listening" for STBs in your network. Once designated the DME will start to listen and actively communicate the found STBs to Rev. Once found, they will automatically show up in Rev under the **Admin** > **Devices** > **Set Top Boxes** > **Pending STBs** tab form for you to then configure.

> **Note**: The DME must be active and set up properly within Rev before it can be set as a STB Connector DME. See: <u>Add a Distributed Media Engine (DME)</u>.

▼ To designate a DME as a STB Connector DME:

1. Navigate to **Admin** > **Devices** > **DME Management**

2. Edit the DME you want to designate as a STB Connector DME. Remember, each STB is sending out SAP announcements and for Rev to see and use the STB, it must be reachable/visible by a STB Connector DME. STBs that cannot reach a DME cannot be integrated with Rev.

3. Select the **Set Top Box Control** check box. Each of the fields below will be auto-discovered for STBs in your network.

Field Name	Required	Description
IP Address	Yes	The IP Address is the SAP Announcement IP Address on which the STB will multicast their SAP announcements. The DME will use the SAP Announcement IP address and Port to receive STB information.
Port	Yes	The Port Address is the port the STB will use, in conjunction with the SAP Announcement IP Address above, to send out the information for each STB. The DME will use the SAP Announcement IP address and Port to receive STB information.
User Name	Yes	The User Name is the default User Name that will be used for initial communications between DME and STB. If STBs have unique User Names or Passwords, those can be customized on the STB Page from the Set Top Box Management Page within Rev. See: <u>Edit Set Top Box Credentials</u>.
Password	Yes	The Password is the default Password that will be used initial communications between DME and STB. If STBs have unique User Names or Passwords, those can be customized on the STB Page from the Set Top Box Management Page within Rev. See: <u>Edit Set Top Box Credentials</u>.

4. Click the **Update** button to save the DME as a DME Connector. The DME will begin "listening" for set top boxes on the network and each one found will appear on the **Admin** > **Devices** > **Pending STBs** tab. You can accept any of those found as current STBs at this point and configure channel settings.

5. You can see at a glance which DMEs are STB Connector DMEs in the MFSTB column on the **Admin** > **Devices** > **DME Management** form.

> **Caution**: The MF-STB may, in some circumstances, reboot if the RTSP stream it is playing does not exist and is being pulled from DME v3.16.x. Please verify all your streams before sending them to the MF-STB.
>
> If you are using DME v3.17 or greater, this behavior has been corrected.

Set Top Boxes

Accept a Pending Set Top Box

Set a Channel Stream for a Current Set Top Box

Configure Rev Channel Streams for Set Top Boxes

Edit Set Top Box Credentials

Set Top Boxes

Use the **Set Top Boxes** module to add and configure set top boxes that have been identified by DMEs in your system. When you designate a DME in your system as a **STB Connector DME** and it receives a SAP announcement from an active STB, it will pass on the relevant information needed by Rev. If all information is correct, the STB will be automatically created under the **Pending STBs** tab. An Account Admin must then accept STBs on the **Pending STBs** tab to in order to administer them and configure **Channel Settings** on the **Current STBs** tab.

To use Set Top Boxes with Rev:

- MF-STB v2.0.1 or greater (Only Vbrick Multi-Format Set Top Boxes are supported at this time)

- You must have Rev 7.16 or greater installed

- You must have DME 3.16 or greater as your STB Connector

- Only RTP/RTSP/H.264 unicast/multicast stream formats are supported

- Videos must be active before they can be streamed from Rev

- If you want to use Rev's Zone features, you must stream the URL through a Presentation Profile

The current steps to integrate an STB for use with Rev are:

1. Upload a Video through a URL Link (Prepare your videos for STB use)

2. Designate a DME as a MF-STB Connector DME (Prepare your DME)

3. Accept a Pending Set Top Box (Prepare your discovered STBs)

4. Configure Rev Channel Streams for Set Top Boxes (Configure previously added video channels)

5. Set a Channel Stream for a Current Set Top Box (Set a channel on your STB)

Delete a Set Top Box
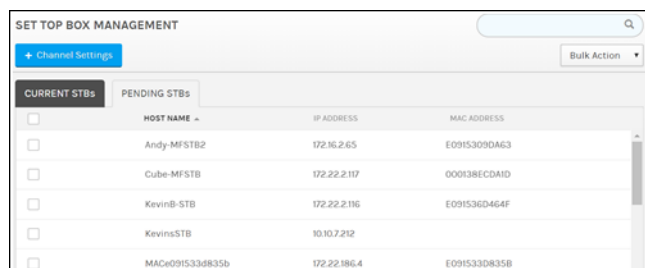
Set the Status of a Set Top Box

Accept a Pending Set Top Box

Once a DME has been designated as a Connector STB, it will listen for the STB you configured and place it under the Pending STBs tab for you to configure. Before you may configure it, however, you must first accept it.

▼ To accept a pending Set Top Box:

1. Navigate to **Admin** > **Devices** > **Set Top Boxes**

2. Click the **Pending STBs** tab

3. Each STB that has been discovered by a DME that has been designated as a STB Connector will be listed.

4. Note that the **Host Name**, **IP Address**, and **MAC Address** of the STB will be displayed if you need it.

5. Select the checkbox to the left next of the STB you want to accept.

6. Click **Bulk Action** > **Accept STBs**.

7. The STB will be moved immediately to the **Current STBs** tab where you can now configure it. This means it is now available to stream a channel.

8. You will receive a confirmation notice next to the **Pending STBs** tab.

Set Top Boxes

Designate a DME as a MF-STB Connector DME

Set a Channel Stream for a Current Set Top Box

Configure Rev Channel Streams for Set Top Boxes

Edit Set Top Box Credentials

Delete a Set Top Box

Set the Status of a Set Top Box

Configure Rev Channel Streams for Set Top Boxes

The Channel Settings button is used to configure channel streams for current STBs in Rev. Keep in mind that you must have previously uploaded an IPTV stream in Rev using the Add URLs tab. (See: Upload a Video Through a URL Link)

▼   To configure Rev channel streams for Set Top Boxes:

1. Navigate to **Admin** > **Devices** > **Set Top Boxes.**
2. Click the **Channel Settings** button.
3. Each channel that has been previously configured will be listed. These are the channels that may be streamed to a STB through **Devices** > **Current STBs**. You may click the **Edit** icon or **Delete** icon as needed.
4. To add a new channel for use with a current STB, click the **Add Channel** button at the bottom of the form.
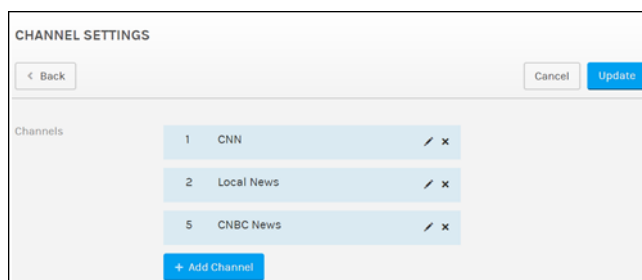
5. When the **Add Channel** form appears enter a **Channel Number** (you may not enter a duplicate) and search for previously added channels in the **Find Items** box.
6. When the channel appears that you are searching for, click the plus sign next to it and it will be added for you. As previously noted, the channel will not appear here unless you have previously set it up to do so. (See: Upload a Video through a URL Link)
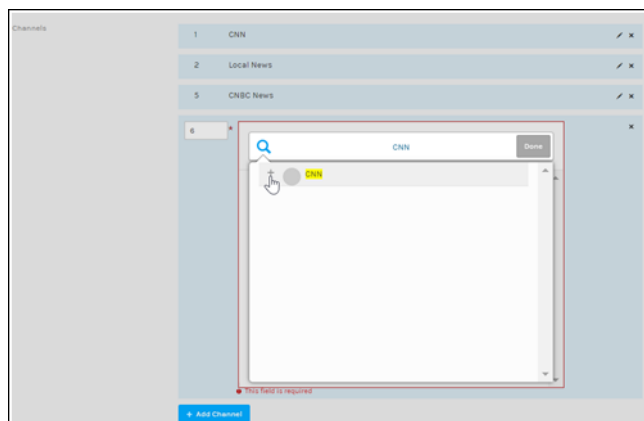
Set Top Boxes

Set a Channel Stream for a Current Set Top Box

Once a pending STB has been accepted, it will be moved to the **Current STBs** tab where you may set a previously configured channel for it to stream.
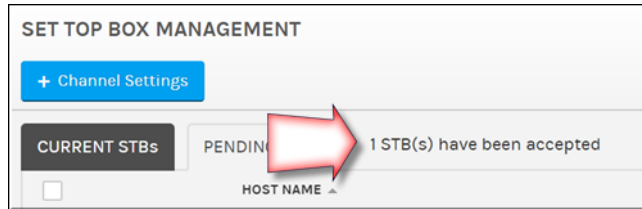
▼   To set a channel stream for a current Set Top Box:

1.   Navigate to **Admin** > **Devices** > **Set Top Boxes**

2.   Click the **Current STBs** tab

3.   Each STB that has been previously accepted will be listed.

4.   Note that in addition to the **Host Name**, **IP Address**, and **MAC Address** of the STB, also displayed is the **Status** and **Current Channel** that is streaming (if previously set).

5.   Select the checkbox to the left of the STB you want to configure.

6.   Click **Bulk Action** > **Set Channel**.

7.   The **Set Channel** dropdown box will appear at the top of the **Current STBs** tab where you can select a previously configured IPTV channel stream to play on the STB. You can also specify if closed captions should be enabled. Note that the video must have closed captions for this to function.

8. Click the **Save** or **Cancel** button to complete the configuration. The **Status** column will display the update once tuning is complete.

> **Note**: If the Connector DME does not receive updates from an STB, it will be marked offline in the Status column.
>
> The MF-STB is a 100 Base-T (100 Mbps) network connection. On 1Gbps network environments, some inexpensive, unmanaged 10/100/1000 Base-T switches (responsible for communicating with the MF-STB) introduce playback issues due to amount of buffering and flow control (specifically for converting 1000 down to 100 Base-T). If you are having playback issues, connect the MF-STB directly to a better managed switch, or investigate a good quality 100 Base-T switch to deploy between the MF-STB and your current managed switch.

Set Top Boxes

Designate a DME as a MF-STB Connector DME

Set a Channel Stream for a Current Set Top Box

Configure Rev Channel Streams for Set Top Boxes

Edit Set Top Box Credentials

Delete a Set Top Box

Set the Status of a Set Top Box

Edit Set Top Box Credentials

Once a pending STB has been accepted, it will be moved to the **Current STBs** tab where you may edit its basic information and credentials if necessary.

▼ To edit information and credentials for a current Set Top Box:

1. Navigate to **Admin** > **Devices** > **Set Top Boxes.**
2. Click the **Current STBs** tab.
3. Click the **Name** of the STB you want to edit.
4. The STB edit page will appear where you may edit the **Device Name**, **Username**, and **Password** for the STB.

> **Warning**: If you create a custom password for the STB in Rev and its control IP or Port is modified in the DME, the STB custom password will have to be re-entered again in REV. Until it is re-entered, the STB's status will appear as "Invalid Credentials".

Set Top Boxes

Designate a DME as a MF-STB Connector DME

Set a Channel Stream for a Current Set Top Box

Configure Rev Channel Streams for Set Top Boxes

Delete a Set Top Box

Set the Status of a Set Top Box

Delete a Set Top Box

One or more set top boxes may be deleted from the **Current STBs** tab through the **Bulk Actions** dropdown. If a STB is deleted from current tab, it will be placed back under the **Pending STBs** tab so that it may be used again in the future if needed.

▼   To delete one or more set top boxes:

1. Navigate to **Admin** > **Devices** > **Set Top Boxes.**
2. Click the **Current STBs** tab.
3. Click the checkbox next to the STB you want to delete.
4. Click **Delete** in the STB dropdown.
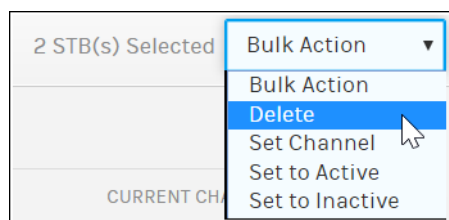
5. The selected STBs will be moved to the **Pending STBs** tab.

Set Top Boxes

Designate a DME as a MF-STB Connector DME

Set a Channel Stream for a Current Set Top Box

Configure Rev Channel Streams for Set Top Boxes

Set the Status of a Set Top Box

Set the Status of a Set Top Box

You may set the status of one or more set top boxes from the **Current STBs** tab through the **Bulk Actions** dropdown.

▼   To set the status of one or more set top boxes:

1. Navigate to **Admin** > **Devices** > **Set Top Boxes.**

2. Click the **Current STBs** tab.

3. Click the checkbox next to the STB you want to modify the status for.

4. Click **Set to Active** or **Set to Inactive** in the STB dropdown.
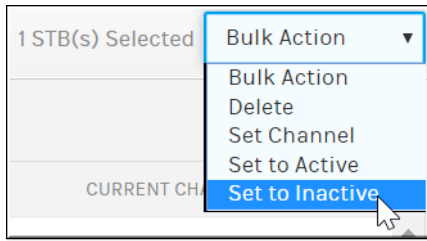
5. The status of the selected STBs will be set accordingly.

When a STB is set to Inactive:

• The current channel is blanked out and will no longer be listed for the STB

• The Status column will be set to Inactive

• Channels may not be set

Set Top Boxes

Designate a DME as a MF-STB Connector DME

Set a Channel Stream for a Current Set Top Box

Configure Rev Channel Streams for Set Top Boxes

Delete a Set Top Box

Device Maintenance

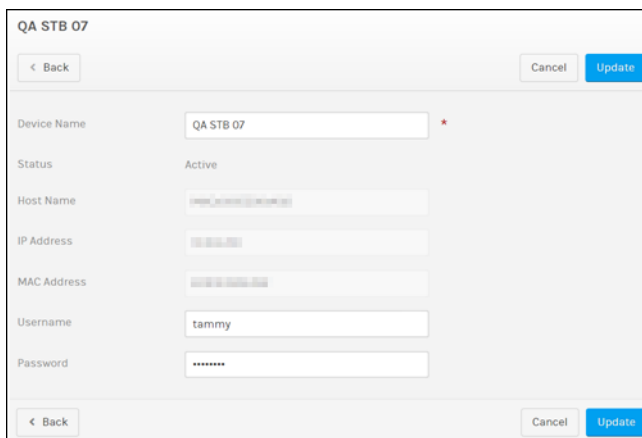## View the Status of a Device

The status of a device determines if it is available for use. After a device has been created, the system will attempt to communicate with the new device using the specified MAC address and API key associated to the device.

In order for Rev to communicate with the device and receive a heartbeat the following must be true:

• A valid **API Key** must be passed

• The device's **MAC Address** must be associated to Rev

Device status states may include:

• **Active**: Device is active in the system and sending heartbeats.

• **Inactive**: Device is inactive in the system.

• **Warning**: Device is active but has not sent a heartbeat in 45 seconds (3 heartbeat intervals).

• **Offline**: Device is active in the system, but has not send a heartbeat in 5 minutes.

▼ To view device status:

1. Navigate to **Admin** > **Devices** > **(Device) Module**.

2. The **Status** column determines whether or not a device is **Active** and available.

> **Note**: If the status of a device remains **Uninitialized** after you have added it, Rev is not detecting your device. Double check the MAC address and Rev Server URL of your device and make sure you have followed the device set up configuration steps correctly. See: Device Initial Configuration and Set Up.

View and Request Device Logs

View and Request Device Logs

Device logs begin keeping a record of events that occur for each device starting with the date the device is added to Rev. The device status is also updated based on Rev communication with the device. For example, if no heartbeat is detected and the device goes offline, this may be viewed in the device logs and the device is set to **Offline** status.

> **Note**: Device log entries are only kept for 60 days.

▼   To view a device log:

1. Navigate to **Devices > (Device) Module.**

2. Click the **View Log** link under the **Actions** column of the device.
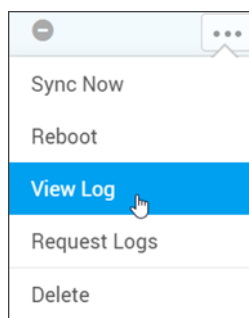
3. The **Server Log** displays.
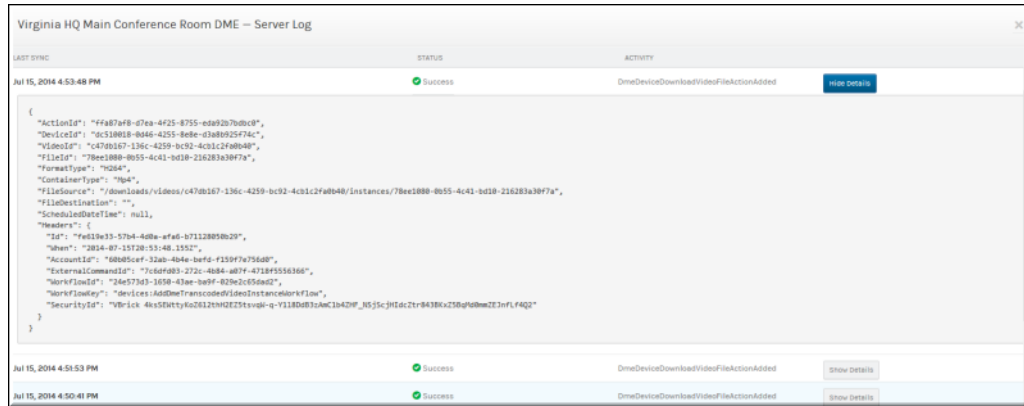
Column	Description
Last Sync	This column indicates the last time the server was synced with your system. In the case of an LDAP server, this sync interval is specified when you add your LDAP device.
Status	Indicates success or fail of the activity that occurred.
Activity	Indicates the activity itself and what occurred; the most recent activity is listed first with the date the device is added listed at the bottom of the log. Device log shows the date and time the device goes offline and back online if this occurs, for example.
Show Details	Click to see the details of the specified activity.

You can also use the **Request Logs** menu item to send device logs to Vbrick Support. You must have DME v3.24+ for this functionality.
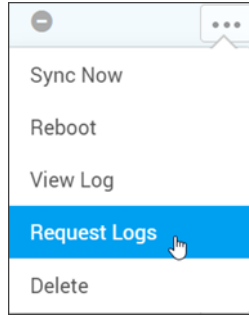
This function is used to gather all the logs for one or more DME devices (under Bulk Actions) during support calls and troubleshooting to send to Vbrick Support. Once the logs are automatically collected and sent to Support, you are notified through email and the Rev notification icon. Note this can be a labor intensive process so you should not prompt this during events.

View the Status of a Device

Edit a Device

Once a device has been added to a module, it may be edited at any time by selecting the device name under the **Name** column.

▼   To edit a device:

1.   Navigate to **Devices** > **Device Module** > **Device Name**.
2.   Make edits to applicable fields and click **Update**.

Delete a Device

You may delete a device from the **a** module by clicking the **Delete** link in the **Actions** column drop-down menu. Keep in mind that once you delete a device, you also delete the device log associated with it. You must add the device again if you intend to use it again and the log will not be restored.

▼   To delete a device:

1.   Navigate to **Devices** > **Device Module**.
2.   Click **Delete** link under the **Actions** column of the device.
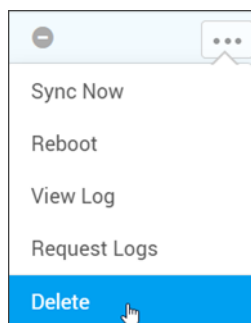
When a device is deleted:

*   Rev will be disabled under **System Configuration** > **Rev Interface** so that heartbeats will no longer be sent to the DME if the deleted device is a DME. If the DME is offline, the command will be queued.
*   Rev will be disabled under **General** > **Vbrick Rev Interface** so that heartbeats will no longer be sent to the Encoder if the deleted device is an Encoder. If the Encoder is offline, the command will be queued.
*   Note: A device may not be deleted if it is being used in a zone or presentation profile.

Role(s): Account Admin

Inactivate a Device

You may inactivate a device from the **Devices** module by editing the device and clicking the **Inactive** icon. Keep in mind that once a device is inactive it is no longer available for use and the media stored on this device is not accessible. You must activate the device again if you intend to use it and its stored content again on your video network.

▼   To inactivate a device:

1.   Navigate to **Devices** > **Device Module** > **Device Name**.

2.   Click the **Inactive** status icon.

When a device is inactive:

•   It is no longer visible in any **Presentation Profile** that has already been created.

    •   Alternative: Keep the device active but indicate it is inactive and not to be used.

•   Any **Presentation Profile** already using the device will not be usable, including any that are *only* using this device.

Role(s): Account Admin

Reboot a Device

You are able to reboot your hardware devices directly from Rev by using the reboot icon.

▼   To reboot a hardware device:

1.   Navigate to **Devices Module** > **Device Name** > **Actions**.

2.   Click the **Reboot** link under the **Actions** column of the device.
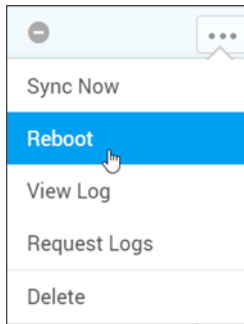
3.   Keep in mind that any one using the device will immediately be booted from the device and unable to access it until the reboot is completed.

Display Devices

The **Display** menu under **Devices** is used to view, activate, and inactivate devices and integrations that have been linked to Rev. Each display device will be described in the topics that follow in this section of Online help.

Currently, the following Display Devices are integrated with Rev:

•   **Rev for Apple TV** is an Apple TV OS application that provides the ability to view Live (Public or All Users) Rev Webcasts on Apple TVs. The application is available on the Apple TV Store and is free to download. For downloading, installation and Rev registration, please refer to the <u>Rev for Apple TV Integration Guide</u> for details. Each individual Rev for Apple TV app will be controlled by name on this page.

The **Display** module **Active** and **Inactive** tabs contain the following information:

Column	Description
Name	Device or integration name.
Version	The current version/build of the device or integration.
Unique ID	The ID of the device or integration.
Last Session	The last time the device or integration was accessed.
Actions	The actions you may perform on the device/integration. • **Edit** — Edit attributes such as status, tags, and configuration notes. See: Edit a Display Device • **View Log** — View a log of recent actions that have occurred on the device. This is good for troubleshooting if your device is not performing as expected.

Additional functionality:

Function	Description
Bulk Actions	**Delete**: Delete the selected device or integration(s). **Activate/Inactivate**: Activate or Inactivate the selected device or integration(s). See: Activate or Inactivate an Apple TV Display Device

Activate or Inactivate an Apple TV Display Device

Edit a Display Device

Activate or Inactivate an Apple TV Display Device

Display devices, regardless of the particular integration, will be in an Active or Inactive status once registered with Rev. Only those that have been moved to **Active Displays** will be able to communicate and work with Rev. Administrators can change the device status by either editing the individual display or by using the checkboxes and Bulk Actions to Activate a number of devices.

To activate or inactivate an Apple TV display device in Rev:

1. Navigate to **Devices** > **Display** from the Admin menu.
2. Click the **Inactive** tab. This tab will list all devices that have been registered in Rev, but have not been activated. These devices cannot receive streams or connect with Rev until they are activated. The **Active** tab, conversely, contains all devices that have been activated.
3. Click **Actions** > **Edit** next to the device you wish to activate or inactivate. An edit screen will come up where you can change the device status from **Inactive** to **Active**. You may also use the **Bulk Actions** drop down to change the status of several devices at once if necessary.
4. For downloading, installation and Rev registration, please refer to the Rev for Apple TV Integration Guide for complete details.

Edit a Display Device

The status of a display device (e.g., a Rev for Apple TV app seen below) as well as some metadata details may be edited within Rev. The display device may also provide the ability to locally (to the device) change configuration.

From the **Active Display** or **Inactive Display** tabs, Administrators can click on the name of the display **Device** to view the edit page. Within the **Edit** page, Administrators can change configurations and information. Some information cannot be changed, however.

To edit a display device:

1. Navigate to **Devices** > **Display** from the Admin menu.
2. Click **Actions** > **Edit** next to the device you wish to edit (you may also click the device Name). You may edit both active and inactive devices. An edit screen will appear where you can change the following device details:

a. Device status from **Inactive** to **Active**. You may also use the **Bulk Actions** drop down to change the status of several devices at once if necessary.

b. **Tags**: Administrators can add metadata tags to each individual display device. While optional at this time, these tags will be used in a future feature for filtering display devices.

c. **Configuration**: Add device-specific configuration. Please refer to the device-specific Integration Guide for details. Do not modify if in question.

Media Settings

Media Settings in Vbrick Rev determine how content is ingested, stored, categorized and ultimately viewed so that it is easily and intuitively found by your end users. You may use media settings to first determine what features are available and then specify how they work together to present, store, tag, and display content in Vbrick Rev.

As with all menu options in Rev, your level of access and visibility depends on your Account and permission settings.
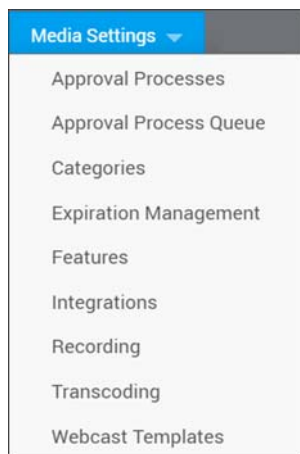
There are nine options under the **Media Settings** menu:

- **Approval Processes** — Use to create approval processes so that you can specify users and groups that must have video uploads approved before they may be viewed by other users of the system.
- **Approval Process Queue** — Provides a view of all videos that have entered an approval process and their current stage and status.
- **Categories** — Provides you the ability to create a classification system for your user's content.
- **Expiration Management** — Create content expiration rules that may be applied to uploaded videos in Rev. Rules may specify number of days before expiration or number of days without views before expiration.
- **Features** — Lets you specify which functionality to enable in Rev that deal mainly with video settings such as categories, comments, and so forth.
- **Integrations** — Access to set up and manage supported integrations with Rev.
- **Recording** — Set which order Rev chooses when selecting a recording device to use when recording content.
- **Transcoding** — Where transcoding presets are defined in your system and the encoding outputs you may produce.
- **Webcast Templates** — Rename, set a default, and delete Webcast Event templates in Rev.

Approval Processes

The **Approval Processes** menu displays each approval process that has been created and allows you to create a new approval process. An approval process in Rev will let you specify select groups and users that must have content approved before it may be viewed by other users of the system. You may create a simple, single layer approval process or a multi-step process with different stages and approvers depending upon the needs of your organization.
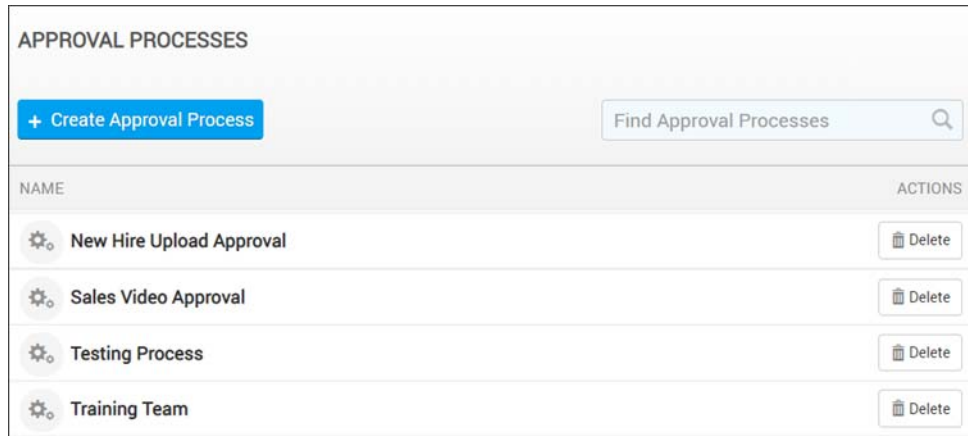
The **Approval Processes** module displays:

Column	Description
Name	The **Approval Process** name. Click to edit the attributes.
Actions	The actions you may perform on an approval process. • **Delete** — When an approval process is deleted, the groups and user accounts associated to it are not deleted; only the association itself.

Additional functionality:

Function	Description
Create Approval Process	Creates a new approval process by taking you to the **New Approval Process** page where you may add groups and users to require approval and new approvers.
Find Approval Process	Search for a specific approval process if you have several created.

Create or Edit an Approval Process

Submit a Video for Approval

Approve or Reject a Video Submitted for Approval

Create or Edit an Approval Process

Rev allows Admin users to create a content **Approval Process** so that specific users or groups must obtain approval before their uploads may be viewed. Further, the approvers that are set

in the approval process may also be user accounts or groups. Only Account Admins and Media Admins are able to create an approval process.

For example, all training materials may need to be approved by a subject matter expert to ensure that information in a video is correct before uploading; or new employees may be placed in a New Hire group with experienced users set as approvers in a New Hire approval process. All uploads created by this group would then be subject to approval by the experienced users and video status will be set to Pending Approval. When the employee is deemed experienced enough, he/she may be removed from this group and no longer subject to approval for uploading.

Additionally, the approval process may be a multi-step approach if different organizational groups need to be involved. For example, you may decide that a video needs to go through both the Sales team and Human Resources before it is approved for public consumption (made Active).

▼   To create or edit an approval process:

1.   Navigate to **Admin** > **Media Settings** > **Approval Processes**.

2.   Click the **Create Approval Process** button. Click a previously created process to edit its attributes.

3.   Enter an **Approval Process Name**.

4.   Specify the users or groups that will require approval. Click the **Find Items...** search box under the **Groups/Users Requiring Approval** section. Begin typing either the user account or groups you want to add and Rev will search the system and complete your entry.

> **Note**: The Rev search engine works similar to popular Web search engines in that using double quotes around your search will narrow it and result in more accurate results if you are looking for a specific user or item.
>
> For example, if you are searching *only* for one specific video, user account, event, etc., enclosing the search in double quotes avoids returns of similar terms or derived words in your search results.
>
> Note that this is also true when using **Find Items** search within the Rev user interface to search for user accounts.

5.   Click **Done** to complete your entry. Notice the image below has a group and one individual user account that will need video upload approval in this approval process.
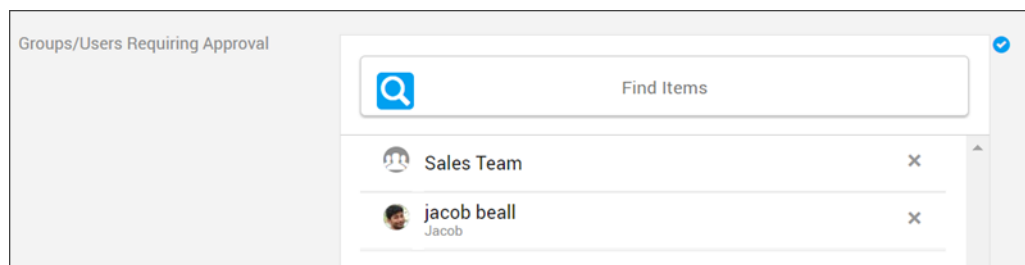
6.   Next, specify the user accounts or groups that may approve content as part of this approval process. You may specify one step or several approval stages involving multiple groups or people.

7.   Enter an **Approvers Step Name**. Every step is required to have a step name.
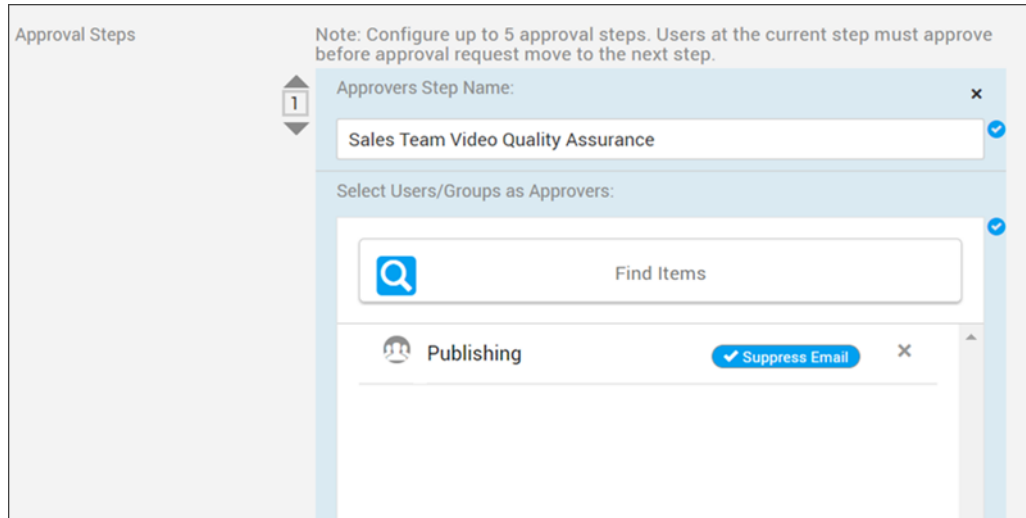
8. Click the **Find Items...** search box under the **Approval Steps** section. Begin typing either the user account or group you want to add and Rev will search the system and complete the entry for you to click on and add.

9. If the **Suppress Email** control is checked next to the Approver, that entry will not receive pending approval emails. Rejection emails will still be sent. This function may be set at all approval stages.

10. Click **Done** to complete your entry. Notice the image below has a group added that will *not* be notified when content has been submitted for approval.

> **Note**: Approvers are required to approve or reject the submitted content before it may be viewed by other users. If more than one approver is designated, only one approver needs to approve the content.
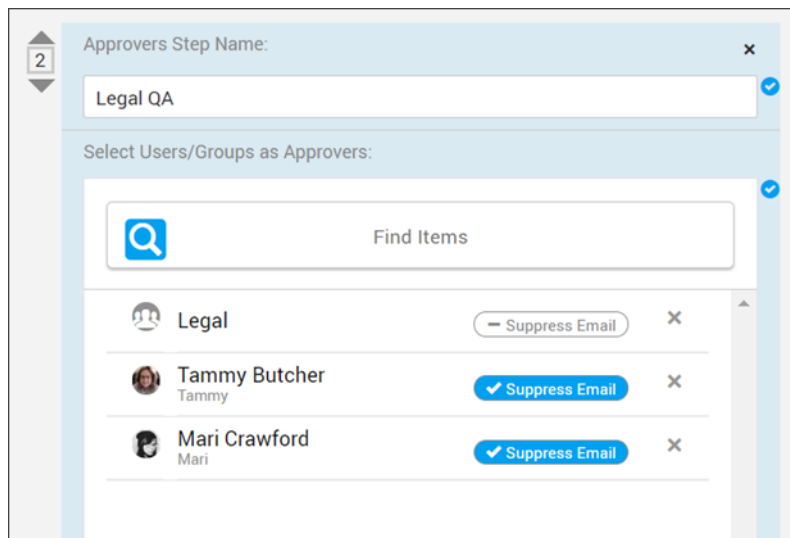
11. Click the **Add Approvers** button at the bottom of the form to add additional approval steps. You may create up to 5 approval steps in an approval process. A video upload will be required to pass all stages before it will be visible.

12. Click **Create Approval Process** to create the new process or **Save Approval Process** if you are editing an existing process.

Role(s): Create Approval Process: Account Admin, Media Admin

Submit a Video for Approval

Approve or Reject a Video Submitted for Approval

Approve or Reject a Video Submitted for Approval

If you have been designated as an Approver in a Rev Approval Process or Approval Step, each time a video is submitted for approval, you will receive an email that informs you the video is ready for review. A URL will be enclosed with the email that will allow you to navigate directly to the video that is Pending Approval.

A **Pending Approval** button will also be visible under each **Media** menu option so that you may always access those videos that have been submitted for approval. Each time a new video has been submitted, the button will also display a numerical value indicating the number of videos in your approval queue that are currently waiting approval.
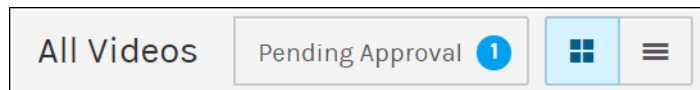
▼   To approve or reject a video submitted for approval:

1. Navigate to the **User** > **Media** > **Videos** >**Pending Approval** tab. (Or click the URL in the email you receive to access to a specific video directly.)

2. Select the video that needs approval.

3. Review **Video Settings** as needed.

4. Click the **Approve** or **Reject** button on the **Video Player** page as required. Approve is selected by default.

5. Notice that if one or more Approval Stages have been set up, the stage will be noted. In the example below, this is the first step of the approval process. The video will need to pass through two more stages of approval before it will be visible. You can check the Approval Queue and what status each video is in by checking **Media Settings** > **Approval Process Queue**.
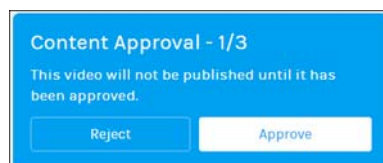
6. Enter an approval (or rejection) message, if desired. This message will be emailed to the uploader/submitter of the video so that it may be corrected and resubmitted if rejected.

VIDEO REJECTED

Please make sure you add this video to the Training collection and category. You should probably update the description to mention it is part of the Corporate Orientation series as well. Thanks.

Cancel   OK
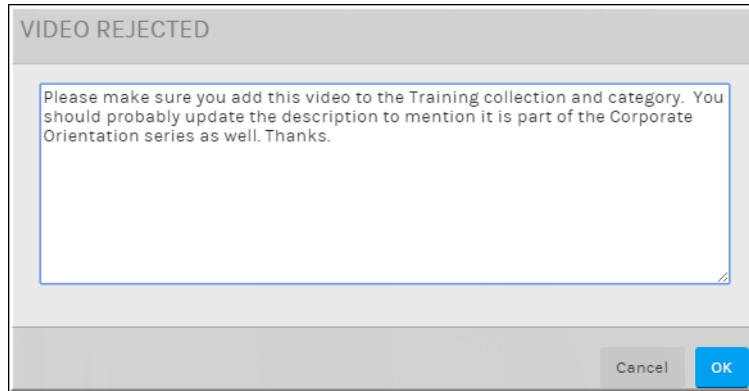
7. If a video is rejected, it must be resubmitted and approved before it may move to the next Approval Step (if there is more than one step).

8. Click **OK**. If approved, the video will be set to **Active** status and will be viewable by other users of the system.

9. If rejected, status will be set to **Rejected** and the submitter will be able to view the video under the **My Videos** tab to make the suggested updates before resubmitting for approval.

10. Account and Media admins are able to view all rejected videos when viewing **Inactive** status videos.

11. Account and Media admins are able to approve/reject on behalf of an approver if needed. This prevents an approver from going on vacation and leaving a video in Pending Approval status.

> **Role(s)**:
> • Create Approval Process: Account Admin, Media Admin
> • Approve Uploads: Approvers, Account Admin, Media Admin on behalf of Approvers

Create or Edit an Approval Process

Submit a Video for Approval

Approval Process Queue

Approval Process Queue

The **Approval Process Queue** menu provides an overview of all videos that are currently in an approval process stage. It displays the following information about each video:

• Title
• Uploader (that submitted the video for approval)
• Approval Process Name
• Date and Time of [last] Status Change
• Status (Pending or Rejected)
• Approval Process Stage (if a multi-step process)

This queue will easily allow you to keep track of content that is involved in approval processes that have many stages and each video's status in the process.

Create or Edit an Approval Process

Approve or Reject a Video Submitted for Approval

Submit a Video for Approval

Categories

Use the **Categories** menu to create a content classification system for your user's content.

The **Categories** menu displays:

Column	Description
Category Name	The name of the category. Click to edit a category. Drag to rearrange a category. Click the (+) icon to view any subcategories.
Items	The number of items (media) that have been assigned to a category.
Actions	The actions you may perform on a **Category**. • **Delete** — When a category is deleted, the content associated to it is not deleted; only the association itself. Deleting a category will also delete all subcategories associated with the category.

Additional functionality:

Function	Description
Create Category	Creates a new category.
Add Child	Adds a subcategory to the category.

Allow Categories on All Media

Add or Delete a Category or Subcategory from a Video

Create or Edit a Category or Subcategory

Categories and subcategories are used to create a classification system for your user's content. Users will only see a category if they have access to at least one video in it. Only Account Admins and Media Admins may create and edit categories in Rev.

▼   To add or edit a category or subcategory:

1.   Navigate to **Admin** > **Media Settings** > **Categories**.
2.   Enter a **Category Name** and click **Create**.
3.   Click the **Add Child** button next to a **Category Name** to add a subcategory to the category.
4.   Keep in mind each category and subcategory name must be unique within each category hierarchy.

> **Tip**: Click a **Category Name** to edit a previously saved category. You may click and drag subcategories to arrange them under parent categories. They are automatically saved in their new position alphabetically.
>
> To add a video to a category, edit the **Video Settings**.

Allow Categories on All Media

Add or Delete a Category or Subcategory from a Video

Bulk Editing Video Categories

Video Settings

Delete a Category or Subcategory

Only Account Admins and Media Admins may delete categories and subcategories in Rev.

▼   To delete a category or subcategory:

1.   Navigate to **Admin** > **Media Settings** > **Categories**.
2.   Click the **Delete** button next to the category or subcategory you want to delete.
3.   Deleting a category will also delete all its subcategories.
4.   Videos associated with deleted categories and subcategories will be disassociated but not deleted.

Allow Categories on All Media

Add or Delete a Category or Subcategory from a Video

Bulk Editing Video Categories

Video Settings

Expiration Management

The **Expiration Management** menu displays expiration rules for video uploads that have been created and allows you to define new expiration parameters for video uploads.

Note: **Expiration Management** must be enabled in **Features** before you may use this feature. See: Enable Expiration Rules for Video Uploads.

Expiration rules may be based on specific dates or how many times a video has been viewed. A default rule may be set for all video uploads in Rev as well.

The **Expiration Management** module displays:

Column	Description
Default	Allows you to set a default expiration rule. Only one default rule may be set at a time. You may also deselect all rules so that no default is set. If a default rule is set, new uploads will automatically be set to expire based on that rule.
Name	The **Expiration Management** rule name. Click to edit the name.
Rule Type / Days	The types of rule you may create. • **Number of Days Before Expiry:** Must be greater than zero. The video will be visible for the number of days in the **Days** column and then be expired and set to either **Inactive** or **Deleted**. • **Number of Days without Views:** Must be greater than zero. The number of days in the **Days** column the video may go without being viewed (or partially viewed) before it will be expired and set to either **Inactive** or **Deleted.** • The video uploader will be emailed 7 days prior to video expiration and again upon the actual expiration no matter which rule is created.
Delete Upon Expiry	Specifies that, if selected, content will be deleted upon expiration.
Delete (x)	Deletes the expiration rule. If you delete an expiration rule, videos that have been set to expire under that rule will no longer expire.

Additional functionality:

Function	Description
Add Expiry Rule	Creates a new expiry rule at the bottom of the form.
Cancel	Cancels any unsaved changes you have made and reverts the form to the previously saved version.
Save Changes	Saves all changes. Once saved, expiration rules may not be modified. If you need to change a rule setting, you will need to re-create the rule and add the videos again (through bulk editing if you have added several videos).

Add or Edit a Content Expiration Rule

Rev allows admin users to create a content **Expiry Rule** so that specific videos may be set to **Inactive** or **Deleted** entirely from the system on specific dates or if they have not been viewed after a certain amount of days.

For example, you could create an Expiry Rule to set a video to Inactive status if it has not been viewed in 365 days. Or, you could create a rule to make sure all Human Resource videos are set to expire after 5 days.

▼   To create or edit an expiry rule:

1.   Navigate to **Admin** > **Media Settings** > **Expiration Management**.

2.   Click the **Add Expiry Rule** button. A new rule will appear at the bottom of the list.

3.   Enter an **Expiry Rule Name**. Click a previously created rule to edit the attributes.

> **Caution**: You may only edit the name, default, and deletion status of a previously created rule. If you want to edit the type and days attributes, you must create a new rule with the attribute settings you want and add your videos again. You may do this through the bulk edit status feature if you have several videos to add. Then delete your old rule.

4.   Specify if the rule is to be **Number of Days Before Expiry** or **Number of Days without Views**. **Number of Days Before Expiry** will keep the video visible by the number you enter in the **Days** field and then expire (or delete) the content on the next day.

     If you specify **Number of Days without View**, the video will expire (or delete) if it has not been viewed (or partially viewed) by the number in the **Days** field.

     The video uploader will be emailed 7 days prior to video expiration and again upon the actual expiration no matter which rule is created.

5.   Check the **Delete Upon Expiry** checkbox if you want the video to be deleted when it expires. Otherwise, it will be set to Inactive.

6.   Click the **Default** checkbox to make the rule the default rule that is selected automatically when a video is uploaded. Only one rule may be a default rule at a time. you may also deselect all rules so that no default rule is set.

7.   Click the **Delete (x)** icon to delete the rule. If a rule is deleted, the content associated with it will no longer expire.

> **Tip**: If a default rule is set, that rule will be automatically selected when a new video is uploaded. However, Account Admin and Media Contributor roles may override the rule or select a different expiration method if desired.

Set an Expiration Date or Rule for a Video

Features

The **Features** menu displays the media features and additional video functions available to enable or disable in Rev. Use the checkboxes available to enable or disable a specific setting.

Allow Categories on All Media

Categories provide a means for you to logically group content that is similar. Only Account Admins and Media Admins are able to enable and disable categories.

▼   To enable categories:

1.   Navigate to **Admin** > **Media Settings** > **Features**.
2.   Select the **Allow categories on all media** checkbox.

Keep in mind:
*   Categories may have sub-categories.
*   Category names *must* be unique within an account.
*   Category names have a maximum of 100 characters and a minimum of 1 character.
*   When deleting a category, content assigned to that category is not deleted; only the association to the category itself is removed.

When categories are *disabled*:
*   A category will not be able to be selected when media is uploaded.
*   Category details will not be displayed on any video page.
*   Category filter options are removed from video search pages.
*   Category Management will no longer be available for admins.
*   The option to **Bulk Edit** categories will no longer be available.
*   If categories are disabled after a category has already been used, the category will not be deleted from the database. However, its display will be discontinued as noted above. (video pages, upload pages, search fields, etc.)

Create or Edit a Category or Subcategory

Allow Tags on All Media

Tags provide a means for your users to provide their own classification system. This feature is enabled by default. Only Account Admins and Media Admins are able to enable and disable tags.

▼   To enable tags:

1.   Navigate to **Admin** > **Media Settings** > **Features**.
2.   Select **Allow tags on all media** checkbox.

When tags are *disabled*:
•   A tag will not be able to be entered when media is uploaded.
•   Tags will not be displayed on any video page.
•   Tag filter options are removed from video search pages.
•   The ability to **Bulk Edit** tags will not be available.
•   If tags are disabled after a tag has already been used, the tag will not be deleted from the database. However, its display will be discontinued as noted above. (video pages, upload pages, search fields, etc.)

Allow Comments on All Media

Comments provide a means for your users to leave interactive feedback on content that has been added to the system. Only Account Admins and Media Admins are able to enable and disable comments.

▼   To enable comments:

1.   Navigate to **Admin** > **Media Settings** > **Features**.
2.   Select **Allow comments on all media** checkbox.

Keep in mind:
•   The Comment field allows a maximum of 1000 characters.
•   Each comment will have the **User's Name** and **Date** noted.
•   When a user leaves a comment, the video owner will receive an email notification of the comment noting the commenter's name, date and time of the comment, and the comment itself along with a link to it.

- Other users may reply to the original comment to create nested comments.
  - Only one level of nested comments will be created.
  - Replies on the second level of comments will be a reply to the original comment.
  - Email notifications are included for nested comments.
- Users may delete their own comments.
- Account Admins and Media Admins may also delete comments.
- If a comment is deleted, it is replaced with placeholder text: "*This comment has been removed*.".
- Once comments have been enabled globally, the **Enable Comments** checkbox appears on the **Video Settings** page which will allow comments to be enabled or disabled for specific videos.
- If this setting is disabled, the **Enable Comments** checkbox will no longer appear on individual videos nor will it appear in the **Bulk Edit** interface.

Comment on a Video

Enable or Disable Comments for an Individual Video

Bulk Editing Video Comments Setting

Allow Ratings on All Media

Ratings provide a means for your users to provide additional feedback on content by using a star-based ranking system. Users can use this feedback if they do not want to leave a comment (or in addition to comments). This feature is enabled by default. Only Account Admins and Media Admins are able to enable and disable ratings.

▼   To enable ratings:

1. Navigate to **Admin** > **Media Settings** > **Features**.
2. Select **Allow ratings on all media** checkbox.

Keep in mind:

- If disabled, there will be no ratings feature on *any* content (either input or display).
- The ability to **Bulk Edit** the ratings feature will no longer be available.
- If ratings are disabled after they have already been submitted, ratings data will not be deleted. If enabled again in the future, existing ratings will once again become visible for the content.
- If ratings are enabled globally, the **Enable Ratings** check box appears on the **Video Settings** page which will allow ratings to be enabled or disabled for specific videos.

Rev Video Player Features

Enable or Disable Ratings for an Individual Video

Allow Downloads on All Media

If downloads are globally enabled, the **Video Settings** page will display an **Enable Downloads** checkbox so that each individual video may then be enabled for download by users to a PC using the **Download** button on the **Video Basic Information** panel flyout. The **Bulk Edit** interface will also feature the ability to modify download enabling/disabling on videos in bulk through a **Downloads** dropdown. This feature is enabled by default. Only Account Admins and Media Admins are able to enable and disable downloads.

▼   To enable downloads:

1.   Navigate to **Admin** > **Media Settings** > **Features**.
2.   Select **Allow download option on all media** checkbox.

When downloads are globally *disabled*:

- There will be no **Enable Downloads** checkbox on any **Video Settings** page.
- This means that there will be no **Download** button on any **Video Basic Information** panel flyout.
- There will be no **Downloads** dropdown on the **Bulk Edit** interface.
- This also means that when users are editing video that video backups of the original may not be made first which is generally advised. You may enable this ability separately however.
- If downloads are globally disabled after they have already been previously enabled, the **Download** button will be removed and the video will no longer be available for download. If globally enabled again in the future, the video will once again be available for download so long as the **Enable Downloads** checkbox on the individual video has not been modified/deselected.

When downloads are globally *enabled*:

- There will be an **Enable Downloads** checkbox on any **Video Settings** page.
- There will be a **Download** button on the **Video Basic Information** panel flyout if the **Enable Downloads** checkbox is selected *and* if the user is accessing the page from a PC. This checkbox is disabled by default.
- There will be a **Downloads** dropdown on the **Bulk Edit** interface.
- When a user selects to download an enabled video, it will download from the DME that they have been directed to for watching the video.
- If there is an .mp4 file available, the user will be provided the .mp4 file.
- If no .mp4 file is available, the user is provided the first non-HLS/HDS file available.
- The user will never be able to download an HLS or HDS file.
- If the video is a Webcast recording with PowerPoint slides, only the video is provided.

Download an Individual Video

Allow Downloads for Video Backup

Bulk Editing Video Downloads Setting

Allow Downloads for Video Backup

This setting is generally used in concert with the **Allow Downloads on All Media Setting** so that backups may still be allowed when editing video if downloads have been disabled globally. It is recommended that an orignal copy of a video be downloaded before editing. For those organizations with security compliance policies in place that prevent downloads, this setting may be used to allow Account and Media Admin accounts the ability to download videos for backup before editing while all other accounts are still prevented from downloading.

▼ To enable downloads for video backup:

1. Navigate to **Admin** > **Media Settings** > **Features**.
2. Select **Allow download from the video editor for backup** checkbox.

When video backup downloads are globally *disabled*:

*   There will be no **Enable Downloads** checkbox on any **Video Settings** page.
*   There will be no **Download** button on the **Video Basic Information** panel flyout.
*   There will be no **Downloads** dropdown on the **Bulk Edit** interface.
*   Video backups may not be made when editing videos.
*   The exception to this are Account and Media Admins who will still receive the message that they may make a download backup of an original video when editing.

When video backup downloads are globally *enabled*:

*   All accounts with edit permissions will be able to download a backup of an original video before editing.

Download an Individual Video

Allow Downloads on All Media

Bulk Editing Video Downloads Setting

Enable Video Embed Code

Video embedding must be enabled if you want to provide access to the embed code that may then be placed on a 3rd party Website or portal so that your viewers are not required to use the Vbrick Rev portal to view your videos. This feature is enabled by default. Only Account Admins and Media Admins are able to enable and disable embedding.

▼ To enable access to embed code:

1. Navigate to **Admin** > **Media Settings** > **Features**.
2. Select **Allow access to embed code on all media** checkbox. This provides access to each video's embed code on the **Sharing** > **Embed** tab.
3. Select the **Autoplay enabled by default** checkbox if you want the embedded video's code to have autoplay applied. This may be modified by the user.

> **Note:** If your videos and playlists are set to autoplay, be aware that they will started muted. This also applies to Webcasts.

When embed code is *disabled*:

- The **Embed** tab is no longer available.
- If a video has been embedded and the functionality is disabled, users accessing the embedded video are displayed a message that indicates embedded playback is no longer available.

Embed a Video

Enable Private Video Metadata Sharing

Enable Add Video via URL Option

When adding video to Rev, you are able to upload it from your hard drive. If you have the **Enable Add URLs** option enabled, you are also able to link to URLs to display video. This feature is enabled by default. Only Account Admins and Media Admins are able to enable and disable this feature.

▼ To enable Add URLs:

1. Navigate to **Admin** > **Media Settings** > **Features**.
2. Select **Allow videos to be added via URLs** checkbox. This adds the **Add URLs** tab on the **Add Content** button on the top menu bar.

When Add URLs is *disabled*:

- The **Add URLs** tab is no longer available.
- If a **Live Video** carousel has been configured on the **Home Page**, it will be removed and the **Live Video** configuration will no longer be available as an option for **Home Page** configuration in the future.
- Any videos uploaded prior to clearing the **Allow videos to be added via URLs** checkbox will still appear under **Recent Videos** and will still be present in Rev. Users with admin access may delete these videos if desired.

Upload a Video through a URL Link

Customize the Home Page Template and Carousels

Enable Playback During Transcoding

When adding video to Rev, you are able to view the original video during transcoding if you have the **Enable Playback During Transcoding** option enabled. This feature is enabled by default. Only Account Admins and Media Admins are able to disable this feature.

▼ To enable and disable playback during transcoding:

1. Navigate to **Admin** > **Media Settings** > **Features**.

2. Select **Allow playback of the original video during transcoding for supported formats** checkbox.

3. Original videos in supported Rev formats are immediately playable even if transcoding is taking place.

4. Note that when the video is playable, a thumbnail is generated even if it is still transcoding.

When this feature is *disabled*:

*   A status message is displayed as recording, uploading, processing, etc., until the video has finished transcoding and is ready to play.

*   When the video has finished transcoding, the user will be notified via the Notifications tray and through email.

*   When the video is playable, a thumbnail is generated even if it is still transcoding.

Enable Prepositioning of Individual Videos

You may want to preposition important content immediately instead of waiting for defined time frames on the DME to occur. If you have the **Enable Prepositioning of Individual Videos** option enabled, you will enable an additional table in **Video Settings** titled **Preposition**. Only Account Admins and Media Admins are able to enable and disable this feature and use the **Preposition** tab once enabled.

▼   To enable prepositioning of individual videos:

1. Navigate to **Admin** > **Media Settings** > **Features**.

2. Select **Enable Prepositioning of Individual Videos** checkbox. This adds a **Preposition** tab in **Video Settings**.

3. The video must be finished processing before this will occur.

When Enable Prepositioning of Individual Videos is *enabled*:

*   The **Preposition** tab is visible to Media and Account Admins but not Media Contributors.

*   This tab can be used to set a date and time to preposition the individual video to all DMEs that have VOD playback set to true.

*   Even those DMEs not marked to preposition content will receive the video at the date and time specified so long as VOD playback is set to true.

*   If other uploads are in progress, the prepositioned individual video will be prioritized.

Designate a DME Video Playback Device

Preposition DME Content

Preposition an Individual Video

Enable Expiration Rules for Video Uploads

The **Enable Expiration Rules** option is used to enable the **Expiration Management** interface and features for video uploads in Rev. Once enabled, expiration rules for video uploads may

be defined by date or views. Additionally, a default rule may be set for all uploads as well. This setting is enabled by default. Only Account Admins and Media Admins are able to enable and disable this setting.

> **Note**: Expiration dates will always be available for video uploads. This topic only refers to enabling expiration rules.

▼ To enable the expiration management interface for video uploads:

1. Navigate to **Admin** > **Media Settings** > **Features**.
2. Select the **Allow videos to expire based on rules** checkbox.
3. This will enable the **Admin** > **Media Settings** > **Expiration Management** interface so that expiration rules may be defined for video uploads.
4. Once expiration rules have been defined, they may be selected under <u>Video Settings</u> for each video upload.

<u>Set an Expiration Date or Rule for a Video</u>

Enable Supplemental Content Option

You are able to attach a supplemental file to a video in Rev from your hard drive if you have the **Enable Supplemental Content** option enabled. This feature is enabled by default. Only Account Admins and Media Admins are able to enable and disable this feature.

▼ To enable Supplemental Content:

1. Navigate to **Admin** > **Media Settings** > **Features**.
2. Select **Allow supplemental content on all media** checkbox. This adds the **Add Files** button on the **Advanced** tab in Video Settings.
3. File types you may include with the video include: PowerPoint presentations (.ppt, .pptx), Word documents (.doc, .docx), Excel documents (.xls, .xlsx, .csv), PDFs, Zip files (.zip, .rar, .7z), Text files (.txt), Images (.jpg, .png, .gif).

When Enable Supplemental Content is *disabled*:

- The **Add Files** button is no longer available.
- Any files attached prior to disabling the **Enable SupplmentaI Content** checkbox will not be deleted. They will reappear with their associated video if the checkbox is re-enabled.

<u>Attach a Supplemental File to a Video</u>

Enable 360 Video Upload

If you have the **Enable 360 Video** option checked, users will be able to upload and view 360-degree videos in Rev. This feature is enabled by default. Only Account Admins and Media Admins are able to enable and disable this feature.

▼ To enable 360 Video:

1. Navigate to **Admin** > **Media Settings** > **Features**.

2. Select **Allow uploading of 360 videos** checkbox. This adds the **360 video** checkbox on the **Upload Files** when adding a new video to Rev.

3. Transcoding presets have been created for the support of 360 videos and will be applied automatically.

> **Warning:** 360 video file sizes, particularly those that are 4k video, can be *very* large. This should be taken into consideration for account management usage when viewing and managing 360 videos.

When 360 video is *disabled*:

• The **360 video** checkbox is no longer available when uploading video.

• Any files uploaded *prior* to disabling the **Enable 360 video** checkbox will not be deleted or hidden.

Upload a Video from Your Hard Drive

Enable Zone Fallback for VOD Streams

If you have the **Allow zone fallback for VOD streams** option checked, zone logic fallback and hierarchies are enabled in Rev. This option is enabled by default. Only Account Admins and Media Admins are able to enable and disable this feature.

▼ To enable fallback and zone logic for VOD streams:

1. Navigate to **Admin** > **Media Settings** > **Features**.

2. Select **Allow zone fallback for VOD streams** checkbox. This adds failover and zone hierarchy logic to Rev for VOD streaming video.

> **Caution:** If this option is disabled, zone logic will only return the playback URL of the DMEs in the user's matched zone and zone logic will *not* return a playback URL from Rev.
>
> Further, if there is no matching URL, then the user will be displayed the following message: "Playback of this video is not available at this time. Please try again later."

When zone fallback logic is *disabled*:

• As noted, zone logic will now only return the playback URL of the DMEs in the user's matched zone.

• Default zone is also ignored. So if you have DMEs only in the default zone, then no Playback URLs are returned and a "Playback of this video is not currently supported in this browser" message is displayed.

• Zone logic will not return a playback URL from Rev as noted.

• Downloads - When there are *no* playback URLs (i.e when no zones match) there are no download URLs as well.

- Downloads - When there *are* playback URLs (i.e when a zone matches but the video is not yet available on the DME) the video downloads from REV until it is ready on the DME. Then it downloads from DME.

Zone Logic and Hierarchy

Enable Flash Playback

If you have the **Allow flash playback** option checked, the Rev player will play all Flash streams encountered. This option is enabled by default. Only Account Admins and Media Admins are able to enable and disable this feature.

▼   To enable flash playback:

1. Navigate to **Admin** > **Media Settings** > **Features**.
2. Select **Allow flash playback** checkbox.

When flash playback is *disabled*:

- Rev will exclude all flash playback URLs (RTMP, Flash multicast, FLV).
- If transcoding is turned off, FLV uploads and downloads are still allowed.

Enable Unlisted Videos

If you have the **Allow Videos to be Hidden from the Rev Interface and Search** option checked, the video is hidden from anyone who does not have edit rights within the Rev UI. The video may be played when accessed directly via embed code or direct link. Unlisted videos may also be manipulated through Rev APIs. This option is disabled by default. Only Account Admins and Media Admins are able to enable and disable this feature.

▼   To enable Unlisted videos:

1. Navigate to **Admin** > **Media Settings** > **Features**.
2. Select **Allow Videos to be Hidden from the Rev Interface and Search** checkbox.

When Unlisted videos is *enabled* and a VOD or Live Stream is unlisted, the videos are hidden from anyone who does not have edit rights to the video; the video is not searchable/viewable in:

- All Videos view
- Browse Categories view
- Dashboard carousels including the Featured Video carousel
- Channels page
- Playlist views
- Global Search

Unlist a Video

Edit Webcast Settings During an Event

Bulk Editing the Unlisted Video Setting

Allow Chat on Webcasts

If you have the **Allow Chat on Webcasts** option checked, the **Enable Chat** toggle becomes available in the **Attendee Engagement** section during Event setup. This allows Event Admins and Hosts to decide whether or not they want Rev's Chat feature for attendees enabled on their Webcast events.

▼   To add Chat functionality during Webcast setup:

1.   Navigate to **Admin** > **Media Settings** > **Features**.

2.   Select **Allow Chat on Webcasts** checkbox in the **Webcast User Engagement** section.

When **Allow Chat on Webcasts** is *enabled*, the **Enable Chat** toggle becomes available in the **Attendee Engagement** section when creating an event. This adds the Chat functionality for attendees during an Event Webcast.

Schedule a Webcast Event

Enable Chat for a Webcast Event

Allow Polls on Webcasts

If you have the **Allow Polls on Webcasts** option checked, the **Enable Polls** toggle becomes available in the **Attendee Engagement** section during Event setup. This allows Event Admins and Hosts to decide whether or not they want to add one or more Polls to their Webcast events for attendees to view and answer.

▼   To add Poll functionality during Webcast setup:

1.   Navigate to **Admin** > **Media Settings** > **Features**.

2.   Select **Allow Polls on Webcasts** checkbox in the **Webcast User Engagement** section.

When **Allow Polls on Webcasts** is *enabled*, the **Enable Polls** toggle becomes available in the **Attendee Engagement** section when creating an event. This adds the Poll functionality during Event setup.

Schedule a Webcast Event

Add a Poll to a Webcast Event

Allow Q&A on Webcasts

If you have the **Allow Q&A on Webcasts** option checked, the **Enable Q&A** toggle becomes available in the **Attendee Engagement** section during Event setup. This allows Event Admins and Hosts to decide whether or not they want Rev's Q&A features available for attendees available on their Webcast events.

▼   To add Q&A functionality during Webcast setup:

1.   Navigate to **Admin** > **Media Settings** > **Features**.
2.   Select **Allow Q&A on Webcasts** checkbox in the **Webcast User Engagement** section.

When **Allow Q&A on Webcasts** is *enabled*, the **Enable Q&A** toggle becomes available in the **Attendee Engagement** section when creating an event. This adds the Q&A functionality during Event Webcast setup.

Schedule a Webcast Event

Enable Q&A for a Webcast Event

Add a Slide Delay for a Webcast Event Live Video

Account or Media Admins can use the **Slide Delay** feature to further sync presentation slide transitions to ensure that live Webcast video presentations are seamless. This feature *only* applies to HLS video streaming live on Webcasts and is an account level setting in that it will affect all Webcasts. You may override this setting at the zone level by specifying a different delay.

▼   To set a slide delay for presentation slides:

1.   Navigate to **Admin** > **Media Settings** > **Features**.
2.   Select the **Manual** option for **Slide Delay for HLS Live Video** in the **Slide Delay** section.
3.   Enter the **Delay in Seconds**. The default is 24 seconds. This is the number of seconds that will occur between each slide transition.

Keep in mind:
•   This feature is disabled by default which means the slides transition in real time.
•   If the video is stopped, slides will also transition in real time.
•   If a user has control, slides will transition in real time.
•   If an HLS failover occurs, the automated delay in seconds will occur.
•   You may override this setting in zone settings.

Control a Presentation During a Webcast Broadcast

Edit Presentation Slide Title and Timing for a Recorded Webcast Event

Edit Video Settings of a Recorded Webcast Event

Add a Zone

Configure a Rebuffering Threshold for Webcast Events

This setting is used to configure a rebuffering threshold for Webcast Events and is normally set by Vbrick. Please consult with Vbrick Support/Operations before modifying this value to avoid any adverse effects.

▼   To set a rebuffering threshold:

1.   Navigate to **Admin** > **Media Settings** > **Features**.

2.   Set a value between 0 and 5000 in the **Experienced Rebuffering Threshold (milliseconds)** field in the **Experienced Rebuffering Threshold** section.

3.   The default value is 500.

Keep in mind:

- Any buffering event that exceeds this threshold may be viewed on the Real Time Dashboard under the System Status tab. See: View Number of Multicast Error Events

- Buffering events that are less than the configured threshold are not counted.

- It does not matter whether that buffering happens at the start of playback or in the middle.

Real Time Webcast Event Analytics Dashboard

View Number of Multicast Error Events

Recording

Use the **Recording** menu to designate the DME order that Rev will use when recording content. You are able to designate a primary and secondary DME device in this manner.

> **Note**: To record content and event Webcasts in Vbrick Rev, you must add a DME device. Once added, use **Monitor > Recording Status** in the DME Admin menu to verify ongoing status updates of DME recordings.

> **Note**: An RTSP unicast stream is required for recording live Webcasts in Rev. Make sure that your stream has a keyframe interval between 2 to 5 seconds and do not use B-frames. Please see your individual encoder (stream source) documentation for setting information.

Record a Webcast Event

Add a Distributed Media Engine (DME)

Set a Primary and Secondary DME

Use the **Recording** module to designate your primary DME and your secondary DME for desired recording preference that Rev will use when recording content. This recording preference and configuration *must* be set before you record content or events in Rev.

▼   To set preferred recording order:

1.   Navigate to **Admin** > **Media Settings** > **Recording**.

2.   Use the **Primary DME** and **Secondary DME** dropdown options to set recording preference order for your system.

Keep in mind:

• Only active DMEs may be selected and used. See: View the Status of a Device

• The **Secondary DME** will be used in the event the **Primary DME** becomes unavailable or reaches maximum storage capacity.

• To avoid maximum capacity issues, the Account Admin is displayed this information upon DME selection. (Total Disk Space / Free Disk Space)

• After you have set a DME, in the DME Admin Menu, navigate to **Monitor > Recording** Status to obtain real-time status updates on any ongoing recordings on this DME (v3.22+). Specifically, you may:

   a.   Verify the existence of an ongoing recording

   b.   Verify status of the ongoing recording

   c.   Get a copy of source URL

> **Note**: To record content and event Webcasts in Vbrick Rev, you must add a DME device.

Record a Webcast Event

Add a Distributed Media Engine (DME)

Transcoding

The **Transcoding** menu displays the recommended transcoding presets included with Vbrick Rev.

The **Transcoding Preset List** displays:

Column	Description
Preset Name	Click a preset name to view and edit parameters. (Note: Editing a preset is not recommended. Duplicate and edit the copy instead).
Type	The type of encoding output the preset will produce when the original is transcoded.
Status	The current status of the preset. Active is the default.
Actions	The actions you may perform on a preset. • **Delete Preset**— Deleting is not recommended. Change the status of the preset to inactive instead so you have it in the future to use should you need it. • **Duplicate Preset** — Produces a copy of the preset (and all its parameters). Recommended instead of editing or deleting so that the original preset is preserved.

Additional functionality:

Function	Description
Add Preset	Creates a new preset.

Settings	Access global transcoding settings and rules.

Transcoding Preset Default Settings

By default, six transcoding presets have been defined for Vbrick Rev when your system is installed. These six presets have been carefully tested and authenticated and are the recommended settings to use to transcode a stored file from one video encoding format to another. They are seen in Table 1 below.

For example, when adding a stored MP4 video, the file can automatically be transcoded to H.264 or HLS format. The presets defined below are used to configure the bitrate, frame rate, aspect ratio, and so forth of the transcoded output.

Admins can also specify which user actions or "rules" will prompt transcoding to occur such as when users add or record a video. If set, when a user performs the action specified, a list of the transcoding presets selected will appear for the user to select.

Table 1: Transcoding Preset Descriptions and Encoding Output Types

Preset Name	Description	Encoding Output
Standard Definition	Distribution Method: Supports a broad range of Internet connections. Target Displays: Works best for embedding on Web pages.	H.264
High Definition 720p	Distribution Method: Best for higher Internet Speeds or Corporate Intranet. Target Displays: Tablets, TVs, and full screen PC viewing.	H.264
High Definition 1080p	Distribution Method: Corporate Intranet. Also useful for local archival and playback. Target Displays: TV, full screen PCs.	H.264
360 Video 1080p	Distribution method: WiFi, 4G+ and Intranet. Delivery: Windows 7 IE11 and other browsers that cannot play HLS	H.264
Adaptive Streaming	Distribution Method: WiFi or 4G+ Delivery Method: iOS and Android smartphones and tablets.	HLS
Adaptive Streaming for 360 Video	Distribution method: WiFi, 4G+ and Intranet. Target Displays: full screen PCs	HLS

Each preset has additional attributes such as an average bit rate versus a peak bitrate setting defined for video and audio.

Table 2: Transcoding Preset Attributes

Preset Name		Video Bitrate	Avg. Bitrate	Peak Bitrate	Frame Width	Frame Height	Audio Codec	Audio Bitrate	Audio Sample Rate
Standard Definition			800	1100	640		AAC-LC	96	48
High Definition 720p			2100	3000	1280		AAC-LC	128	48
High Definition 1080p			4000	5400	1920		AAC-LC	160	48
360 Video 1080p			2000	2200		1080	AAC-LC	160	48
Adaptive Streaming	Setting 1 Setting 2	2962 1296			1280 640		AAC-LC	128	44.1
Adaptive Streaming for 360 Video	Setting 1 Setting 2 Setting 3 Setting 4	8000 5000 2000 1200			2160 1440 1080 720		AAC-LC	160	48

> **Note**: Each transcoded instance of the video is presented to the user on the Video Settings page. Further, the user may choose which instance to play in the Video Player. See: <u>View all Transcoded Video Instances</u>.
>
> Keep in mind, the user will be presented with the following playback options to select when more than one instance of the video is available:
> - Auto where auto = HLS or the lowest quality stream available.
> - Each available video quality where the transcoding output type = H.264.

> **Warning:** Safari browsers will not play MP4 videos from Rev when the 1080p original transcoding option is selected. To use this playback option, the user should clear browser cache and then make sure that the "Always Allow"option is selected for Cookies and Website data under Privacy data.

<u>Supported Video and Audio File Formats</u>

Modify a Transcoding Rule

Transcoding may occur, with one or more transcoding presets selected, when a user performs the following actions:

- Adds a Video
- Adds a 360 Video
- Records a Video

By default, transcoding rules select the **High Definition 720p** preset for each action and ingest the original file after transcoding.

Action	Transcoding Preset	Ingest Original File
User Adds a Video	High Definition 720p	Yes
User Adds a 360 Video	• Adaptive Streaming for 360 Video • 360 Video 1080p	Yes
User Records a Video	High Definition 720p	Yes

Account Admins and Media Admins may view and edit transcoding rules.

Keep in mind:

- Admins may select additional transcoding presets used for an action; or change the current transcoding preset used.
- Admins can specify that no transcoding should occur for a given action.
- Admins can specify whether the original file should be transferred to DMEs.
- Ingesting the original file is different from "keeping" an original file in Rev. Rev always keeps an original file even if ingest is unchecked. However, if ingest original file is selected, Rev will also ingest the file to DMEs. This is a subtle but important distinction.

▼ To edit a default transcoding rule setting:

1. Navigate to **Admin**> **Media Settings** > **Transcoding** > **Settings** button.
2. Click **Edit** next to the action you want to modify.
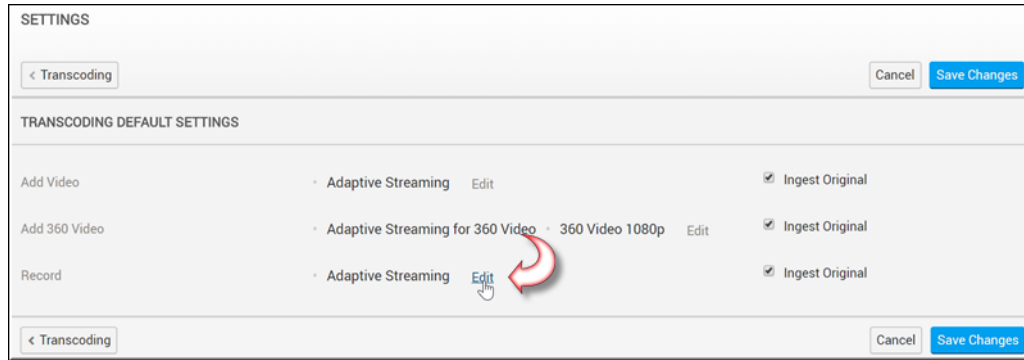
3. Click on a format in the **All** column to add it to the **Assigned Preset** column.

4. To remove a format, click on it in the **Assigned Presets** column and it will be removed.
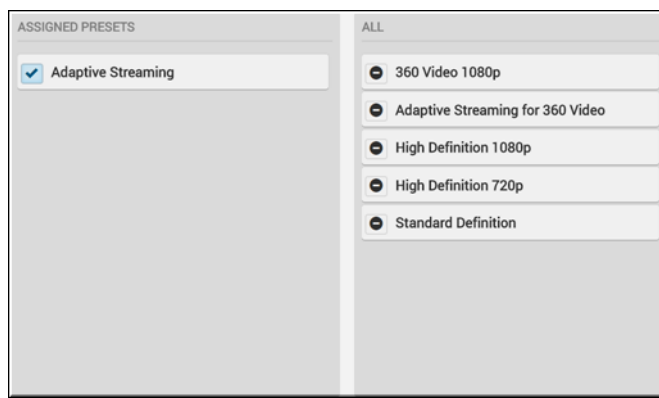
5. Click **Save Changes**.

6. The action will now transcode video into the new settings when performed and the modified preset is selected.

> **Note**: To transfer the original video to DMEs after transcoding, click the **Ingest Original** checkbox. You may *not* have transcoding disabled for a rule (no preset selected) and have **Ingest Original** deselected for the same setting.

Supported Video and Audio File Formats

Add a New Transcoding Preset

By default, four transcoding presets have been defined for Vbrick Rev when your system is installed. These four presets have been carefully tested and authenticated and are the recommended settings to use for most of your transcoding needs. Should you decide you need additional transcoding presets, you may easily define them. It is recommended that you work with Vbrick Professional Services to define your own settings.

▼ To add a new transcoding preset to your system:

1. Navigate to **Admin**> **Media Settings** > **Transcoding** > **Add Preset** button.

2. Complete each section of the form as described below..

> **Tip**: You do not have to start adding a preset from scratch if a default preset has most of the settings you need. Use the **Duplicate Preset** icon in the **Actions** column to copy the preset and then edit the parameters you need. More importantly, the format of the original preset is preserved.

Transcoding Name and Description

Field/Function	Description
Preset Name	Choose a descriptive name for the preset.
Description	A meaningful description of what the preset is intended to do.
Status	Status of the preset. Active is the default.

Video Settings

Field/Function	Description
Transcoding Output Type	The type of output that will be produced. For suggestions on best practices, see: Transcoding Preset Default Settings
Transcoding Profile	Profiles control which encoding techniques are used to produce the encoded output. The **Baseline** profile should be selected to produce a file that will play on devices with minimal CPU power and memory whereas the **High** profile may be used to produce output that will play using more powerful platforms (most computers built in the last five years will play output produced using the **High** profile). Note that **Baseline**, **Main**, and **High** profiles are only applicable to H.264 outputs.
Codec	This value is automatically set based on the **Transcoding Output Type** that is selected.
Prevent Upscale	If enabled, Rev will only transcode using the preset if the input file's resolution is greater than or equal to the resolution specified for H.264 and WM outputs. For HLS, Rev will transcode to all resolutions in the preset that are less than or equal to the resolution of the input file. If disabled, Rev will transcode to the preset regardless of the input file's resolution for H.264 and WM. For HLS, Rev will transcode to all resolutions specified in the preset. If the input video's resolution is less than that indicated by the preset, the video will be scaled up to meet the dimensions specified. The recommended best practice is to disable this attribute for the lowest resolution preset. This will ensure that all files are being transcoded to at least one preset with higher resolution files being generated as well if the input file is a higher quality file.
Key Frame Interval	Specifies the number of seconds between key frames.
Frame Rate (FPS)	Specifies the number of frames per second for the transcoded video. This may be explicitly set or it can be left as the same as the incoming video by selecting "source".
Aspect Ratio	Specifies the aspect ratio of the output frame (proportional relationship between the width and height of the output video and typically expressed in **4:3** and **16:9** in video); choose **Source** to match the aspect ratio and pixel aspect ratio of the source file being transcoded.
Bitrate Type	**Constant** versus **Variable**. Refers to amount of output data that is consumed per time segment.
Dimensions and Quality	Select the target **width**, **height**, and **bitrate**.

Audio Settings

Field/Function	Description
Codec	This value is automatically set based on the **Transcoding Output Type** that is selected.
Bitrate	Specifies the bitrate (kilobits per second) of the audio. The higher the bitrate, the more space it will take.
Sample Rate (kHz)	Specifies the sample rate of the audio. Current professional/ consumer standards for recording and playback are 128 and 48 kHz.

Webcast Templates

Account Admins are able to easily manage the catalog of Webcast templates through the **Webcast Templates** menu. This includes the ability to rename, delete, and set a default template.

▼   To view a list of saved Webcast Templates:

1. Navigate to **Admin** > **Media Settings** > **Webcast Templates**.
2. A previously saved list of templates appear. The date the template was created and the template author is detailed.
3. Use the **Actions** dropdown menu to set a default template, clear a default template, delete a template, or rename a template.

> **Note**: Rev includes a **Standard Template** out-of-the-box for new accounts or for those accounts that have been upgraded from Rev versions prior to the Webcast template feature release. The **Standard Template** reflects "hard coded" Rev defaults for a new Webcast event in terms of enabled options and settings and is set as the default template.
>
> This template may be deleted by an Account Admin or may be cleared as the default template as desired.

Create a Webcast Event Template

Apply a Template to a Webcast Event

Set a Default Webcast Event Template

Account Admins may specify a Webcast template to be the default template for all new events that are created. This means that the settings in the template will automatically populate and the Admin has control over which settings for new events are enabled or disabled by default. For example, Q&A and Polls could be disabled by all new Webcasts by default if desired.

▼ To set a default Webcast template:

1. Navigate to **Admin** > **Media Settings** > **Webcast Templates**.
2. A previously saved list of templates appear. If a default template has been previously set it is noted by a **Default** label.
3. Use the **Actions** dropdown menu to set a default template.

4. Use the **Actions** dropdown menu and select **Clear Default** to deselect a previously selected default template.

> **Note**: Rev includes a **Standard Template** out-of-the-box for new accounts or for those accounts that have been upgraded from Rev versions prior to the Webcast template feature release. The **Standard Template** reflects "hard coded" Rev defaults for a new Webcast event in terms of enabled options and settings and is set as the default template.
>
> This template may be deleted by an Account Admin or may be cleared as the default template as desired.

Create a Webcast Event Template

Apply a Template to a Webcast Event

Video Settings Templates

Account Admins are able to easily manage the catalog of Video Settings templates through the **Video Templates** menu. This includes the ability to rename, delete, and set a default template.

▼ To view a list of saved Video Setting Templates:

1. Navigate to **Admin** > **Media Settings** > **Video Templates**.
2. A previously saved list of templates appear. The date the template was created and the template author is detailed.
3. Use the **Actions** dropdown menu to set a default template, clear a default template, delete a template, or rename a template.

> **Note**: Rev includes a **Standard Template** out-of-the-box for new accounts or for those accounts that have been upgraded from Rev versions prior to the Video Settings template feature release. The **Standard Template** reflects "hard coded" Rev defaults for a new video upload in terms of enabled settings and is set as the default template.
>
> This template may be deleted by an Account or Media Admin or may be cleared as the default template as desired.

Create a Video Settings Template

Apply a Template to a Video's Settings

Set a Default Video Settings Template

Account or Media Admins may specify a <u>Video Settings</u> template to be the default template for all new videos that are uploaded. This means that the settings in the template will automatically populate and the Admin has control over which settings for new videos are enabled or disabled by default. For example, specific categories and tags could be automatically set for certain videos.

▼ To set a default Video Settings template:

1. Navigate to **Admin** > **Media Settings** > **Video Templates**.

2. A previously saved list of templates appear. If a default template has been previously set it is noted by a **Default** label.

3. Use the **Actions** dropdown menu to set a default template.

4. Use the **Actions** dropdown menu and select **Clear Default** to deselect a previously selected default template.

> **Note**: Rev includes a **Standard Template** out-of-the-box for new accounts or for those accounts that have been upgraded from Rev versions prior to the Video Settings template feature release. The **Standard Template** reflects "hard coded" Rev defaults for a new video upload in terms of enabled settings and is set as the default template.
>
> This template may be deleted by an Account Admin or may be cleared as the default template as desired.
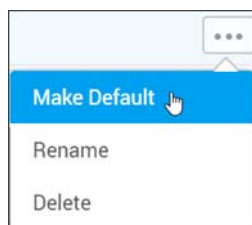
Create a Video Settings Template

Apply a Template to a Video's Settings

Integrations

The **Integration** menu displays all the supported media integrations that are available for use with Rev in once place. It includes such items as Webex video conferencing (Teams and Meetings), VoiceBase transcription services, and so forth.

This menu option also contains the Rev IQ module (AI & Machine Learning) with Facial Recognition abilities. What is visible here depends largely on what licensing has been purchased or activated in Rev, detailed below. If you need more information, contact your Account Manager or Support Services.

Section	Description
AI & Machine Learning	**Facial Recognition** - Only visible if you have licensed AI hours and Rev IQ credits. Disabled by default. • Enable Facial Recognition **Rev IQ Transcription and Transcription** - Always visible. • Enable Rev IQ Transcription and Translation **VoiceBase** - Always visible. • Enable VoiceBase Integration **Automatic Transcription** - Only visible if a transcription service (Rev IQ or VoiceBase) is enabled. • Configure Automatic and Default Transcription and Translation Settings **Default Transcription and Translation Settings** (Service/Language) - Only visible if a transcription service (Rev IQ or VoiceBase) is enabled. • Configure Automatic and Default Transcription and Translation Settings
Microsoft Office365	**Microsoft Teams Integration** - Always visible. • Enable Microsoft Teams Integration
Video Conference Recording and Streaming	This section must first be enabled by Vbrick. Speak to your Account Manager if it is not visible. **Video Conference Recording** - Enables video conference recording in the video Upload menu. • Enable Video Conference Recording for Video Uploads **Webcast Streaming** - Enables video conference streaming and recording for Webcast events. • Enable Webcast Streaming from a Video Conference
Webex Meetings	Used to enable the **Webex Meetings** integration including support for Live Streaming, Single Sign On, Common Identity (CI) Sites, and import settings. See: Add and Configure a Webex Meetings Site

Section	Description
Webex Teams	Used to enable the **Webex Teams** integration. See: Enable Webex Teams Integration
Zoom Meetings	Used to enable the Zoom Meetings integration. • Enable Zoom Meetings Integration

Apply a License Type or Add-On Component to a Child Account

Enable Facial Recognition

Facial Recognition in Rev extends the functionality of both video tagging (on the **In This Video** form) and on the Video Player interface through timeline tagging (on **Video Basic Information** and **Video Pulse** flyout tabs) for videos in the Rev library.

This functionality is disabled by default and must be enabled. It also requires a valid profile picture to work correctly. Users may decide to opt-out at any time, even if this functionality is enabled, by updating their **Profile Settings** (See: Update Your Rev Profile Settings).

> **Note**: Facial Recognition functionality requires the purchase of additional AI Hours licensing components. Speak to your Account Manager for details.
> See: Rev License Types and Add-On Components

▼ To enable Facial Recognition:

1. Navigate to **Admin** > **Media Settings** > **Integrations**.
2. Scroll to the **AI & Machine Learning** section.
3. Select the **Allow tagging of users in a video using profile pictures** checkbox and click **Save Changes**. **Note**: If this checkbox is not visible, you must purchase additional licensing. Contact your Account Manager for details.

When a Facial Recognition license is purchased and tagging is active:
- Rev builds a search index based on profile pictures that have been uploaded. This index is updated continuously to account for additions and deletions to profile pictures.
- This means that Rev can now "predict" the speakers that will appear in a given video (based on profile pictures of those users that have *not* opted-out through profile settings or deleted their profile image).
- A **Tag Users in this Video** button is now visible in the **In this Video** form in Video Settings. When clicked, Rev automatically tags users found in the video in place of using the **Find Items** box to manually tag individual users. If Facial Recognition is disabled, individuals must be manually tagged once more using Find Items.
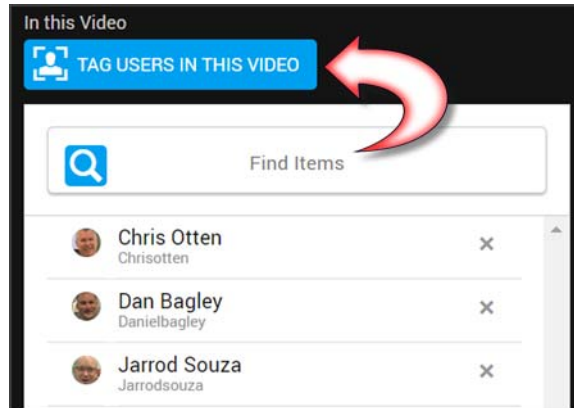
- Timeline tagging is now active in the <u>Video Basic Information Flyout</u>, notated by an arrow **>** next to each profile picture. Clicking a profile image highlights the time-frame where the speaker appears in the video on the playback bar (<u>Player and Playback Bar</u>). Profile images are still displayed here if Facial Recognition is *not* activated though they are not active/clickable.
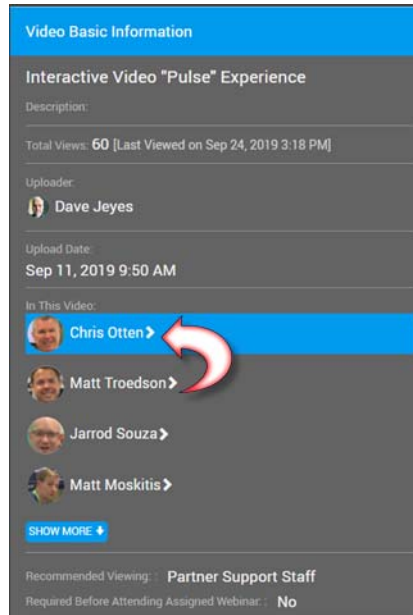
- Timeline tagging is now active in the <u>Video Pulse Flyout</u>. Similar to the **Video Basic Information** flyout, indicated by an arrow next to profile pictures **(>)**. When active, the Pulse panel highlights each user interactively (during playback) as they appear in real-time along with audio transcript highlighting (if SRT file is uploaded).
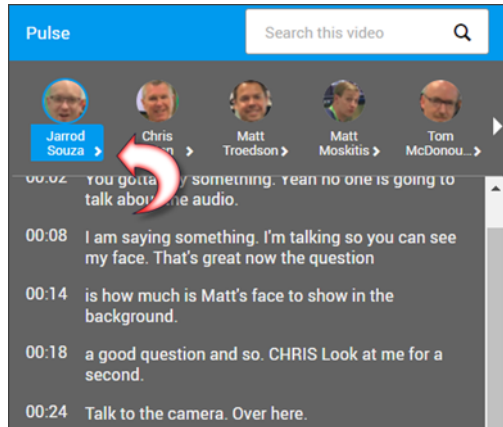
Caution: Individual user accounts may *always* opt-out of Facial Recognition by modifying their Profile Settings even when it is active.

Tag Users In This Video

Tag Users Automatically with Facial Recognition Activated

Update Your Rev Profile Settings and Picture

Video Metadata and Flyout Menu Options

Generate Subtitles for a Video with Rev IQ

Generate Subtitles for a Video with VoiceBase

Enable Rev IQ Transcription and Translation

You may generate a transcription file for a video and have a SubRip (.srt) file created directly from Rev using **Rev IQ Transcription and Translation** services if you have purchased a Rev AI license. Rev IQ transcription files may be automatically (or individually) translated to additional supported languages if desired.

You must have a Rev AI license and Rev IQ credits available to use transcription and translation feature(s).

Note: Prior to the v7.34 release of Rev, the **Rev IQ Transcription and Translation** service was titled **Vbrick Transcription**.

▼ To enable Rev IQ Transcription and Translation in Rev:

1. Navigate to **Admin** > **Media Settings** > **Integrations**.
2. Select the **Enabled** checkbox next to **Rev IQ Transcription and Translation** in the **AI & Machine Learning** section.

3. Configure automatic and default transcription and translation settings.
4. Click the **Save** button to save your Rev IQ transcription settings.

This adds the following functionality to Rev:

- Automatic transcription and translation file generation for new uploaded videos if you configured the **Automatic Transcription** checkboxes.
- A **Generate Subtitles** tab in the **Subtitles** section of **Advanced Video Settings**.
    - This tab will allow you to generate a .srt file for the selected video using Rev IQ or VoiceBase transcription services (whichever is enabled or selected) or continue to create your own using Rev's upload feature.
- The ability to translate the transcript to additional (supported) languages when using Rev IQ transcription.

Generate Subtitles for a Video with Rev IQ

Configure Automatic and Default Transcription and Translation Settings

Translate a Subtitle File to Additional Languages

Licensed Add-On Components

Enable VoiceBase Integration

Rev integrates with VoiceBase so that, if you have a VoiceBase account, you may send a video for transcription and have a SubRip (.srt) file created directly from Rev. Once your video has been transcribed and the .srt file returned to Rev, your videos are deleted from VoiceBase, ensuring your account's security.

> **Note**: As of this time, English is the only supported language in VoiceBase. You must have a VoiceBase account created at https://www.voicebase.com/ before you begin this process.

▼ To enable the VoiceBase Integration in Rev:

1. Navigate to **Admin** > **Media Settings** > **Integrations**.
2. Select the **Enabled** checkbox next to **VoiceBase Integration** in the **AI & Machine Learning**. section.

3. Enter the **Bearer Token** obtained from your VoiceBase account.
4. To obtain a Bearer Token, log in to https://apis.voicebase.com/developer-portal.
5. Navigate and click the Bearer Token Management widget.
6. Click the **New Key** button in the upper right corner to generate a new Bearer Token.
7. Copy the generated token into the **Bearer Token** field in Rev.
8. Configure Automatic and Default Transcription and Translation Settings.
   a. **Note**: While automatic transcription may be configured, VoiceBase transcription may not be used for automatic translation services at this time.
9. Click the **Save** button to save your transcription settings.

This adds the following functionality to Rev:

• A **Generate .srt Files** tab in the **Subtitles** section of **Advanced Video Settings**.
• This tab will allow you to generate a .srt file for the selected video using VoiceBase or continue to create your own using Rev's upload feature.
• Keep in mind that VoiceBase has its own pricing structure and is pay as you go per video file.

> **Tip**: If you need to disable VoiceBase, the integration values entered for will be saved should you enable the integration again.

Generate Subtitles for a Video with VoiceBase

Configure Automatic and Default Transcription and Translation Settings

Translate a Subtitle File to Additional Languages

Configure Automatic and Default Transcription and Translation Settings

When you enable transcription services in Rev, you can configure what type of transcription occurs automatically for new video uploads as well as the default transcription service and language used.

If you use the **Rev IQ Transcription and Translation** service, you can also choose automatic translation services to occur at the same time and select default languages to use.

Keep in mind that the following must be true to use automatic transcription and translation:

• At least one type of transcription service must be activated and enabled.
• To use automatic translation, you must use **Rev IQ Transcription and Translation**.
• The **Rev IQ Transcription and Translation** service must also have the following configurations applied:
   • A primary language set in Rev account settings (VoiceBase is always set to English at this time).
   • The Rev AI license applied and Rev IQ credits configured.
• Note that Large videos may not be transcribed; the limits are a file length of 4 hours or file size of 2 GB.

Configure Transcription Settings

▼   To configure automatic transcription settings:

1. Enable a transcription service as you normally would in **Admin** > **Media Settings** > **AI & Machine Learning**.

2. Enable the **Automatic Transcription** checkbox settings desired for the service. When enabled, this means that new video uploads are *automatically* transcribed by selecting the following options:

    •   New Live Event Recordings (including video conference based events)

    •   All Other Uploads (including video conferenced based imports and uploads)

3. Select your **Default Transcription Service** by choosing Rev IQ or VoiceBase Transcription. **Note**: If you only have one transcription service enabled, this default service is selected automatically for you. Otherwise, you may select which one is the default service you would like to use. If you plan to configure automatic translation services, you *must* choose **Rev IQ** here.

4. Choose your **Default Transcription Language**. **Note**: Only English is available for **VoiceBas**e at this time.

Configure Translation Settings

▼   To configure automatic translation settings:

1. Make sure that the **Rev IQ** transcription service has been selected in **Admin** > **Media Settings** > **AI & Machine Learning**. VoiceBase transcription may not be used for automatic translation services at this time. See: Enable Rev IQ Transcription and Translation

2. Make sure you have configured **Automatic Transcription** settings as described above. **Note**: If you do *not* enable **Automatic Transcription** settings, you will still be able to translate individual videos as needed but new video uploads will *not* be translated automatically.

3. Choose your **Default Transcription Language**. This is the source language the transcription file will generate the .SRT file from for new uploads if the **Automatic Transcription** checkboxes are configured.

4. Select your **Default Translation Language(s)** from the supported languages. The additional languages the transcription file will be translated and generated into automatically for new uploads if **Automatic Transcription** checkboxes are configured.

Enable Rev IQ Transcription and Translation

Generate Subtitles for a Video with Rev IQ

Translate a Subtitle File to Additional Languages

Generate Subtitles for a Video with VoiceBase

Enable Microsoft Teams Integration

Rev integrates with Microsoft Teams so that, when enabled:

•   You may view Rev content in a Microsoft Teams Channel tab. This includes:

    •   Rev Event Calendar

    •   Rev (VOD) videos

- • Rev Categories
- • Microsoft Teams are available as a Rev Webcast source and as a VCI Recording source. This enables two functions:
  - • Record a Microsoft Teams Meeting
  - • Schedule a Microsoft Teams Webcast Event

> **Caution**: The ability to use Microsoft Teams as a Webcast and VCI Recording source is in early access with limited release for **Rev v7.37**. Speak to Vbrick Customer Support for details.

View Rev Content in Microsoft Teams Channel Tab

When you enable the Microsoft Teams Integration, you are able to publish Rev content to a Teams Channel Tab. Content that may be viewed includes the Rev Webcast Calendar, VOD videos, and Rev Categories.

▼ To view Rev content in a MS-Team Channel Tab:

1. Navigate to **Media Settings** > **Integrations** > **Microsoft Office365** section.
2. Select the **Enabled** checkbox next to **Microsoft Teams Integration**.
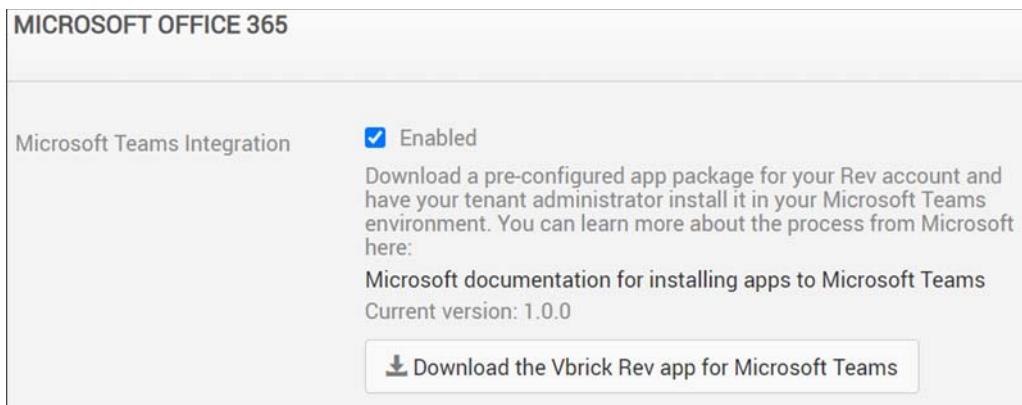
3. Click the **Download the Vbrick Rev app for Microsoft Teams** button and download the Vbrick Rev app zip file. Your Microsoft Teams Admin uses the Zip file to add the Rev app to your Microsoft Teams tenant so that it can be used across all teams. Alternatively, the application package can be uploaded for use with a specific team.
4. **Note**: If you need assistance with installing a custom app in Microsoft Teams, please refer to the Microsoft Teams documentation. The following article may be of assistance:
   a. Tenant-wide Deployment: "Publish Apps in the Microsoft Teams Tenant Apps Catalog"
   b. Specific Team Deployment: "Upload your package into a team using the Apps tab"
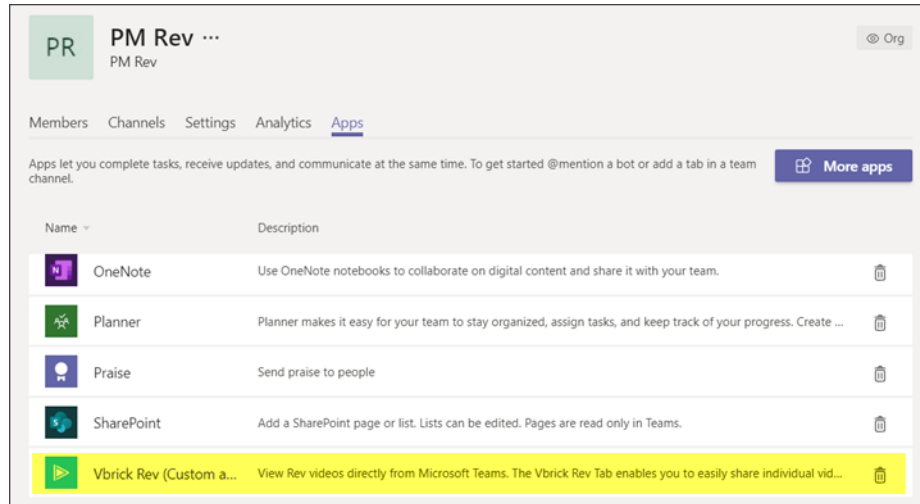
5. Once your Microsoft Teams Admin has added the Vbrick Rev app to your Microsoft Teams tenant (or to a specific team), you may add the new Rev tab to your Team channels. The Vbrick Rev tab enables you to:

   • Share a list of upcoming Rev Webcast events with other members of the team.

   • Share a video from the Rev VOD library.

   • Share a Rev video category for quick access to all the videos in that category.

   • Share a Rev Channel's video collection for quick access to all the videos for that category.

   • See: Accessing your uploaded configurable tab for details on how to add tabs to your channel from a custom App.

Record and Schedule Microsoft Teams Meeting

When Microsoft Teams Video Conferencing is enabled, Rev is able to record and stream your Microsoft Teams meetings from Webcast events and the Video upload menu.

> **Caution**: The ability to use Microsoft Teams as a Webcast and VCI Recording source is in early access with limited release for **Rev v7.37**. Speak to Vbrick Customer Support for details.

▼ To record and schedule Microsoft Teams Meetings:

1. Navigate to **Media Settings** > **Integrations** > **Microsoft Office365** section.

2. Select the **Enabled** checkbox next to **Microsoft Teams Video Conferencing**.

3. Once enabled, your Microsoft Admin must click the registration URL that appears to authorize Rev to connect with Teams. This automatically registers Rev with your Microsoft Teams account and allows it to be used as a streaming source.

Note: If you disable the Microsoft Teams integration in Rev, Rev content will no longer be displayed or shown within the Microsoft Teams tabs. However, the Rev tabs themselves remain until you manually remove them from your Microsoft Teams channels.

The Microsoft Teams tab(s) will also be removed from Webcast Events and the Recording tab as a source.

Schedule a Microsoft Teams Webcast Event

Record a Microsoft Teams Meeting

Supported Video Conference (VC) System Integrations

Enable Video Conference Recording for Video Uploads

The ability to record from a Video Conference is accessed through the **VC Recording** tab on Rev's video **Upload** menu. This tab must first be enabled.

▼ To enable Video Conference recording from the Upload menu:

1. Navigate to **Admin** > **Media Settings** > **Integrations**.
2. Scroll to the **Video Conference Recording and Streaming** section.
3. Select the checkbox next to **Enable Video Conference Recording** to enable it.

This adds the following functionality to Rev:

• A **VC Recording** tab becomes visible on the **Upload** menu.
• You can enter a **Video Address** or **SIP** address.

Record a Video Conference

Schedule a Video Conference (VC) Live Webcast Event

Schedule a Webex Team Webcast Event

Enable Webcast Streaming from a Video Conference

Rev supports the ability to stream and record from a Video Conference (as the video source) to a Rev Webcast event. The final recordings will capture both active speakers and content streams (if available). This functionality must be enabled first.

▼ To enable Webcast streaming and recording from a Video Conference:

1. Navigate to **Admin** > **Media Settings** > **Integrations**.
2. Scroll to the **Video Conference Recording and Streaming** section.
3. Select the checkbox next to **Enable Webcast Streaming from Video Conference** to enable it. **Note**: **Video Conference Recording** must also be enabled before this checkbox is visible.

This adds the following functionality to Rev:

- A **Video Address** tab becomes visible as a **Video Source** during Webcast Event set up that allows you to use your Video Conference/SIP address as a source.

Record a Video Conference

Schedule a Video Conference (VC) Live Webcast Event

Schedule a Webex Team Webcast Event

Add and Configure a Webex Meetings Site

Users may upload their Webex meeting recordings (**My Webex** > **My Files** > **My Recordings**) if a Webex Meetings site has been added and configured. Only Account Admins and Media Admins are able to add and configure a meeting site in Rev.

If your organization supports multiple Webex Meetings sites, Rev allows you to configure as many as needed with supporting functionality to edit, delete, and duplicate sites.

> **Caution**: This integration requires that **AllowDownloadRecordingWithoutPwd** is enabled for your Webex site as described in, "F9847 A New Download URL is able to Download Recording Directily".
> Submit a ticket to the Webex Provisioning Team to enable this flag before proceeding.

▼ To add a Webex Meetings site:

1. Navigate to **Admin** > **Media Settings** > **Integrations**.
2. Scroll to the **Webex Meetings** section.
3. A list of existing Webex Meetings sites displays with the following information displayed:
   - **Name**: User-provided name of the site when it was configured.
   - **CI-Enabled**: Read-only checkbox that specifies if the site is enable for Common Identity (CI).
   - **Auto Import**: Specifies if the site is available or used for live streaming.
   - **Manual Import**: Specifies if the site is available for manual import.
   - **Status**: Specifies if the site is linked, unlinked or not applicable (blank).

- **Actions**: Provides an Actions menu (described below).

4. Click the **Add Webex Meeting Site** button to create a new site. You may also click the **Actions** menu next to an existing site to access the following menu options:

    - **Edit**: Allows you to modify the clicked site's current settings.
    - **Delete**: Deletes the site. Note that any pending scheduled auto-imports are also removed. This does not need interrupt an in progress import however.
    - **Duplicate**: Copies the selected site's settings.

5. To add a basic Webex Meetings site, complete and **Save** the following fields/settings as needed:

    - **Hosted Website**: The **Site Brand Name** field found in the Site Administration section when logged in Webex Meetings as an Admin. You *must* include https:// here.
    - **Support for Webex Meeting Live Streaming**: Controls live streaming from Webex Meetings options. **See**: Enable Webex Meetings Live Streaming Support
    - **Support for Import Recordings**: Controls manual and auto import options for recordings from Webex Meetings. Also opens ability to enable Common Identity (CI) enabled site. **See**: Configure a Common Identity (CI) Webex Meeting Site, Configure Manual Import Settings for Webex Meetings, Configure Auto Import Settings for Webex Meetings.

Upload a Video from Webex Meetings

Stream a Webex Meeting to a Scheduled Rev Webcast Event

Enable Webex Meetings Live Streaming Support

When support for live streaming from Webex is enabled in Rev, you are able to access the following functions directly from your Webex Meeting client:
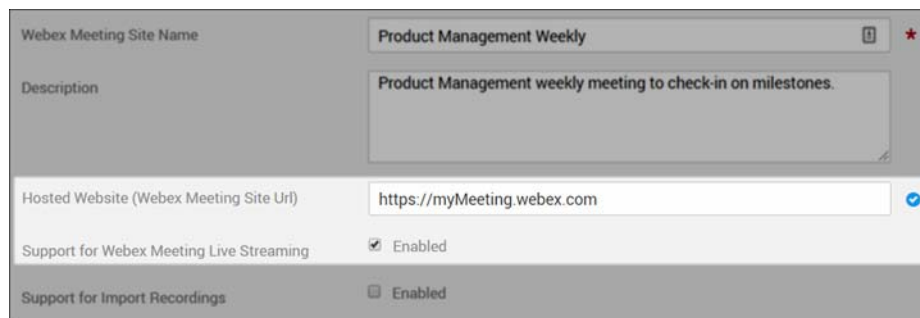
- **Stream a Webex Meeting to a New Rev Webcast Event.** Start and broadcast your Webex Meeting, including the ability to save your meeting as a (VOD) video once

completed, to a new Rev Webcast event. Some Rev Webcast event features will be limited until after the event starts (such as polls and Q&A) at which point you may edit them inline.

• **Stream a Webex Meeting to an Existing (Scheduled) Rev Webcast Event.** Start and broadcast your previously scheduled Rev Webcast event directly from your Webex Meeting, including the ability to save your meeting as a (VOD) video once completed.

• **Stream a Webex Meeting as a new VOD recording**. This records your Webex Meeting as a new (VOD) video in Rev. Once complete, update the Video Settings in Rev as you normally would.

> **Caution**: This is a Rev Cloud only feature that requires Rev v7.31 or later and Webex Meetings WBS39.10 or later.

▼ To enable Webex Meetings Live Streaming Support:

1. Navigate to **Admin** > **Media Settings** > **Integrations**.
2. Scroll to the **Webex Meetings** section. Select the Webex Meetings site you want to enable for streaming. (Edit it by clicking its name or through the **Actions** menu)
3. Select the **Support for Webex Meeting Live Streaming** checkbox.

Webex Meeting Site Name	Product Management Weekly		🗓	*
Description	Product Management weekly meeting to check-in on milestones.			
Hosted Website (Webex Meeting Site Url)	https://myMeeting.webex.com			●
Support for Webex Meeting Live Streaming	☑ Enabled			
Support for Import Recordings	☐ Enabled			

You may now use Webex Meetings live streams as the source for both Webcast Events and VOD recordings in Rev.

Stream a Webex Meeting to a Scheduled Rev Webcast Event

Stream a Webex Meeting as a New VOD Recording

Configure a Common Identity (CI) Webex Meetings Site

When you create a CI-enabled site, users are supported with a Common Identity which means that those with multiple accounts (with the same email address) will always be directed to the Common Identity login flow.

To create a CI-enabled Site, you must create a Webex Teams app to grant Rev permissions to Webex Meetings (specifically, **spark:all** scope permissions). This is done through the Cisco Developer site by creating a new **Integration**. When creating the CI-enabled site, **Client ID** and **Client Secret** can then be obtained from the App.

> **Note**: If you previously created the Webex Teams app to enable the Webex Teams integration in Rev, you may modify your existing app instead of creating a new one here.
>
> See: Enable Webex Teams Integration

▼ To create a CI-enabled site for your Webex Meetings integration:

1. Navigate to **Admin** > **Media Settings** > **Integrations** and select the Webex Meetings site you want to enable.

2. Select the **Support for Import Recording** checkbox. This will make the CI checkbox visible.

3. Select the **Common Identity (CI) Enabled Site** checkbox.

4. Make sure your Webex Teams App is created or modified with the **spark.all** scope permissions and you have obtained your Client ID and Client Secret from the **OAuth Settings** section once saved.

5. A new set of fields will appear for providing authentication options. All fields are required and should be completed by a Webex Site Admin.

6. **Site Name**: This is normally provided by Webex. By default, it is the sub-domain on the webex.com URL. For example, for acme.webex.com, the site name is acme.

7. **Client ID**: Provided by the Webex Teams app.

8. **Client Secret**: Provided by the Webex Teams app.

9. **Link to Webex Site** button: Once you have completed the fields above, this button launches authentication to Webex to obtain an access token. Status is displayed directly on the button.

   • **Green checkmark**: Linked - authentication is established and access token was received and is valid (last known).

   • **Red X**: Not currently authenticated or the access token is now no longer valid or in a current state of authentication.

10. Keep in mind that the user will be prompted to log in with a valid Webex Meetings account each time if not already logged in. (If SSO is not enabled). **See**: Configure Manual Import Settings for Webex Meetings

Warning: For CI-enabled sites, it is possible for the Webex access token to expire or become invalid.

If this occurs:
- The **Linked** status next to the **Link to Webex Site** button will flip to an **Unlinked** status.
- A notification email will be sent to the Rev Account Admin that originally authenticated to Webex that the integration should be updated/authenticated again. This email is displayed next to the status indicator.
- A Rev notification flag will appear.

Add and Configure a Webex Meetings Site

Enable Webex Meetings Live Streaming Support

Configure Manual Import Settings for Webex Meetings

Configure Auto Import Settings for Webex Meetings

Enable Webex Teams Integration

Configure Manual Import Settings for Webex Meetings

When you add a Webex Meetings site, you need to decide how you will import your saved video as part of that site configuration. You may choose to manually import or to auto import each time a meeting is saved as a video.

▼ To configure manual import settings for a Webex Meetings site:

1. Navigate to **Admin** > **Media Settings** > **Integrations** and select the Webex Meetings site you want to configure.
2. Select the **Support for Import Recording** checkbox. This will make the Common Identity (CI) site configuration options available and, below them, also make your manual and auto import checkbox options available.
3. Click the **Manual Import of Webex Meetings** Recordings.
4. Click the **Use user's email for SSO** checkbox for additional authentication with Webex Meetings.
   - The user will be prompted to log in with a valid Webex Meetings account each time if not already logged in. (If SSO is not enabled)
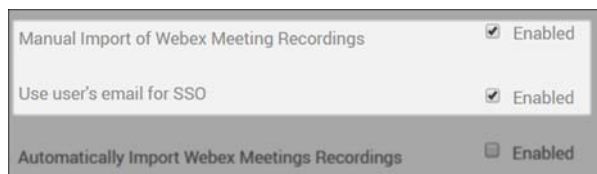
What this does:
- This site will now appear in the meeting dropdown when you click the **Add Content** > **Tools** > **Webex Meetings** icon. **See**: Upload a Video from Webex Meetings

- Keep in mind that the **Import** tab will list the 100 most recent video files (within the last 180 days only) that are available in MP4 format. (**Note**: Legacy Webex accounts with .arf files are not supported in this integration)
- Only the newest video files are listed first with the following attributes:
    - Recording name
    - Create date and time
    - File size (MB)
    - If the file has already been imported to Rev (if previously uploaded and deleted, it will not be marked as imported)
    - Multiple files may be selected and imported

Add and Configure a Webex Meetings Site

Enable Webex Meetings Live Streaming Support

Configure Auto Import Settings for Webex Meetings

Enable Webex Teams Integration

Configure Auto Import Settings for Webex Meetings

When you add a Webex Meetings site, you may choose to automatically import your saved meeting videos. This allows you to leverage Rev as the repository for all recorded Webex Meetings and have Rev automatically ingest any new recordings from your Organizational site.

There are a number of filters that are available when you choose to configure auto-import. They include:

- Automatically delete recorded Webex Meetings from the Webex Site once they have been imported into Rev.
- View how many Site meeting recordings remain to be imported into Rev.
- Stop an import process if needed.

▼   To configure auto import settings for a Webex Meetings site:

1.   Navigate to **Admin** > **Media Settings** > **Integrations** and select the Webex Meetings site you want to configure.
2.   Select the **Support for Import Recording** checkbox. This will make the Common Identity (CI) site configuration options available and, below them, also make your manual and auto import checkbox options available.
3.   Click the **Automatically Import Webex Meeting Recordings** checkbox.
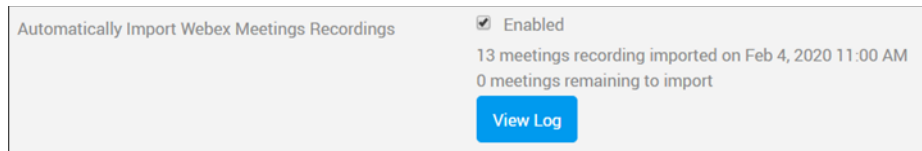
4.   Several options and filters become visible. Complete them as needed below.

View Number of Auto Imports and Remaining Auto Imports

Once enabled, Rev automatically keeps track of the number of imports that has occurred (every 30-60 minutes) and the number of Webex Meetings videos left to import based on the settings you configure. This is viewed directly under the Auto Import checkbox.

Under the checkbox, the following information is displayed:

- Date and time of the last (most recent) import.
- Number of meeting recordings imported on the last run of the import.
- Number of meeting recordings remaining to import (if any). **Note**: If import in progress, a **Postpone** button will be visible next to this detail to postpone the import.
- Date and time of next scheduled import (if applicable).

Automatically Import Webex Meetings Recordings	☑ Enabled
	13 meetings recording imported on Feb 4, 2020 11:00 AM
	0 meetings remaining to import
	View Log

Click the **View Log** button for more details on specific dates of the imports. **Note**: You are also able to view this log from the **Actions** dropdown menu next to the Webex Site. You are able to observe:

- Date and time of the import run.
- Number of meetings imported on that run.
- Number of meetings not imported (individual videos are disabled from importing).
- Number of meetings postponed.
- Status (Success, Partial, Error)
- Details
    - Partial (Exceeded maximum videos allowed per day)
    - Errors/Warnings
        - Admin must re-authenticate with Webex
        - Exceeding available storage
        - Other system errors

VIEW LOG

Date	Imported	Postponed	Status	Details
Feb 4, 2020 1:00 PM	0	18	Partial	MaxImportExceeded
Feb 4, 2020 11:00 AM	13	0	Success	
Feb 3, 2020 2:00 PM	0	27	Partial	MaxImportExceeded
Feb 3, 2020 1:00 PM	3	0	Partial	MaxImportExceeded

Note: Rev will only allow a maximum of 100 hours of ingested recordings per day and/or 10 hours of ingested recordings per recurrence to prevent overwhelming the system at any one time.

A recording will not be re-imported if it has previously been ingested even if it has since been removed or deleted from Rev.

Set Auto Import Meeting Days and Default Uploader

You have the option to specify how many days back Rev should go when auto importing video from a Site. For example, you can specify that Rev should only import meetings that have been recorded within the past 10 days if necessary. You can also configure a default Uploader and email address to assign to the import.

This is accomplished through the following:

- **Skip importing meetings older than (# of days)** - In the image above, videos older than 50 days will not be auto imported.
- **Select Default Uploader** - You may enter a default user account that will be assigned as the video uploader in this field. Otherwise, you may use autouploader here. **Note**: The user account must be a Media Contributor or higher and cannot be a group.
- **Use Email Address to Match Uploader** - If this checkbox is enabled, then the video uploader is set as the Rev user account that matches the Webex Host's email address. If no matching email address is found, then the Default Uploader field is used instead.

Select Recording Types to Auto Import

Use the **Select Recordings to Import** control to specify which types of recordings to auto import.

- **All Recordings** - This will import all available recordings in the Webex Meeting
- **User Recordings** - This will import only the recordings specified users or groups specified in the Find Items control. **Note**: If a Team is set and the effective Uploader does *not* have Team Contributor or higher permissions for the selected Team, then the video will not be assigned to that Team.

Delete Auto Import Recordings

Use the Delete Recordings checkbox if you want to remove the videos from your Webex Meetings site once they have been ingested into Rev.

> **Caution**: Be aware that if you use this setting, your videos will be *permanently* deleted from your Webex Meeting and you will *not* be able to retrieve them. Use with caution!

Configure Auto Import Video Settings

Finally, you may configure several Video Settings with the auto import setting just as you normally would when uploading a video. They are:

• Access Control

• Status

• Expiration Rules

• Categories

• Tags

For more details, see the corresponding Video Settings help topic.

Add and Configure a Webex Meetings Site

Enable Webex Meetings Live Streaming Support

Configure Manual Import Settings for Webex Meetings

Enable Webex Teams Integration

Enable Webex Teams Integration

Users can share videos by posting a message to a Webex Team space containing a link to a Rev video directly from Rev. Other users in the space can then launch and play the video. Additionally, users can subscribe a Webex Team space to a specific Rev category so that each time a video is added to that category, a message containing a link to the new video will be posted to the subscribed space.

In order to enable the Webex Team integration, you must create a Webex Teams app to grant Rev permissions to Webex Teams. This is done by creating a new **Integration** on the Cisco Developer site.

When creating the Webex Team app, enter the following Rev-specific required information below:

1. **Redirect URI(s)**
   a. \<Rev URL>/spark/oauth/cb
   b. Example: YourOrgsRev.com/spark/oauth/cb
2. **Scopes** - Select the following scopes:
   a. spark:messages_write (Post and delete messages on your behalf)
   b. spark:rooms_read (List the titles of rooms that you are in)
   c. **Note**: If you also plan to enable the Webex Meetings integration, you may use this same Teams App and select spark:all here instead.
3. Once the **Add Integration** button is clicked and it is saved, use the **Client ID** and **Client Secret** under the **OAuth Settings** section to enable the Webex Teams integration in Rev, described below. (**Note**: You can always return to your App by clicking your Profile image in the Cisco Dev Center)

▼ To enable the Webex Teams integration in Rev:

1. Navigate to **Admin** > **Media Settings** > **Integrations**.
2. Scroll to the **Webex Teams** section.
3. Select the **Webex Teams Integration** checkbox.
4. Enter the **Client ID** provided to you by the App in the **OAuth Settings** section.
5. Enter the **Client Secret** provided to you by the App in the **OAuth Settings** section.
6. Click the **Save** button.

This adds the following functionality to Rev:

• A **Share to Webex Teams** button on the **Sharing** tab in **Video Settings**.
• A **Subscribe Webex Teams** button on each category page under **Media** > **All Videos**.

> **Tip**: If you need to disable Webex Teams, the integration values entered for **Client ID** and **Client Secret** will be saved should you enable the integration again.

Share a Video to a Webex Team

Subscribe a Category to a Webex Team

Schedule a Webex Team Webcast Event

Add and Configure a Webex Meetings Site

Enable Zoom Meetings Integration

Rev integrates with Zoom so that you are able to use a Zoom Meeting conference call as the video source for a Rev Webcast Event.

To use this integration you will need the following:

• A **Zoom Meeting Pro Account** with at least one Room Connector/SIP license.
• An Akamai Live device set up in Rev Devices. See: Add an Akamai Live Device.

▼ To enable and install Zoom in Rev:

1. Navigate to **Admin** > **Media Settings** > **Integrations**.
2. Scroll to the **Zoom Meetings** section.
3. Select the **Zoom Meetings Integration** checkbox to enable the integration.
4. Click the **Install Zoom Integration** button.

> **Caution**: If you are currently running two separate Rev accounts and attempting to install and associate the same Zoom account to both, it may be necessary to reinstall the Zoom integration on your first Rev tenant in some circumstances.
>
> Zoom only supports one integration per one Rev tenant at this time.

5. You will be redirected to the Zoom Login page where you need to authorize Rev with access to your Zoom account.

6. Once authorized, the Vbrick Rev app will be installed for you from the Zoom marketplace. Keep in mind that you may return to the **Integrations** page to uninstall the integration at any time.

Enabling the Zoom integration adds the following functionality to Rev:

Zoom Meeting Webcast Events

- A **Zoom Meeting** tab becomes available as a **Video Source** on a Webcast Event.
- All Zoom scheduled meetings appear automatically when you select this tab as the Video Source for your Webcast Event. **Note**: Meetings that are in the past do not appear.
- If you do not have any meetings scheduled, you will need a **Zoom Meeting ID** or **Zoom Meeting URL** to stream a Zoom Meeting video to your Webcast Event.

- Using this option provides you the full features and options of the Rev platform in conjunction with your Zoom meeting.
- For detailed usage, see: Schedule a Zoom Meeting Webcast Event

Zoom Meeting VC Recording

- A **Zoom Meeting** becomes available as a Video Conference option on the Rev **Add Content > Recording** tab.
- You must enter a valid **Zoom Meeting ID** or **Zoom Meeting URL**.
- For password protected Zoom meetings, you must enter a the H323/SIP numeric **Password** for the meeting.

Schedule a Zoom Meeting Webcast Event

Record a Zoom Meeting

System Settings

System Settings Overview

System Settings in Vbrick Rev determine how security is handled, contact and billing information for your organization, and system environment options such as keys, branding, and the **Home Page** look and feel.
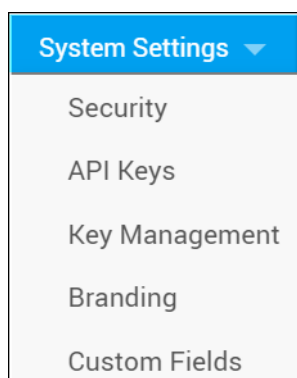
Options under the **System Settings** menu include:

- **Security** — Used to configure password options that will be used for your system such as how complex it is and whether or not it will use upper or lower case letters, numbers, and special characters. Lockout settings, session timeout, sharing/embedding settings, public access options, and single sign on settings are also defined here.
- **API Keys** — Define and manage the API keys you have added to your system to connect Rev with external devices.
- **Key Management** — Used to manage your own encryption Master Key for use with Rev and AWS S3.
- **Environment** — Configure the system's email server and settings so that emails are sent automatically to your user accounts when necessary. (Note: This menu is only visible from an Admin Account of the root account environment. If you are not an admin or are not logged into the Rev root account, you will not see this menu option. See: "Root Account System Settings" in the Rev Root Account Functions User Guide on the Documentation Site)
- **Branding** — Customize the colors and logo of the system. Apply custom styles and colors to the Rev header and Featured Video carousel.
- **Custom Fields** — Add custom fields to Rev to add details to video content that are specific to your organization.
- **System Messages** — Set a system message, such as a maintenance message, to appear at a specific start date and time that will continue until an end date and time that you specify. (Note: This menu is only visible from an Admin Account of the root account environment. If you are not an Admin or are not logged into the Rev root account, you

will not see this menu option. See: Rev Root Account User Guide on the Documentation Site for more details)

Manage Security Settings

Security in Rev is configured on multiple tiers; user passwords, lockout settings, and session settings. This allows you to configure how stringent access to your system will be. You may also use this menu to set up single sign on if needed as well as direct your DME streams to specific zones. based on user's location.

You must have the Account Admin role to modify these settings.

The **Security** module handles all security based configuration settings for your system.

It includes:

- **User Password Parameters** — Configure user password complexity rules, including the ability to select three predefined options and custom rule configuration.
- **User Lockout Settings** — Define how many log in attempts a user may try before being locked out by the system. This setting dictates password attempts and security question attempts when resetting a password.
- **Session Settings** — Specify how long a user may remain inactive before being automatically logged out by the system.
- **Public Access** — Options to provide a Rev Guest Portal (log-in not required) and the ability to use public Webcasts and videos.
- **Sharing and Embedding** — Specify how and where videos may be shared and embedded on social media.
- **Single Sign On** — Use to set up a single sign on configuration in Rev as the SAML service provider when setting up an Enterprise SSO system.
- **User Location** — Specify Rev to point to the DME that will be able to obtain a user's IP address so that Rev may route the user to the appropriate zone defined in Rev.
- **Email to Suspended Users** — Enable to allow email to go to suspended user accounts.
- **DME Stream Authorization Lockdown** — Sets all DMEs to a lockdown state where playback of Live or VOD HLS assets requires Rev authorization.
- **Legal Hold** — Allows Rev videos to be placed into a Legal Hold status.
- **Login Messages** — Allows you to display a login message to users in various languages.

Configure Security Settings and Password Rules

User Password Parameters may be configured using three predefined rules included with your system; **Basic**, **Medium**, and **Strong**. You may also create your own **Custom** password rules if desired.

▼ To set a password rule:

1. Navigate to **Admin** > **System Settings** > **Security.**
2. Select a **Password Complexity Rule**.

3. **Password Complexity Rules** have three predefined formats:

   a. **Basic** — User is required to enter at least 8 characters when creating a password for his/her Account. This is the default setting.

   b. **Medium** — User is required to enter at least 8 characters when creating a password for his/her Account *and* the password must *also* contain 1 lower case letter, 1 upper case letter, and 1 number.

   c. **Strong** (not shown) — User is required to enter at least 12 characters when creating a password for his/her Account *and* the password must *also* contain 1 lower case letter, 1 upper case letter, 1 number, and 1 special character (!, %, ^, etc). Special characters may be any keyboard symbol other than a <space> or <enter> character.

4. Select the **Custom** checkbox to define a custom password rule. When **Custom** is selected, you choose the number of characters required as well as the specific type of characters that must be included, as seen below.

Reset a User's Password

Unlock a User's Account

Reset a User's Security Question

Reset Your Rev User Account Password or Security Question

Configure User Lockout Settings

User Lockout Settings define how many incorrect log in attempts are allowed by a user before he/she is locked out and the password must be reset.

When a password is being reset by the user through the **(Forget Password?)** hyperlink, he/she must answer the security question that was set up upon account creation. **User Lockout Settings** also dictate how many attempts to answer the security question may be answered

incorrectly before it must also be reset. You may also specify a lockout period of time and a time interval for locking out a user if desired or needed.
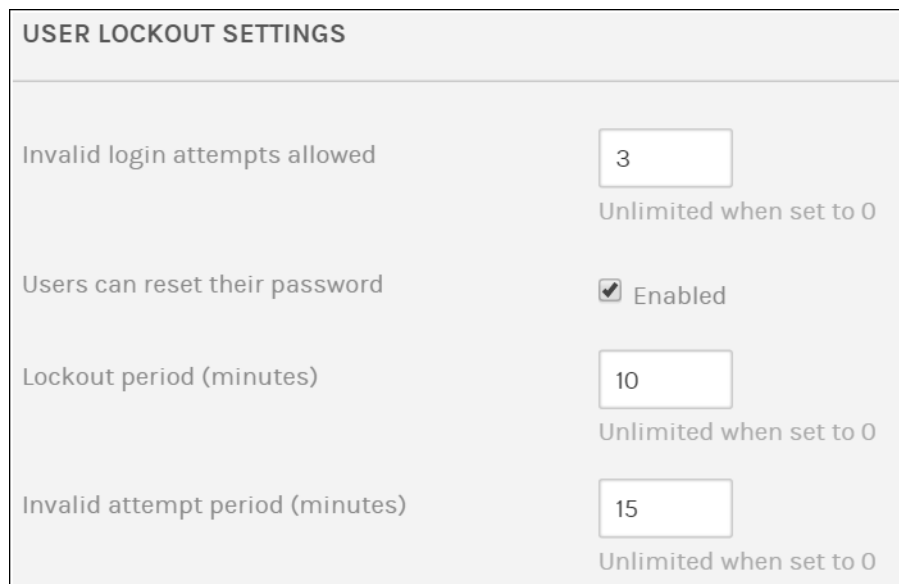
▼   To specify lockout settings:

1. Navigate to **Admin** > **System Settings** > **Security.**

2. Enter the number of times a user may enter the incorrect password or security question before being locked out in the **Invalid login attempts allowed** field.

    The default is five. Any number between 1 and 100 may be entered. If this field is set to 0, the user will never be locked out.

    If a user exceeds the number of attempts here, this message is displayed:

    "You reached the limit for incorrect login attempts. You must reset your password to access your account or contact your administrator."

USER LOCKOUT SETTINGS

Invalid login attempts allowed   3

                                      Unlimited when set to 0

Users can reset their password   ☑ Enabled

Lockout period (minutes)   10

                                      Unlimited when set to 0

Invalid attempt period (minutes)   15

                                      Unlimited when set to 0

3. Select **Locked users can reset their password** if users may reset their own passwords from the log in page (through the **Forgot Password?** hyperlink). Otherwise, an Admin will need to reset the password.

    When this link is selected, this message is displayed:

    "An email has been sent to your email address to reset your password. The email may take a few minutes to be received. If you do not receive an email, please contact your administrator."

4. Set the specified period of time that users are locked out if the password is entered incorrectly (using the invalid login attempts field value) in the **Lockout period (minutes)** field. In the image above, if the password is entered incorrectly 3 times, the user is locked out for 10 minutes before he/she will be able to try again. The default value is 0 which means there is no "waiting period".

> **Note**: If the user attempts to use the **Forgot Password** hyperlink during the **Lockout** period, no email message is received and the user will need to contact an Admin to unlock or reset the Password.
>
> If **Forgot Password** is used after the **Lockout** period, an email is received normally and the password can be reset without Admin assistance.
>
> As noted, if the **Lockout** period is set to 0, there is no **waiting period** and the email is sent immediately.

5. If you want the user locked out after the password is entered incorrectly (using the invalid login attempts field value) for a specified time interval, use the **Invalid attempt period (minutes)** field. In the image above, the user is locked out when the password is entered incorrectly three times within 15 minutes.

> **Tip**: Admins may reset a user's password by editing the user account.

Reset a User's Password

Unlock a User's Account

Reset a User's Security Question
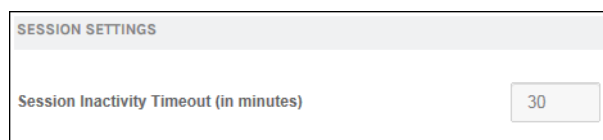
Reset Your Rev User Account Password or Security Question

Set Session Inactivity or Timeout Settings

Session Settings specify how long a user's session may remain inactive before they are logged out of the system automatically.

▼ To specify session settings:

1. Navigate to **Admin** > **System Settings** > **Security.**
2. Enter the number of minutes a user may remain inactive in **Session Inactivity Timeout (in minutes)**. The default setting is 30 minutes.
3. If a user is logged out due to inactivity, he/she will be returned to the login page with the message, "Your session has expired due to inactivity. Please log in again.".

Enable Public Webcasts

Rev allows the ability to create and host Public Webcasts. This means that a user need not authenticate or possess a Rev user account to view a Webcast. However, this functionality must first be enabled by a Rev Admin account in System Settings.

▼ To enable the ability to create Public Webcasts:

1. Navigate to **Admin** > **System Settings** > **Security**.

2. Scroll to the **Public Access** section and click the **Enable Public Webcasts** checkbox if not already selected.

3. If Public Webcast access is *not* enabled, this means that Event Admins and Hosts will *not* be able to set the event **Listing Type** to **Public** during set up. The tab will not be visible. See: Schedule a Public Webcast Event

4. Account Admins may also create custom registration fields to use with Public Webcasts. See: Add a Public Webcast Registration Field

Schedule a Public Webcast Event

Enable Guest Portal or Public Video Access

You can allow users to view videos from Rev without logging in to a Rev user account by enabling the **Guest Portal** and **Public Video Access** controls in System Settings. When enabled, user accounts with the ability to edit videos will have an additional **Public** option video access control in video settings. Shared links to videos marked as **Public** will not require a login to view the video.

Additionally, if the Guest Portal setting is enabled, users can be directed to the Rev Guest Portal URL, where they may view all active videos that have been designated with the **Public** option. Guest users will *not* have any access to any Rev menu functions with the exception of the **Search Media**, **Filters**, and **Sort** functions.

▼ To enable Public Video Access and the Rev Guest Portal:

1. Navigate to **Admin** > **System Settings** > **Security.**

2. Scroll to the **Public Access** section.

3. Select the **Enable Public Video Access** checkbox to enable the **Public** Access Control for videos in **Video Settings**. This will allow users to view the video through embedded means or through the Rev Guest Portal without logging in once they are designated Public.

4. Select the **Enable Guest Portal Access** checkbox to enable the Rev Guest Portal.

5. You may provide users the guest URL displayed under the checkbox for access to all videos that have been specified Public.

6. As noted, public visitors will have limited access and be able to view only those videos that are set to **Public** access and **Active** status and will *not* have access to any of the major menus or events.

7. If public video access is *not* enabled, users cannot set the access control for a video to **Public**. This prevents anyone from accessing a video in the system without logging in (embedded or otherwise) first and keeps videos secure.

> Tip: If a user sets a video's access control to Public, a password for guests may also be set. This password will be required before that individual video may be viewed through any public or embedded URL.

Set Video Access to Public

Enable Private Video Metadata Sharing

You can enable private video metadata sharing so that Rev video links shared on sites like Facebook, LinkedIn, and Twitter will render a thumbnail, title, and friendly description of the video. When you enable this setting, Rev modifies the HTML text in the 'Header' element to produce the enhanced link sharing.

▼ To enable private video metadata sharing:

1. Navigate to **Admin** > **System Settings** > **Security**.

2. Select the **Allow Sharing of Metadata for Private Videos** checkbox under **Sharing and Embedding** to enable enhanced link sharing.

3. Specify which social sites returning metadata that Rev will accept by entering a valid User Agent bot (as seen in the image above) in the **Recognized User Agents** form.
   - See the following links if you need further suggestions on how to obtain and/or formulate these:
   a. https://oembed.com/
   b. http://ogp.me/
4. Now when you Share a Video on external social sites like Facebook, LinkedIn, and Twitter a thumbnail, title, and friendly description of the video will be displayed.

> **Note**: Enabling this feature also populates the thumbnails for Private videos that are embedded in other Websites for users that are not logged in.

Share a Video

Embed a Video

Configure Single Sign On (SSO)

Rev provides Single Sign On (SSO) functionality via the SAML 2.0 protocol. Use the **Single Sign On** section in **System Settings** to configure Rev as the SAML Service Provider if you are using an Enterprise SSO system set up and want to configure it for use with your enterprise Identity Provider server. You should be familiar with SAML and SSO deployment methods before attempting to configure the fields below.

A good, high level overview may be reviewed on the Eclipse open source SAML2 wiki page.

> **Note**: Rev also provides Single Sign On (SSO) with user provisioning so that user accounts may be created upon log-in without the need for an LDAP connector deployment. See: Configure Single Sign On (SSO) with User Provisioning Enabled.
>
> User provisioning must be enabled on the root account by Vbrick Support Services before this feature may be used.

▼ To configure single sign on in Rev:

1. Navigate to **Admin** > **System Settings** > **Security**.
2. Select **Enable Single Sign On** checkbox under **Single Sign On** section.
3. Complete the fields below as necessary.

Field Name	Required	Description
Enable Single Sign On	Yes	Select to enable SSO in Rev.
Identity Provider Metadata	Yes	Paste your Identity Provider server's metadata XML code in this field. You will need to obtain the Identity Provider metadata (XML) from your Identity Provider server.
SAML Identity Location		Choose either the **NameIdentifier Element** or **Attribute Element** depending upon which element in the SAML Authentication Response will have the username.
		Note that if you select **Attribute Element** (default), you must provide the **Identify Attribute Element Name** or Rev will not authenticate.

Field Name	Required	Description
Identity Attribute Element Name	Yes	If **Attribute Element** is selected as the **SAML Identity Location**, this field *must* be completed or SSO will not work. The **Identity Attribute Element Name** is the field in the SAML Authentication Response (XML) that will contain the username. For example, in the code below, name is specified as SFDC_USERNAME. This is what would be pasted in **Identify Attribute Element Name** field in Rev, as seen in the image above. ``` <saml:AttributeStatement> <saml:Attribute FriendlyName="fooAttrib" Name="SFDC_USERNAME" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname- format:unspecified"> <saml:AttributeValue xmlns:xs="http:// www.w3.org/2001/XMLSchema" xmlns:xsi="http:// www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string"> user101@salesforce.com </saml:AttributeValue> </saml:Attribute> </saml:AttributeStatement> ```
Signature Algorithm	Yes	Options to be used for signing. Select either SHA1withRSA or SHA256withRSA.
Sign SAML Request		Only enabled when the URL of the redirect exceeds 2048 characters which may occasionally cause issues with Internet Explorer or IIS/ADFS. Be aware that checking and un-checking this box will require the service provider metadata be re-downloaded to get the latest version again once saved. Contact Vbrick Support Services for assistance with this option.
Download Service Provider MetaData		This is the Rev Service Provider XML metadata that is provided to the Identity Provider server. It should be downloaded and used with the IDP server similar to how the IDP's metadata XML is pasted in the **Identity Provider Metadata** field above.
Regenerate Cert		This will regenerate the Service Provider's certificate and metadata. If you decide to do this, keep in mind you will need to download the Service Provider MetaData again for re-insertion into the IDP server.

The diagram below represents the technical implementation of SSO in Rev.
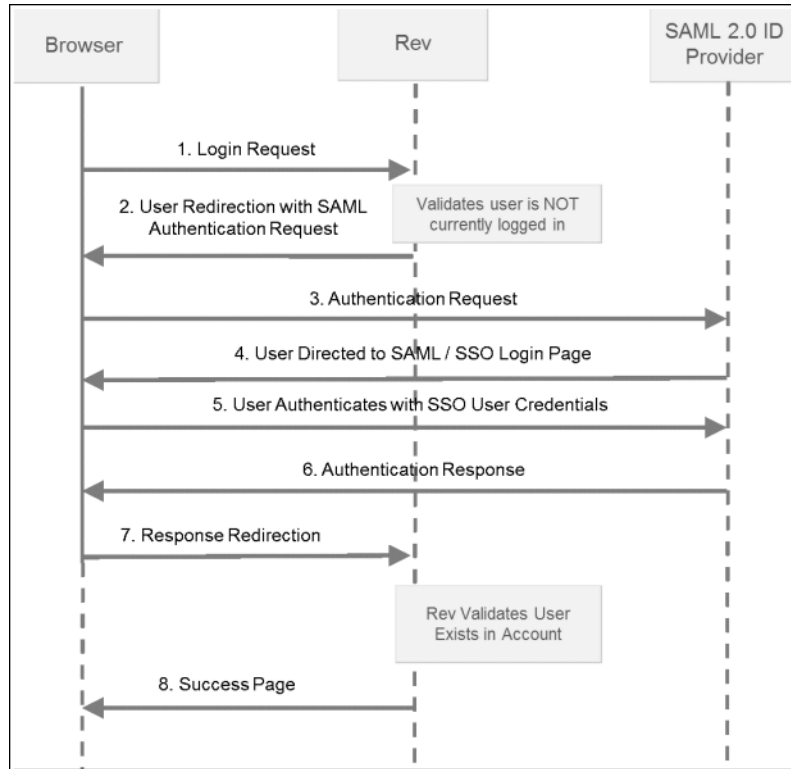
Keep in mind:

- If SSO is enabled without user provisioning, user accounts must be created in Rev manually or through the LDAP connector. See: Configure Single Sign On (SSO) with User Provisioning Enabled.

- If an admin creates a user account manually with SSO enabled, the user created is set to "Unlicensed" until log in and then set to "Active". No user or email confirmation is required. If no licenses are available for the Rev account, the user will be displayed a message to contact the Account Admin and will not be logged in.

- When SSO is enabled, an SSO login page is created for authentication that is different from the native Rev login page. For example:
  - Rev Native Login Page: `http://<RevURL>/#/login`
  - SSO Login Page: `http://<RevURL>/SSO/login`

Add or Edit a User Account

Upload and Edit User Accounts and Groups Using a CSV File

Configure Single Sign On (SSO) with User Provisioning Enabled

Configure Single Sign On (SSO) with User Provisioning Enabled

Rev also provides Single Sign On (SSO) with user provisioning so that user accounts may be created upon log-in without the need for an LDAP connector deployment.

In this case, SSO is configured exactly as described in the Configure Single Sign On (SSO) topic with additional Identity Server provider fields to map to Rev fields for user account creation, which are described below.

> **Note**: User provisioning must be enabled on the root account by Vbrick Support Services before this feature is enabled and before you may configure SSO with user provisioning.
>
> You can check if user provisioning has been enabled on your Account form. See: View Contact and Billing Information for an Account

▼ To configure SSO with user provisioning in Rev:

1. Navigate to **Admin** > **System Settings** > **Security.**

2. Select **Enable Single Sign On** checkbox under **Single Sign On** section.

3. Make sure that **User Provisioning** has been selected. If not, contact Vbrick Support Services.

4. Complete the fields below as necessary.

Field Name	Required	Description
Enable Single Sign On	Yes	Select to enable SSO in Rev.
User Provisioning	Yes	Will be enabled by Vbrick. Not user configured.

Field Name	Required	Description
SAML Identity Location		Choose either the **NameIdentifier Element** or **Attribute Element** depending upon which element in the SAML Authentication Response will have the username. Note that if you select **Attribute Element** (default), you must provide the **Identify Attribute Element Name** or Rev will not authenticate.

Identity Attribute Element Name	Yes	If **Attribute Element** is selected as the **SAML Identity Location**, this field *must* be completed or SSO will not work.
		
		The **Identity Attribute Element Name** is the field in the SAML Authentication Response (XML) that will contain the username.
		
		For example, in the code below, name is specified as SFDC_USERNAME. This is what would be pasted in **Identify Attribute Element Name** field in Rev, as seen in the image above.
		
		`<saml:AttributeStatement>`
		`    <saml:Attribute FriendlyName="fooAttrib"`
		`Name="SFDC_USERNAME"`
		`NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">`
		`        <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">`
		`            user101@salesforce.com`
		`        </saml:AttributeValue>`
		`    </saml:Attribute>`
		` </saml:AttributeStatement>`

First Name Attribute Element Name		The first name of the user account.
Last Name Attribute Element Name	Yes	The last name of the user account. Similar to Identity Attribute Element Name above, this is a required field and must be completed in order to authenticate correctly.
Email Attribute Element Name	Yes	The email of the user account. Similar to Identity Attribute Element Name above, this is a required field and must be completed in order to authenticate correctly. Correct email format must also be used and the field must be unique.
Title Attribute Element Name		The title of the user account.
Phone Attribute Element Name		The phone number of the user account.

Field Name	Required	Description
Identity Provider Metadata	Yes	Paste your Identity Provider server's metadata XML code in this field. You will need to obtain the Identity Provider metadata (XML) from your Identity Provider server.
Signature Algorithm	Yes	Options to be used for signing. Select either SHA1withRSA or SHA256withRSA.
Sign SAML Request		Only enabled when the URL of the redirect exceeds 2048 characters which may occasionally cause issues with Internet Explorer or IIS/ADFS. Be aware that checking and un-checking this box will require the service provider metadata be re-downloaded to get the latest version again once saved. Contact Vbrick Support Services for assistance with this option.
Download Service Provider MetaData		This is the Rev Service Provider XML metadata that is provided to the Identity Provider server. It should be downloaded and used with the IDP server similar to how the IDP's metadata XML is pasted in the **Identity Provider Metadata** field above.
Regenerate Cert		This will regenerate the Service Provider's certificate and metadata. If you decide to do this, keep in mind you will need to download the Service Provider MetaData again for re-insertion into the IDP server.

Keep in mind:

- If SSO is enabled without user provisioning, user accounts need to be created in Rev manually or through an LDAP connector. See: Configure Single Sign On (SSO).

- If an admin creates a user account manually and SSO with user provisioning is enabled, the user created is set to "Unlicensed" until log in and then set to "Active". No user or email confirmation is required. If no licenses are available for the Rev account, the user will be displayed a message to contact the Account Admin and will not be logged in.

- When SSO is enabled, an SSO login page is created for authentication that is different from the native Rev login page. For example:

  - Rev Native Login Page: `http://<RevURL>/#/login`
  - SSO Login Page: `http://<RevURL>/SSO/login`

Add or Edit a User Account

Upload and Edit User Accounts and Groups Using a CSV File

Configure Single Sign On (SSO)

The DME User Location Service

Zone logic in Rev depends on routing users to the correct zone and closest DME to ensure optimal video distribution. This is critical for both live and Video on Demand (VOD). Consider, for example, the distribution of video across organizations with hundreds of DMEs, serving thousands of viewers. Viewing from the closest DME is paramount.

To facilitate zone logic and routing, you must designate at least one "location services" DME with the DME Location Service in Rev. The location services DME will validate a user's location and be used by zone logic. For this reason, you must make sure that the DME that is specified is accessible to all Rev users behind the firewall

Keep in mind:

• As noted, the location services DME must be accessible to all Rev users behind the firewall.

• In the event that the location services DME is not accessible, you may designate an optional secondary USL URL.

• Additional security steps must be followed based on if you are using "Cloud hosted Rev" versus "On Premise Rev". Each method will be explained below.

• If you are unfamiliar with zone logic, see the Zone Logic and Hierarchy topic before proceeding.

Cloud Hosted Rev

Vbrick is dedicated to ensuring security for cloud hosted Rev instances which means that all communications are encrypted over SSL/TLS connections - thus protecting communication from the customer site to the cloud. This also means that customer security certificates (certs) are necessary for the DME supporting location services specified in Rev.

▼ To specify a location services DME in cloud hosted Rev:

1. Make sure that the DME has a customer cert installed. See: *DME Admin Manual* > "SSL Certificates" topic.

2. Navigate to **Admin** > **System Settings** > **Security.**

3. Select the **Enabled** checkbox for **Validate User Location** under the **User Location** section.

4. Enter a valid DME URL in the **User Location Service URL** field. This must be the DME's fully qualified domain name. Alternatively, this may also point to a load balancer that will then point to specific DMEs on your network.

   For example, a valid URL might be: **https://mydmename.mycompany.com/cgi-bin/ localip.cgi**

   Where **mydmename** is the DME hostname, and **mycompany.com** is the enterprise domain.

5. You may enter a secondary URL in the **Secondary User Location Service URL** field if desired. This DME is used in the event the first DME is not available.

6. Click the **Test** button next to either field to verify that the server(s) are available and retrieving IP addresses correctly.

7. When a user plays a video or logs into Rev, the system will validate the user's location through the Location Service and direct the user to the correct zone.

8. The user's location is cached for the remainder of the session.

On Premise Rev

To specify a location services DME in an on premise Rev installation, the exact steps described in cloud hosted Rev are followed with the following exception:

- A DME customer cert does *not* need to be installed (described in step 1) unless you are using https. If you *are* using https, you will need to install a cert and follow the exact steps described above even if using on premise Rev.

Add a Zone

Zone Logic and Hierarchy

Suppress System Email Messages to Suspended User Accounts

Admins can decide if suspended user accounts will receive system email messages. By default, suspended accounts receive all system generated email.

▼ To disable suspended user accounts from receiving system emails:

1. Navigate to Admin > System Settings > Security.
2. Deselect the **Enabled** checkbox in the **Email to Suspended Users** section.
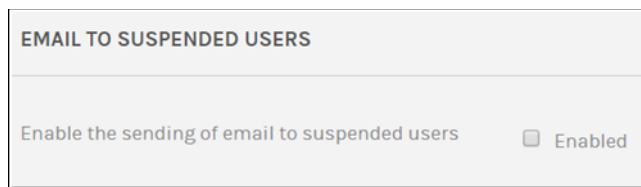
When disabled, suspended accounts will no longer receive email for the following:
- security settings
- video approval notifications
- video comment added notifications
- video expiration notifications
- video publishing notifications
- report a video notifications
- license expiration notifications
- device download video file action notifications
- device status change notifications
- video processed notifications
- LDAP notifications

System Emails

Enable DME Stream Authorization Lockdown

Enable this setting to place all DMEs to a lockdown state where playback of Live or VOD HLS assets requires Rev authorization. Rev automatically provides authorization encoded

into the playback URLs. Admins may put their entire systems into and out of this lockdown state as needed or required.

> **Important Note**:
>
> All deployed DMEs *must* be on version 3.21.x (or later). DMEs on previous versions are *not* used for content distribution. Best Practice is to update all your DMEs before attempting to use this feature.
>
> This feature requires the use of 3rd party cookies within the browser. Please be aware that some browsers restrict this feature by default which requires user or IT Support intervention to change the default.

▼ <u>**Before**</u> you enable this feature, complete the following steps:

1. Make sure all DMEs are updated to version 3.21.x or later. DMEs that are on previous versions may corrupt the ability of the Stream Authorization feature.

2. For distribution, make sure all of your DMEs are "Pushing" streams from DME to DME when Stream Authorization is enabled.

   As part of the DME Stream Authorization feature, DMEs will no longer serve RTMP, RTSP, or TS. Any DME that is actively "Pulling" an RTMP / RTSP / or TS from another DME will fail. DMEs may still continue to "Push" RTMP / RTSP / TS to other DMEs.

   For example, DME-1 is pulling RTMP-Stream2 from DME-2. When Stream Authorization is enabled, that pull will fail. DME-2 will need to be reconfigured to "Push" RTMP-Stream2 to DME-1 in order to get the stream on DME-1.

3. Configure your Recording DMEs for Stream Authorization.

   Rev currently supports two Recording DMEs. Streams that need to be recorded must be native on the Recording DME (they cannot be "Pulled"). Make sure all streams that need to be recorded are "Pushed" (from origin) to the Recording DMEs. Recording will fail if the stream is not provisioned to the recording DME.

4. If you are utilizing a DME for the **Rev** > **System Settings** > **User Location** feature, confirm that the DME URL is using https (per recommendations suggested at <u>The DME User Location Service</u> help topic).

5. Once you have completed all the preceding steps, you are ready to enable DME Stream Authorization.

▼ To enable DME Stream Authorization Lockdown:

1. Navigate to Admin > System Settings > Security.

2. Select the **Enabled** checkbox in the **DME Stream Authorization Lockdown** section. Note: If this section is not visible, contact Vbrick Customer Support to review availability.
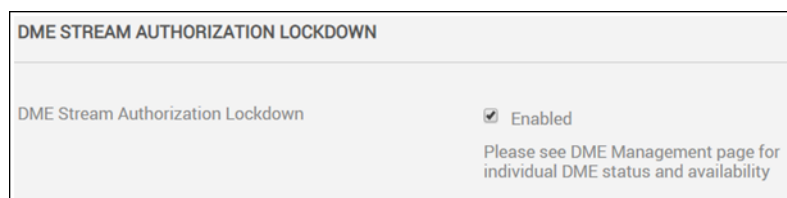
3. When enabling (or disabling) this feature, Rev directs each DME to change its Stream Authorization state. There are several configuration items that are necessary for a DME to enter this state including enabling NTP services, forcing HTTPS content sharing, and validating the DME's Security Cert. If these are not set correctly, the DME will not be

used to distribute content which means that Rev will not point users to that DME for content playback. See: <u>DME Stream Authorization Lockdown Management</u> for details.

4. It may take several moments for the DMEs to report back a successful lockdown status. Status state can always be reviewed on the <u>DME Management</u> and <u>DME Network Statistics</u> page(s).

5. Test fully. Test DME configured distribution and make sure your streams are propagating through the system correctly with Pushes. Test that your Recordings are happening for all necessary streams.

Keep in mind:

• Only authorized viewers will be able to see a particular video asset once enabled

• Streams will be authorized on a per-user, public, or all users level

• Individual levels will receive individual tokens to thwart sharing

• This setting is disabled by default

> **Note**: Once enabled, view the <u>DME Management</u> page for the status of individual DMEs and authentication settings.

> **Caution**: This setting is not recommended during events or high system usage.

<u>DME Stream Authorization Lockdown Management</u>

<u>DME Management</u>

<u>DME Network Statistics</u>

Enable Legal Hold Functionality

Admins can decide if account Admins will have the ability to place a legal hold on one or more videos at a time in Rev. To do this, the legal hold functionality in Rev will need to be enabled system wide first.

▼ To enable the legal hold functionality:

1. Navigate to Admin > System Settings > Security.

2. Select the **Enabled** checkbox in the **Legal Hold** section.

When enabled:

• The **Apply Legal Hold** option appears under **Video Settings** so that a legal hold may be applied to an individual video. This is visible to account admins only.

When disabled:

• The **Apply Legal Hold** option is removed from **Video Settings**.

• Removes legal hold from all videos where it was previously applied while keeping their status inactive.

- For videos currently in an approval process, the approval process starts again with the first approver needing to re-approve.
- An email is sent to all account admin that the **Legal Hold** functionality has been disabled and details which videos have been affected.

Apply or Remove a Legal Hold from an Individual Video

Bulk Editing Legal Hold Status on Multiple Videos

Create a System Login Message

System Admins in Rev may create a system login message that may be used to create messages that user accounts see when they log in to Rev so that messages such as Terms of Service may be created and updated when needed. When a system login message is created, the user must accept that they have seen the message the first session they log in after the message is created (or updated) by the admin. Each successive session after that, the message will no longer be viewed unless the admin resets the message.

▼   To create a system login message:

1. Navigate to Admin > System Settings > Security.
2. Enter the login message you want to use in the **Login Messages** section.
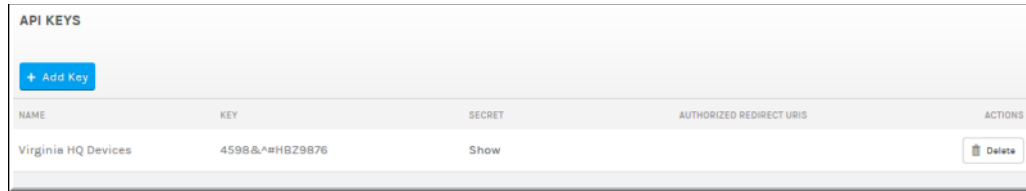
3. Click **Save**.
4. All users will be forced to acknowledge your login message upon their next login.

5. The message will not be viewed again until the **Reset** button is pushed in the event the message is updated and you need your users to view and accept the message again.

The API Keys Module

The **API Keys** module displays the API keys used with Vbrick Rev and system devices.

Rev API code examples are found on the <u>Vbrick Rev Swagger Site</u>. API versioning is detailed and maintained on the documentation site under the <u>Rev API</u> section.

The API Keys module displays:

- **Name** — The user created name of the API key.
- **Key** — The user created key that will connect a device with Vbrick Rev.
- **Secret** — The secret that is generated when a key is created; used in conjunction with Rev's REST authorization API. See the Rev REST API Online help in the Rev <u>Documentation</u> area. Click the **Show** hyperlink to display a specific key's **Secret**.
- **Actions** — Actions you may perform on the API keys in use.

<u>Add an API Key</u>
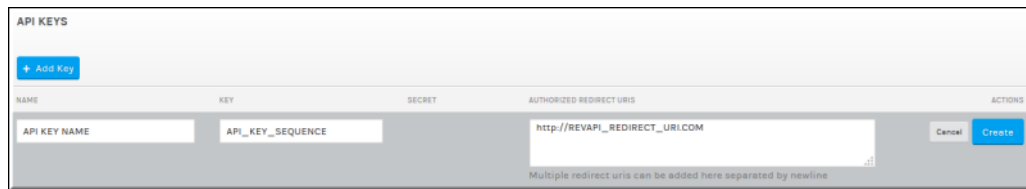
Add an API Key

API Keys are created and added to Vbrick Rev for linking devices for use with Rev. You *must* create an API key for each type of device you plan to use with Rev, including LDAP Connectors. Once the API key is created, enter the key in the Rev API field of its corresponding device before you add the device in the **Device** module in Rev.

> **Additional Information**: See the <u>Device Initial Configuration and Set Up</u> topic for more information on how to set up devices.

▼ To add an API key:

1. Navigate to **Admin** > **System Settings** > **API Keys** > **Add Key** button.

2. Enter a descriptive **API Key Name**.
3. Enter the **API Key**. You may use any combination of letters and numbers of your choice.

Caution: It is *highly* recommended that symbols and special characters are *not* used in the API key field.

Note: While an API Key is required for every device created in Rev, you do not have to create separate API Keys for each device. This is a distinction that is often overlooked.

For example, you may create one API Key that is used for each location you have, such as headquarters (or the United States), and then use that same API Key for each device in that location if that is your preference. Then you may create a different API Key for a location in the UK or training rooms and use that key for the devices in only those locations.

4. Enter any redirect URIs needed if you plan to use any integrations and the OAuth API. This field is checked that the redirect URIs specified in the authorization and token request match and provides an additional security check to ensure that the correct user is making the request. Multiple URIs may be provided but at least one must match the authorization request to be redirected.

5. Click **Create**.

6. Use this same key in the device you plan to add and link to Rev for use. See the corresponding device's Admin technical manual for more information on where to enter this key.

Return to the main API module to display the API's **Secret** that is generated (for use with Rev's REST authorization API) if needed.

Add a Distributed Media Engine (DME)

Add a Distributed Media Engine (DME)

View the Status of a Device

Configure and Import LDAP Groups in Vbrick Rev

The Encryption Key Management Module

The **Key Management** module provides the ability to activate a new Master Key and also maintains a **History of Master Key Rotations**.

Note: In order to use this feature, a waiver must be on file with Vbrick.
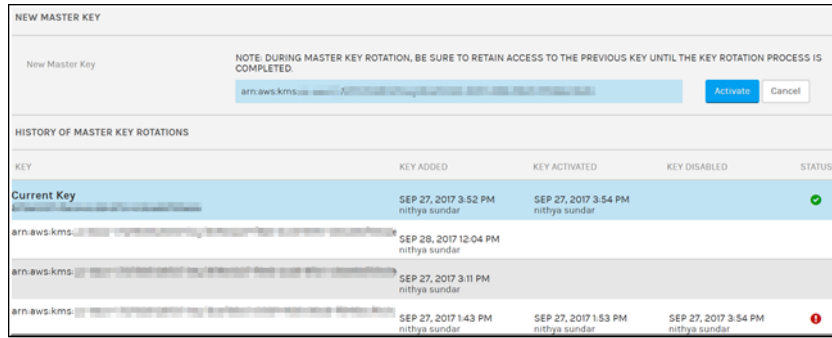
The Key Management module displays:

- **Key** — The current Master Key and all previous keys used. Note: The actual Master Encryption Key is not stored in Rev.
- **Key Added** — The date each key was added and the user name that added the key.
- **Key Activated** — The date each key was activated and the user name that activated the key.
- **Key Disabled** — The date each key was disabled and the user name that disabled the key.
- **Status** — They key's status. The number of files that failed encryption will be noted here.

Add a Master Key

Add a Master Key

Adding a Master Key transfers complete ownership of encryption keys to you allowing you to own, manage, and control access to all of your assets independently of Vbrick through Rev's use of the Amazon Web Service (AWS) S3 Key Management Service. You have the assurance of knowing that you retain complete control of your video assets, even when they are in the cloud. Further, Rev keeps track of Master Key rotations so that you are fully aware of past key history and usage.

> Note: The actual Master Encryption Key is not stored in Rev. In order to use this feature, a waiver must be on file with Vbrick.

▼ To activate a Master Key:

1. Navigate to **Admin** > **System Settings** > **Key Management**.
2. Enter a new Master Key in the **New Master Key** field.
3. Click the **Activate** button.
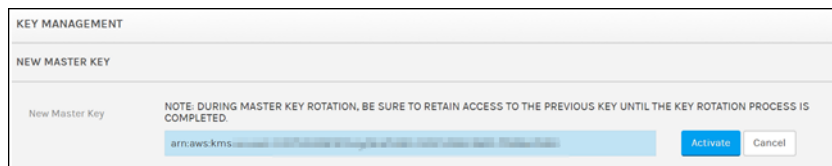
> Caution: If you are replacing a Master Key, be sure to retain access to your previous Master Key until the key rotation process is complete.

4. As noted, previous Master Keys used are detailed below the **Current Key** in use.

The Encryption Key Management Module

Customize and Brand a Rev Portal

Rev's **Branding** menu allows you to turn your entity into a true video portal styled with your organization's logo, colors, and font preferences. You can choose different themes and designs for your landing page to ensure your portal is a true reflection of your organization's style. This section of help details the designs, colors, and formatting options that are available to you using Rev's branding features.

See the Rev style guide on the Vbrick Documentation portal for details on all the colors and fonts available to you and how they are applied.

Note: You must be an Account Admin to use Rev's Branding functions.
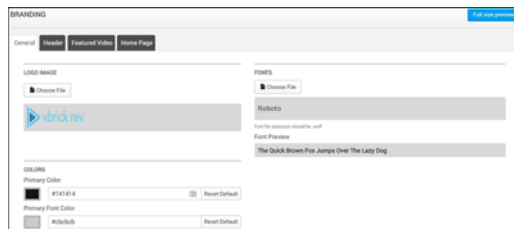
Anatomy of the Home Page

The **Home Page** is displayed when a user first logs in. Rev considers the **Home Page** comprised of three parts:

- Header
- Featured Video carousel
- Home Page carousels (Default carousel options are Recently Added Videos, Live Videos, Upcoming Events)

You can customize the **Header**, **Featured Video**, and carousel branding displayed on the **Home Page** by choosing templates as part of Rev's **Branding** menu.

There are four tabs under Rev's **Branding** menu to assist you when branding your Rev portal; **General**, **Header**, **Featured Video**, and **Home Page**. Making selections under each tab will maximize your ability to showcase your organization's brand when setting up your Rev portal.

The Home Page

Use a Custom Logo for Your Rev Portal

A custom logo may be used to replace the Vbrick logo in the upper left corner of the user interface so that you may brand your Rev portal with your own logo and colors. If you change the logo, system email templates will also be branded with the customized logo you use. Otherwise, the default Rev logo will be used.

▼ To use a custom logo:

1. Navigate to Admin > System Settings > Branding > General tab.

2. Click the **Choose File** button in the **Logo Image** section.

3. Select an image to load from your local drive. Keep in mind:
    *   The image may be in .jpg, .png, or .gif format
    *   You may upload a logo of any size, however, there are recommended sizes based on the Header template you use. Specifically:

> **Classic** - Maximum height recommended is 50 pixels
> **Two Tier** - Maximum height recommended is 75 pixels
> **Modern** - Maximum height recommended is 75 pixels

4. Click the **Full Size Preview** button if you want to preview your logo before saving it.

5. Click the **Reset Default** button to return to the Rev logo.

6. Click the **Save** button to apply your logo.

7. If a custom logo is not used, the default Rev logo will continue to be used in the system and in all generated HTML emails.

Customize Rev Primary and Accent Portal Colors

Use the **Colors** section to specify Primary and Accent colors for the portal and fonts. The default color of each section is demonstrated in the image below.
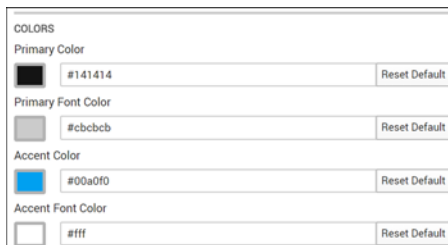
*   **Primary Color:** Background color of all inner pages with the exception of the Header and Featured Video.
*   **Primary Font Color:** The font color of all inner pages (upcoming release).
*   **Accent Color:** Taken mainly from the company's main branding color (for example, if your organization's main branding is blue, the accent color will be blue)
*   **Accent Font Color:** Remaining font colors *not* on inner pages

▼ To modify a custom color:

1. Navigate to Admin > System Settings > Branding > General tab.

2. Click the color picker next to the color you want to modify. You may also enter a Hexadecimal value.

3. Click the **Full Size Preview** button to preview your changes.

4. Click the **Save** button to apply the new color.

5. Click the **Reset Default** button to revert back to the default colors of Rev.

Customize Rev Portal Fonts

Rev's default font for the portal is Roboto. You may modify this and upload your own fonts to use so long as they have the Web Open Font Format (.woff) extension.

▼ To use a custom secondary color:

1. Navigate to Admin > System Settings > Branding > General tab.
2. Click the **Choose File** button to select a new font to upload.

3. Click the **Full Size Preview** button to preview your changes.
4. Click the **Save** button to apply the new color.
5. Click the **Reset Default** button to revert back to the default colors of Rev.

Customize the Rev Portal Header

You can change the Rev Header on your portal by modifying its colors and the template from the classic Rev template to a two-tiered or modern look and feel. Remember that based on which header template you select, there is a recommended logo size to use with it. See: Use a Custom Logo for Your Rev Portal.

▼ To use a custom Header for Rev:

1. Navigate to Admin > System Settings > Branding > Header tab.
2. Use the **Header Color** section to modify the background and font color.

3. Click the color picker next to the color you want to modify. You may also enter a Hexadecimal value. The colors applied here *only* apply to the header of the portal.
4. Click the **Full Size Preview** button to preview your changes.
5. Click the **Save** button to apply the new color.
6. Click the **Reset Default** button to revert back to the default colors of the header.
7. Use the **Header Template** section to modify the Header's style and UI.

8. The **Classic** template is the default style.
9. Each style is previewed next to its template. However, you may also click the **Full Size Preview** button to preview the template before clicking the **Save** button and applying your changes.

10. Depending on which Header template you use, various default colors and recommended logo size dimensions are used. These are described below.

Classic Header Template

The default header template in Rev. This is the header that is used until it is changed by an admin.

Two Tier Header Template

This header is a two tiered or layered header that splits the menu options into a separate layer from the logo, search, upload, and notification icon layer. When this template is used, the next upcoming event is also displayed in the center of the header.
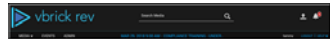
Modern Header Template

This header features a flyout menu dropdown on the left and places the logo in the center giving it a mobile, modern appearance.

Customize the Featured Video Playlist Template

You can change the Rev **Featured Video** template on your portal from its default classic style. Depending on the template you use, different options are available for customization.

▼   To modify the Featured Video template:

1. Navigate to Admin > System Settings > Branding > Featured Video tab.
2. Select between the **Classic**, **Poster Carousel**, and **Tiles** templates. The options for each are explained below.

Featured Video Classic Template

The default **Featured Video** template in Rev until it is changed by an admin. There are no limits to the amount of videos that may be used in the Featured Video playlist when using this template.

There are two selections that must be made when you choose the Classic template:

• Banner Background
• Auto Scroll (on or off)

The **Banner Background** for the **Classic** template may be a color or an image.
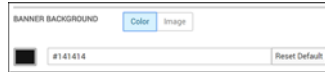
- The default color is #141414 (black).
- If you select **Image** as your **Banner Background**, an image that is at least 1600 pixels wide by 1200 pixels high (no larger than 2mb) is required.
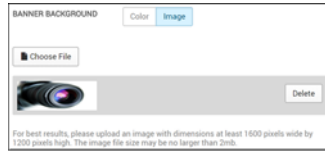
- The image selected will only appear across the **Featured Video** on the **Home Page**.
- You must also decide if **Auto Scroll** is on or off. By default, this setting is off. If you elect to turn Auto Scroll on, you must enter a number between 1 and 10. This will be the number of seconds each video in the Featured Playlist is on the screen before it auto scrolls to the next video in the playlist. If auto scroll is off, the user must manually click the next arrow to view the next video.

- As with all template selections in branding, you may click the **Full Size Preview** button to preview your selection before you click the **Save** button to apply it on the portal.

Featured Video Poster Carousel Template

This template features a full screen "poster" version of each video's thumbnail as the background along with the video title and a **Watch Now** button. There are no limits to the amount of videos that may be used in the Featured Video playlist when using this template.

There is one selection that must be made when you choose the Poster Carousel template:

- Autoscroll

Just as with the **Classic** template above, you must decide if **Auto Scroll** is on or off. By default, this setting is off for the **Poster Carousel** template as well. If you elect to turn Auto Scroll on, you must enter a number between 1 and 10. This will be the number of seconds each video in the Featured Playlist is on the screen before it auto scrolls to the next video in the playlist. If auto scroll is off, the user must manually click the next arrow to view the next video.

Featured Video Tiles Template

There are no additional settings that must be made when you choose the **Tiles** template for the Featured Video playlist. You may modify what appears here by re-ordering the Playlist itself. If more than five videos are in the playlist, *only* the first 5 are used.

See: Create a Featured Playlist and Upload a Custom Thumbnail for a Video if you need a refresher on how to do this.

Customize and Add Additional Help Links to Rev

You may specify additional help links for Rev and customize the default help link for Rev as well if you want to include your own branded help topics for your organization. You may link to an email address or a URL as needed.

▼ To use customize and add help links:

1. Navigate to Admin > System Settings > Branding. > Header

2. Click in the **Customize Default Help Link** field to modify the default Rev help URL. Note that you will no longer be linked to Rev's default (and official version) of Help if you modify this URL. If you still want to be able to view the default Rev Help and add your own help settings, add your own additional help links instead.

3. Add additional help links by clicking the **Additional Help Links** drop-down and specifying whether you want to add either an **Email Address** or **URL**. Enter a description and then where the link will branch to or email address.

4. Click the **Reset Default** button once you have updated the URL if you want to reset the URL.

5. Click **Save** to apply your updates.

6. Click the **Add Help Link** button if you need more options.

7. Once saved, clicking the **Help** button in Rev will now display the description(s) you added. The default Help link will branch either to the default Rev Help as usual or, if you modified it, to your new customized Help link. The additional new options will either branch to the new URLs or pull up an email window to email the email address you added.
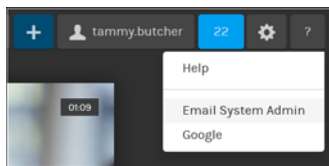
Customize the Home Page Template and Carousels

You can tailor the **Home Page** settings on your Rev portal by specifying branding options and the number of carousels that appear along with the content of each.

Up to seven carousels may be configured to appear on the **Home Page**. By default, the carousels are displayed as follows:

- Recently Added Videos
- Live Videos

- Upcoming Events
- Category
- Channels List (Displays the Channels the user is a member of, if applicable. No Channel is displayed if the user is not a member of a Channel.)
- Continue Watching (Includes videos that have only been partially viewed. Those videos that have been completely viewed are not displayed)
- In addition to the default options above, you may also set carousels to display:
  a. Channel Videos: Displays all the videos of the selected Channel. You may select multiple Channel Video carousels to display on the Home Page if desired.
  b. Playlist: All playlists you create and the Featured Playlist are available to select here.
  c. Recommended for You: Displays video recommendations based on popularity, freshness, and the user's viewing history.
- You may also select **None** and the carousel will not display as a result.

> **Note**: Be aware that the **Access Control** level of the videos in the selected carousel are in effect. In other words, if you add a **Private** video to a carousel, some users may not be able to view it based on their permissions/ access.

▼ To customize the Home Page:

1. Navigate to Admin > System Settings > Branding > Home Page tab.
2. Select between the **Classic** or **Carousels With Sidebar** templates for your Home Page. Each template is explained below.
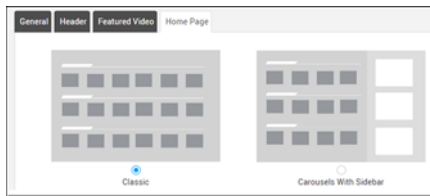
3. The carousels display in the order you select on the template. To disable the carousel, select **None**.
4. To select a category, select **Category** and begin typing the category name until it appears. Only videos that are assigned to that category will appear in the carousel.
5. Click **Save** to save your template customizations.

Keep the following in mind:
- The carousel is always required and may not be set to None.
- The same value may not be set in more than one carousel.
- The same category or channel may not be selected for multiple carousels.
- Carousel videos are sorted based on the user's viewing history first and then by videos that are more popular and recently uploaded. For complete details on how relevancy and sorting works in Rev, view the Search Media and Video Content topic.
- If Continue Watching is set as a carousel, and a video is accessed as a direct link (rather than the carousel), keep in mind that the progress will not be displayed as opposed to if it is accessed via the Continue Watching carousel.

> **Note**: If the **Add URLs** option has been disabled in **Media Settings**, you will not be able to add a **Live Videos** carousel as a **Home Page** setting.

Classic Template

The default carousel template on a **Home Page** until changed by an Admin. You may display up to seven carousels that will appear under the **Featured Video**.

Carousels With Sidebar Template

When this Home Page carousel template is selected, you must select three sidebar sections in addition to your carousels. Sidebar sections appear to the right of your carousels and under your **Featured Video**, demonstrated in the image below.

The sidebar selections that may be made are:

• Events (Upcoming events specific to the logged in user's permission levels)

• Channels (Specific to the logged in user's channels only)

• Categories (Top level category display only if categories are enabled)

• None (no sidebar will be displayed)

The first **Home Page Sidebar** dropdown is required and may not be set to None similar to the first carousel option.

The Home Page

Enable Add Video via URL Option

Manage Custom Fields in Rev

The **Custom Fields** module is only visible to Account Admins. This module provides the ability to create, edit, and delete fields in Rev that are specific to your organization only. You can then add them to videos and Webcasts to collect that information from viewers.

> **Note**: If you create either a Video or Webcast template with custom fields they will be saved as part of the template.

Configure Custom Fields

Custom fields can be configured to appear within Video Settings and public Webcast registrations. Custom fields display on the Rev interface just as default fields do if visibility is enabled. You may also specify if they are required when settings are completed for a video upload or during Webcast registration. Searching and bulk edits may be performed on custom fields as well.

Add a Custom Field

▼ To add a custom fields:

1. Navigate to **Admin** > **System Settings** > **Custom Fields**.
2. Click the **Add Custom Field** button.

Field Name	Required	Description
Name	Yes	The name of the custom field. This will be the label displayed to users. This is a required field and must be unique to the account.
Type	Yes	The type of field you are adding. You may add a custom text field or a pick list where the user may choose from a list of items that you create. This is required.
Required		Default = No. This field determines whether the custom field must be populated by the user when editing video settings.
Public Display		Default = Yes. This field determines whether or not the custom field is visible to users that are not editing the video settings.
Include in Webcast Event Settings		Default = No. This setting determines if the custom field will be usable during Webcast Event setup.

Add a Public Webcast Registration Field

▼ To add a Public Webcast Registration Field:

1. Navigate to **Admin** > **System Settings** > **Custom Fields**.

2. Click the **Add Registration Field** button. By default, name and email address are collected by guest users when logging in to a public Webcast. To collect more information, you must create custom fields and configure them to appear in all Webcasts.

Field Name	Required	Description
Name	Yes	The name of the custom registration field. This will be the label displayed to users. This is a required field and must be unique among registration fields.
Type		The type of custom registration field you are adding. You may add a text field or a pick list where the user may choose from a list of items that you create.
Required		Default = No. This field determines whether the custom registration field must be populated by the user when registering for a public Webcast.
Included in All Webcasts		Default = No. This field determines whether or not the custom registration field will be visible in all Public Webcasts.

Keep in mind the following:

• Admins can edit all settings with the exception of the Type attribute.

• If the Required attribute is changed from No to Yes, the custom field will be required the next time a user edits the video or Webcast.

• The custom field may be deleted by clicking the **Delete** button. This will also delete all content associated with the field.

- You may order the way the custom fields display to users on the **Manage Custom Fields** main page by clicking the up and down arrows. You may also order pick list items in the same manner.

Add a Custom Field to a Video

Add a Custom Field to a Webcast Event

Bulk Editing Custom Fields

Accounts

Monitor Account Information and Activity

The **Accounts** menu consists of tabs and data created to assist Account Admins in maintaining Rev account information.

Contact and **Billing** data about your organization is entered and maintained here. Licensing and timezone attributes are also tracked here.

Child Accounts may also be created that contain the features and functionality of the parent account while at the same time maintaining separate user accounts.
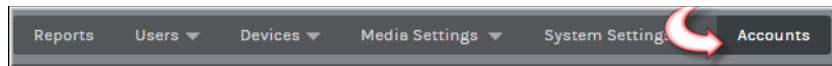
The Contact Module

The **Contact** module is used to set contact and billing information for the organization.

By default, billing information is the same as contact information. You must edit and click the **Enter a different billing address** checkbox to modify billing information if you want billing information to be different from contact information.

View Contact and Billing Information for an Account

The **Contact/Billing** modules contain contact and billing information for an account. To edit contact and billing information for an account, click the **Edit** button on either module.

Field	Required	Notes

Account Name	Yes	The root (parent) account name. Normally the organization name.
Account Host Name	Yes	The IP or URL address of the account. Use extreme caution when changing. This field is tied to the FQDN that is initially set up upon installation of Rev. If this is modified, you need to provision the new DNS first and then point the new Account Host Name at the new DNS. It is *strongly* recommended that you contact Vbrick Support Services if you need to modify this field since you could deny access to your Rev media management portal if you do not modify this field correctly.
Timezone		The timezone that the various time based settings of your Rev account will be based on.
Enable User Provisioning		Display only, not editable in Rev-cloud. Used by Vbrick to enable user provisioning for use with SSO. See: Configure Single Sign On (SSO) with User Provisioning Enabled
License Type		Specifies the type of license applied to your Rev account; **Users** or **Hours.** See: Rev License Types and Add-On Components
Licensed User Count		If your Rev account has a **User** license applied, the number of user accounts that may be created on the account.
Licensed Hours		If your Rev account has an **Hours** license applied or add-on hours applied, the number of viewing/recording hours allotted, used, and expiration dates.
Rev IQ Credits		The number of Rev IQ Credits that have been applied to the account along with the number used and expiration date. Rev IQ credits are used for Facial Recognition functionality. Three IQ credits are equivalent to 1 hour of Facial Recognition processing time. See: Enable Facial Recognition
Rev Connect		Peer mesh allotment for Rev Connect (display only for Rev cloud) and the ability to enable Rev Connect zones. See: Rev Connect Enabled Zones
First Name		First name of your Rev portal manager.
Last Name		Last Name of your Rev portal manager.
Contact Email Address	Yes	Must be in the format for a valid email address (xyz@abc.de)
Address Line 1		Address line one.
Address Line 2		Address line two.

Country		Country
State		If Country is other than the USA, State will be a free-form text field.
City		City
Postal Code		Zip Code / Postal Code
Phone Number		Valid phone number where your Rev portal manager may be reached.

Edit Contact and Billing Information for an Account

To edit contact and billing information for an account, click the **Edit** button on either module.

The **Contact Information** section displays the contact fields that may be modified as desired. To modify billing information, select the **Enter a different billing address** checkbox. Otherwise, billing information is the same as contact information by default.

Once selected, the **Billing Information** section and fields will appear below the **Contact Information** fields and may be modified as well.

Role(s): Account Admin

Rev License Types and Add-On Components

When your Rev portal is initially configured, a **User** based or **Hours** based license type is purchased and applied depending upon your organizational needs. Additional licensing and add-on components may also be purchased and added to either type license.

Note: Rev Cloud licenses are managed and applied by Vbrick. However, you may manage your own Child Account.

Keep in mind:

*   User based license: Viewing and recording is dictated by the number of user accounts purchased. All guest/external viewing (non-Rev accounts) is dictated by the number of add-on *hours* purchased for guest viewing.
*   Hours based license: *All* viewing and recording (Rev and guest accounts) is dictated solely by the number of hours purchased.

The table below further illustrates the feature differences between license types.

License By Users	License By Hours
Included Live/IPTV • Named - Unlimited, included in user license* • Anonymous - Counts against annual hour allotment	Included Live/IPTV • Named/Anonymous • Both count against per hour consumed
Webcast • Named - Unlimited, included in user license* • Anonymous - Counts against annual hour allotment	Webcast • Named/Anonymous • Both count against per hour consumed
Video Conference Recording • Counts against annual hour allotment	Video Conference Recording • Counts against hour recorded
Hours Included (Annual Expiration): • 2500 hours included per 1,000 named users. Add hours by selling an hourly bucket PID.	**Buckets (Annual Expiration):** • 5k Hours (Vbrick Only) • 10k Hours • 50k Hours • 100k Hours

* Acceptable usage policy to govern "unlimited" when delivered by Akamai.

Licensed Add-On Components

Once a license type is purchased, you may also select additional add-on license components. They may be added to either type of license, User or Hours-based, as requested. These are required for certain functions in Rev..

Component	Description
Viewing Hours	Add-on viewing hours; Normally purchased for additional guest viewing on User-based licenses. Auto-ingested Webex Meetings video are also taken from viewing hours allotments. One ingested hour consumes one viewing hour.
Rev Connect Peer Meshes	Used to specify the Peer Mesh Allotment (Child Accounts only for Rev Cloud) and add Rev Connect enabled zones to Rev. See: • Apply a License Type or Add-On Component to a Child Account • Rev Connect Enabled Zones
Rev AI Hours	Used to allocate Rev IQ Credits which can then be used to enable and use AI & Machine Learning components in Rev. This includes such features as Facial Recognition and Vbrick Transcription and Translation services. • Apply a License Type or Add-On Component to a Child Account • Enable Facial Recognition • Enable Rev IQ Transcription and Translation

The table below details how many Rev IQ Credits are required for each hour of video processing per Rev AI feature. Please make sure you confirm this with your Vbrick Account Manager.

Rev AI Feature (per hour)	Rev IQ Credits Required
Facial Recognition	3
Rev IQ Transcription & Translation	1

Keep in mind:

- The Admin Dashboard will keep track of hours and users allotted and used.
- VOD viewing hours are rounded to the nearest hour. Each viewing session is tracked from internal (Rev user accounts) and public users so that totals for both can be tracked.
- When no more VOD viewing hours are available on a **User** based account, external users will be displayed a message that the video is temporarily unavailable. Internal users (Rev user accounts) will still be able to view the video.
- When no more VOD viewing hours are available on an **Hours** based account, no video will be able to be played for either internal (Rev user accounts) or external users.
- Webcast viewing is only calculated once the event is concluded; therefore, if your account has one hour left, you may still start your Webcast with no issues if you plan you have external viewers attend.
- Email notifications will be sent to account Admins when an account has reached 75% and 100% usage of its allotted viewing hours for both **User** and **Hours** based accounts.
- When an account is switched from **Hours** based to **User** based, Rev will switch all users in **Active** status to **Unlicensed** status.

> **Caution**: While documentation will always attempt to remain up-to-date, you should *always* check with your Account Manager before making any major licensing decisions or purchases.

> **Role(s)**:
> - Parent Account Admin to modify and apply license.
> - Child Account Admin to view user account and hours remaining.

The Admin Report Dashboard

Admin Report Usage Tab

The Child Accounts Module

The **Child Accounts** module enables Account Admins to create a child account within the parent account domain. The advantage of this is that the child account acts as an entirely separate domain with its own set of **User Accounts**, **Groups**, **Permissions**, and **Roles**. It functions and acts as its own entity which means that you will have different content for it as well since it will have its own URL.

For example, you could make your root or parent account your corporate organization account and then create separate child accounts for each regional office with user accounts, groups, content, and so forth applicable to each individual regional office (or child account).

The **Child Accounts** module displays:

Column	Description
Accounts	The **Child Account Name** upon creation.
Status	The status of the child account.
Contact Person	The point of contact for the child account.
URL	The **Account Host Name** entered when creating the account.
Actions	The actions you may perform on a **Child Account**. • **Edit:** Allows you edit the attributes of a previously created child account. See Add or Edit a Child Account. • **Delete:** Deletes a previously created child account and all associated data. You may not undo this process. See: Delete a Child Account.

Additional functionality:

Function	Description
Add Account	Creates a new **Child Account**.

Navigate Between a Parent and Child Account

Clicking an account name in the **Accounts** column of the **Child Accounts** module branches you to the child account where you may create entirely new **Users**, **Groups**, **System Settings**, and so forth if desired.
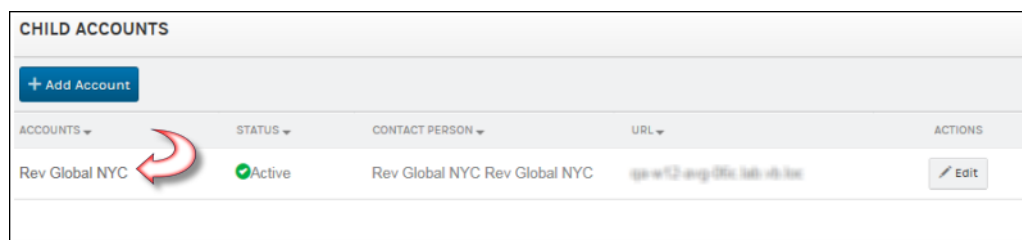
Parent and Child Menu

You may also access it (and navigate back to the parent account) through the parent and child menu option.
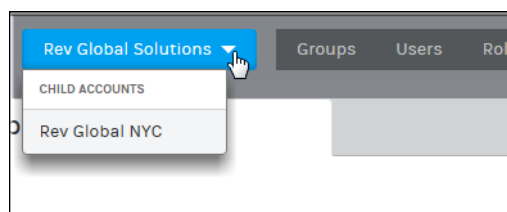
Add or Edit a Child Account

You may create multiple layers of child accounts. However, be aware that a child account is only accessible through the parent account admins that create it. Admins of other domains will not be able to access it including the root account admins.

▼ To add or edit child account:

1. Navigate to **Admin** > **Home** > **Add Account** button. To edit a previously existing account, click the **Edit** button in the **Actions** column.

2. Complete **Account Information**:

Field	Required	Notes
Account Name	Yes	The account name. Normally the organization name. This may not be a duplicate name under the same parent account.
Account Host Name	Yes	The IP or URL address of the account. The host name must create a unique Web address across the entire root account. Further, it may only contain lower case letters, numbers, and hyphens.
Timezone	Yes	The timezone that the various time based settings of your Rev account will be based on.
Enable User Provisioning		Specify if user provisioning should be enabled for SSO. See: Configure Single Sign On (SSO) with User Provisioning Enabled

License Type	Yes	Specifies the type of license applied to your Rev account; **Users** or **Hours.** See: <u>Apply a License Type or Add-On Component to a Child Account</u>
Licensed User Count	Yes	If your Rev account has a **User** license applied, the number of user accounts that may be created on the account.
Licensed Hours	Yes	If your Rev account has an **Hours** license applied, the number of viewing/recording hours allotted, used, and expiration dates.

3. Complete contact and billing information. See: <u>Edit Contact and Billing Information for an Account</u>.

4. If additional add-on components have been licensed, you may allocate them as needed/desired. See: <u>Licensed Add-On Components</u>.

5. Click **Create**. The child account will be accessible in the **Child Accounts** module.

> **Note**: Keep in mind that child accounts do *not* share content with the parent account. The child account is a fully partitioned separate account.
>
> Further, an Account Admin on the parent account will be able to access the child account features and functionality. However, an Account Admin for the child account is *not* able to access parent account features and functionality and is an Admin *only* for the child account.

> **Role(s)**:
> • Parent Account Admin to access and edit all child accounts and functions.
> • Child Account Admin to access and view specific child accounts and functions only.

Apply a License Type or Add-On Component to a Child Account

When your Rev root account is initially configured, a **User** based or **Hours** based license type is selected and applied depending upon your organizational needs. When adding child accounts, you must also choose a license type for the child account.

Keep in mind that the license type that is selected for a child account is *inherited* from the root or parent account hierarchy. For example, if the parent account is an Hours based license account, the child account may only be an Hours based account as well. (See: Rev License Types and Add-On Components)

> Note: The Rev Cloud Root license type may not be modified without the assistance of Vbrick Support Services. However, Child Accounts may have different license types and add-on components provisioned and modified as described in this topic.

▼   To modify a license type or add-on component allocations to a child account:

1.   Navigate to **Admin** > **Accounts** and **Add/Edit** the Child Account.

2.   Complete **Account Information** as your normally would. See: Add or Edit a Child Account

3.   Select the **Users** or **Hours** tab for the **License Type** in the **License Information** section and complete the associated field selection(s).

Field	Required	Notes
License Type	Yes	Specifies the type of license applied to your child account; **Users** or **Hours**. Based on your root or parent account settings and licenses hierarchy.
		Further, the licenses allotted to the child account are subtracted from the root account license total.
		Only the parent/root user Account Admins may modify license settings or allocations.
		See: Rev License Types and Add-On Components

Licensed User Count		If your child account has a **User** license applied, the number of user accounts that may be created on the child account is set here.
		Rev internal user accounts have unlimited viewing and recording options on this license type but are limited by the number of user accounts that may be created by the number in this field. For guest/public viewing options on a user based license type, additional hourly buckets must be purchased and allocated.
		Hourly based license types have unlimited user account creation.
		To track user licenses used, view the **Users** module page by navigating to the **Admin** > **Users** menu. The total number of user licenses allotted, used, and remaining is always displayed for the current account.
Licensed Hours		If your child account has an **Hours** license applied, the number of hours allotted, used, and expiration dates by bucket. User based accounts may also use this field to allocate public viewing hours for guests/external viewing as well.
		When allocated viewing hours are empty or expired, hourly based accounts must be re-purchased for all viewers no matter if the account is internal or external. User based accounts must re-purchase hours for guest/public viewing only; internal Rev accounts will still be able to view VOD videos when hours allocations are empty or expired.
		Note: You must save the Rev account first before you may allocate viewing hours into buckets.

4. If you have purchased any additional licenses or add-on components, they will be displayed as well and you may allocate additional hours or credits as needed. In some cases, you may enable functionality depending on the license purchased.

REV IQ CREDITS

Licensed Credits	LICENSED CREDITS	EXPIRES	USED
	100	Jan 9, 2020 7:00 PM	0:00

Allocate Credits

REV CONNECT

Peer Mesh Allotment   0   *
Total Allotment 0, Available 0

Rev Connect   Enabled

Field	Required	Notes

Rev IQ Credits		If you purchase an AI License component, you may allocate Rev IQ Credits in support of AI & Machine Learning functionality. This includes such features as Facial Recognition and Vbrick Transcription for example.
		See: <u>Enable Facial Recognition</u>, <u>Enable Rev IQ Transcription and Translation</u>
Rev Connect		If a Rev Connect add-on component is purchased, you may specify how many peer meshes may be allotted to this Child Account and enable Rev Connect zones.
		See: <u>Rev Connect Enabled Zones</u>

Caution: While documentation will always attempt to remain up-to-date, you should *always* check with your Account Manager before making any major licensing decisions or purchases.
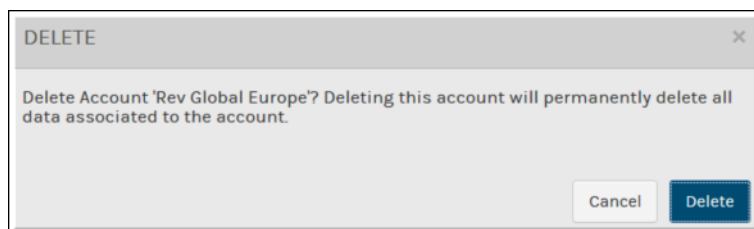
Role(s):
• Parent Account Admin to modify and apply license.
• Child Account Admin to view user account and hours remaining.

Delete a Child Account

You can delete child accounts for your account as long as the account does not have its own children. If you have an account hierarchy, you must delete from the bottom up (accounts without child accounts first).

▼ To delete a child account:

1. Navigate to **Admin** > **Accounts** > **Delete** button under the **Actions** column of the child account.
2. You will be prompted with a confirmation dialogue box.
3. Click **Delete** to confirm the delete account process. Keep in mind this process is irreversible! All data and processes associated with the child account will be lost forever.

Note: Keep in mind that child accounts do *not* share content with the parent account. The child account is a fully partitioned separate account. If you delete a child account, content on the parent account will not be deleted.

Role(s): Parent/Child Account Admins for a specific child account or Root Account Admins for all child accounts

LDAP

Configure and Import LDAP Groups in Vbrick Rev

Vbrick Rev easily imports LDAP groups that have been set up on a single Active Directory (AD) server. This enables you to manage your users separately from the system and, further, designate how often your AD synchronizes back to Rev with any group updates as well. You may import all LDAP groups associated with an AD server or you may specify which groups you want to import to make more efficient use of your time if you do not need all imported at once.

There are three steps to configuring Vbrick Rev so that LDAP groups may be imported and synchronized. LDAP configuration *must* be completed before you may import LDAP groups.

▼　To configure LDAP for use with Rev:

• Add an API Key (Needed when installing the LDAP Connector for Rev Cloud)
• Download and Install the LDAP Connector for Rev Cloud
• Add an LDAP Connector Device

Once you have completed the steps above to install and configure LDAP for Rev, you may import an LDAP group.

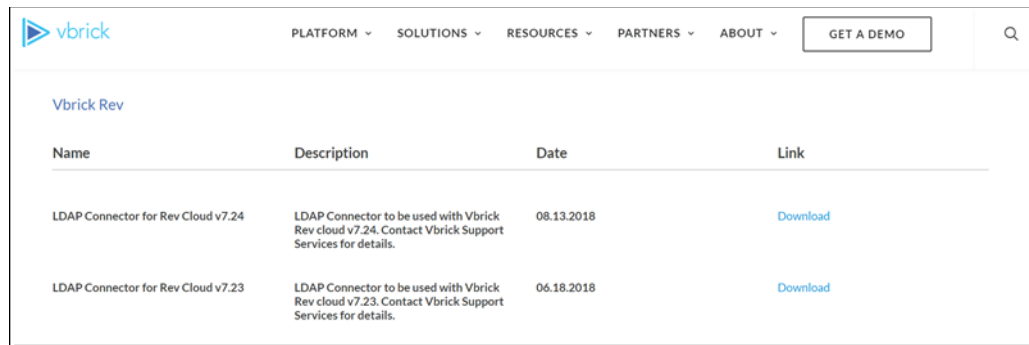Import an LDAP Group

Add or Edit a Group

Download and Install the LDAP Connector for Rev Cloud

Before you may begin importing LDAP groups, you must first download and install the LDAP Connector for Rev Cloud.

The latest version may be found on the Vbrick Downloads site under the **Applications** tab.

During installation, you will be prompted for the following information:

• URL to your Rev instance
• The API you previously created to use with your LDAP Connector

Once the connector is installed, you will need to restart the **Vbrick Rev LDAP Connector Service** in the Window Task Manager.

For complete installation instructions, view the Vbrick Rev LDAP Connector Installation Guide under the Rev Supplementary Documentation section on the Vbrick Documentation Site.

> **Note**: You do not need to download this application if you are using On-Premises Rev. Proceed to Add an LDAP Connector Device.

Add an LDAP Connector Device

Before you are able to import an LDAP group, you must first create a means for Vbrick Rev to communicate with Active Directory and LDAP groups. This is accomplished by creating an LDAP Connector and then running that connector on a host or through a direct connection if you have an on-premise installation. Be aware that the connector will *always* need to be running on the host you choose for importing and synchronizing your LDAP groups and users if you do not have a direct connection enabled.

▼ To add an LDAP Connector:

> **Note**: Depending upon the **Directory Type** you choose, most fields are completed for you when adding an LDAP Connector. If you intend to modify those fields and are unsure of exact values, consult the **Directory Type's** documentation for more information:
> • Active Directory

1. Navigate to the **Admin** > **Devices** > **Source Devices and LDAP Connectors** option.
2. Click **Add a Device** > **Add an LDAP Connector**.
3. Complete each section of the form as described below.

Add the LDAP Connector as a Direct Connection

The **Device Name** section first needs to be completed as either a **Direct Connection** (normally for on-premises installations) or for use with the LDAP Connector for Rev Cloud that you previously downloaded and installed. In this case, you will need to inactivate Direct Connection and enter at least one **Mac Address** (of the laptop/server of the previously installed connector).

This example has Direct Connection in inactive status since Rev Cloud is in use.

Field Name	Required	Description
Device Name	Yes	The unique Device Name you will use to import your LDAP groups.
Status		Designates whether or not your connector is currently active or inactive.
Direct Connection		Enabled by default. This setting is used for On-Premise Rev installations to provide a direct connection to Active Directory. If this setting is enabled, you will *not* be required to download and install the Rev Cloud LDAP connector. You will, however, be required to enter at least one Mac Address which is used to run one or more LDAP Connectors.
Allow LDAP Authentication for Users		Enabled by default. Specifies if users will use LDAP authentication. If disabled, user/group sync will use LDAP while user authentication will use SAML. See: Disable LDAP Authentication for Users.

Add a MAC Address for the LDAP Connector

To use the LDAP Connector for Rev Cloud, make sure you *disable* the **Direct Connection** and enter a **MAC Address** for each **Connector Node** you plan to use. You may configure the status per node or through the entire LDAP Connector as desired (unless there are no active nodes). If more than one node is configured, the system will distribute tasks among the available nodes.

Field Name	Required	Description
Connector Nodes / MAC Address	Yes	Only visible if Direct Connection is set to inactive status. The **Mac Address** for the **Connector Node** is required if Direct Connection is inactive and you will be unable to create the connector without it if you plan to run your connector on a host. This should be the address of the host you plan to run your connector from or previously entered connector host location. This is easily obtained by entering the command `getmac` from a command prompt. The Mac Address is the first line with no dashes. You may add additional nodes by clicking the **Add Connector Node** button. Further, you may change the status of each node at will by clicking the **Active** and **Inactive** buttons. Click the **Remove** button to remove a node. **Note**: The LDAP Connector for Rev Cloud version in use is displayed under each address. It is not recommended that different versions of the connector be in use at the same time. The first two **MAC Addresses** of each node you add may be viewed on the main **Source Devices and LDAP** page under the **Network Address** column.

LDAP Connector Status depends on the following node states:

• If LDAP Connector is active and all active LDAP nodes are online: Active
• If LDAP Connector is active and at least one active LDAP node is offline: Warning <# of offline nodes/# of active LDAP nodes>

- If LDAP Connector is active and all active LDAP nodes are offline: Offline (See image above)
- If LDAP Connector is inactive: Inactive

LDAP Server Settings

Once you decide how you are going to run the connector, complete the **LDAP Server Settings** section.
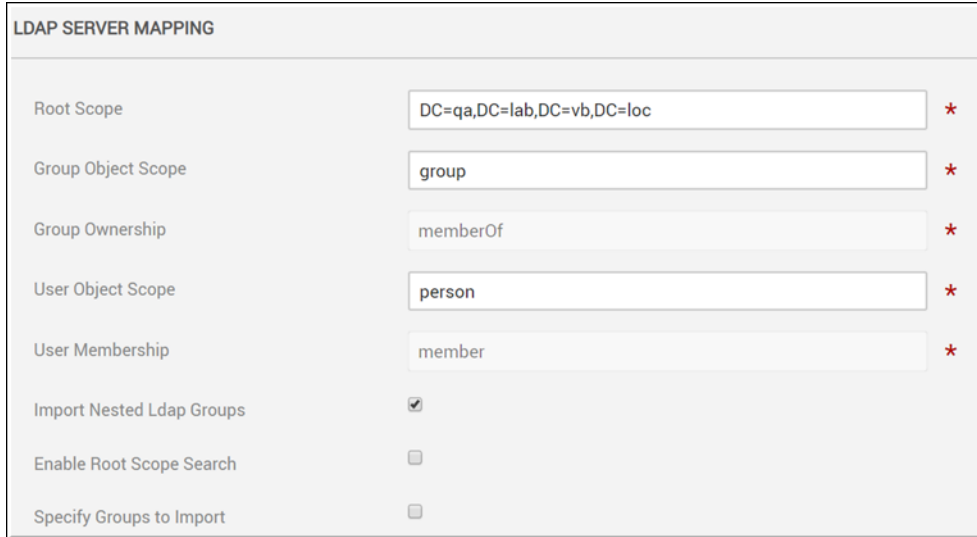
Field Name	Required	Description
Directory Type	Yes	The directory type that the **LDAP Connector** supports; Note that when you choose a directory type, the <u>LDAP Server Mapping</u> fields will be automatically populated with the recommended default settings for that type.
LDAP Server Host	Yes	The IP address or name of the host.
Port	Yes	The default port is 389. Use 636 if using SSL.
SSL		Indicates the LDAP connection is over SSL if selected.
TLS v1.2		Enables TLS v1.2 support. Must have SSL enabled first before this becomes available.
Username	Yes	The user name/password to connect to LDAP Server. **Note**: Click the **Change Username and Password** button to access Credentials.
Password	Yes	The user name/password to connect to LDAP Server. **Note**: Click the **Change Username and Password** button to access Credentials.

Tip: This topic uses **Active Directory** as the **Directory Type** when creating an LDAP Connector. However, selecting **Generic LDAP** is much the same process.

LDAP Server Mapping

Most of the **LDAP Server Mapping** section is populated with recommended default values and formats when you choose a **Directory Type** in the LDAP Server Settings section. The image below displays the server mappings for **Active Directory**. These fields may be modified if needed. Most fields are required.
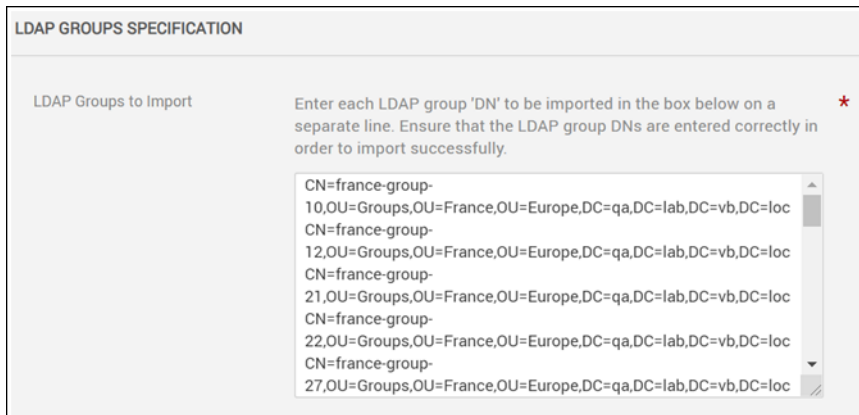
> **Note**: Keep in mind that if you change the **Root Scope** field in the **LDAP Server Mapping** section after you have already imported groups and users, you will need to re-import your group.

LDAP Groups Specification

The **LDAP Groups Specification** section is used to import specific LDAP groups only and is only visible if the **Specify Groups to Import** checkbox is selected in the previous LDAP Server Mapping section.

If you are an organization with hundreds (or even thousands) of LDAP groups, this may take a considerable amount of time to import. You may use the **Specify Groups to Import** checkbox to enter the LDAP group you want to import instead. This will open the **LDAP Groups Specification** section where you may enter the Distinguished Name (DN) of the LDAP group to be imported seen in the example below.

By default, the **Specify Groups to Import** checkbox is deselected which means that *all* LDAP groups associated with your Active Director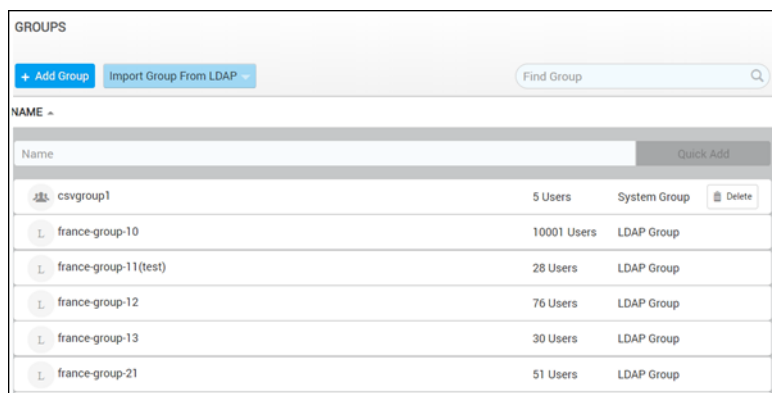y server will need to be retrieved and displayed for potential import when you click the **Add Groups** action for an LDAP Connector device or the **Import Group From LDAP** button from the **Groups** module, seen in the image below.

Keep in mind:

• You must enter the LDAP DN name exactly as it appears. If it is misspelled or entered incorrectly it will not import. **Note**: It is *not* case sensitive.

• If you use this method, you may no longer use the **Add Groups** action for an LDAP Connector device or the **Import Group From LDAP** button from the **Groups** module until the **Specify Groups to Import** checkbox is once again deselected.

• If the checkbox is deselected and you want to import new groups, then the **Reset Connector Sync** button must used to manually sync the connector; or you may also wait until the next scheduled sync interval has been performed. See: LDAP Server Synchronization Settings.

User Record Mapping

Similar to the LDAP Server Mapping section, the **User Record Mapping** section is populated with recommended default values and formats when you choose a **Directory Type** in the LDAP Server Settings section. The image below displays the user record mappings for **Active Directory**. These fields may be modified if needed. Most fields are required.

Caution: You must have the LDAP Connector v7.30+ deployed to map the **User Profile Image** field. This must be a jpeg format image no larger than 5MB or an error will be generated.

Merge Users

The **Merge LDAP and non-LDAP users** checkbox is disabled by default. If this is checked/ enabled, the LDAP connector will process and merge the incoming user even if the user currently exists in Rev (if unchecked, a "duplicate user" error is generated).

Keep in mind:

- The incoming user will be treated as an update and this is **permanent** and **not reversible**.
- The update only occurs if *both* username and email address match.
- The source of the user account will be modified to LDAP.
- If the Rev user account had additional roles, those will be retained.
- If the Rev user account was manually suspended, that user will remain suspended.
- Active and unlicensed status will remain unchanged.
- LDAP fields override Rev user field values, including any blank fields.
- As noted, if this checkbox remains disabled, then the LDAP connector will continue to display an error message for any duplicate username/email addresses found.

LDAP Server Synchronization Settings

The **LDAP Server Synchronization Settings** section is used to specify the sync interval from Active Directory to Vbrick Rev. You can also specify how Suspended user accounts are treated during syncs and in accordance with LDAP groups edits.

Sync intervals are specified in minutes or hours. The recommended interval is 24 hours; particularly if importing and/or syncing large groups of users so you do not tie up server resources during peak usage time by your end users. Note that you *must* specify a synchronization interval.

Select the **Delete Suspended Users Who have never logged** in checkbox to delete those LDAP accounts that were synced and imported but then subsequently never logged in to Rev. An

example of this may include a user account that was created and imported but then left the company before logging in.

```
LDAP SERVER SYNCHRONIZATION SETTINGS

Sync Interval                                24 Hours              ▼   *

Delete Suspended Users Who have never        ☐
logged in
                                             Deleting user is permanent

Do not suspend users when removed from       ☐
all LDAP groups or LDAP group is removed
```

Select **Do not suspend users when removed from all LDAP groups or LDAP group is removed** if you want to disable the suspension of users when users are removed from the LDAP group/ groups that are being synced with Rev. The following rules apply for this setting when enabled:

- When removing users from all groups in LDAP they are removed from groups but not suspended in Rev.
- When a group is no longer selected for an LDAP import in the Connector users are not automatically suspended.
- This option is disabled by default. Also note that for those users already suspended in Rev, this option has no effect and does not change their status.

Finally, if your sync needs to be reset for any reason, you may use the **Reset Connector Sync** link in the Actions drop-down on the All Devices form to do so.

Reset the LDAP Connector Sync

Import an LDAP Group

Disable LDAP Authentication for Users

Delete or Suspend an LDAP Group or User

Reset the LDAP Connector Sync

When you first add your LDAP Connector, the **LDAP Server Synchronization Settings** section is used to specify the sync interval from Active Directory to Vbrick Rev. However, you may also manually reset the sync if necessary by using the Actions drop-down menu on the All Devices form.

▼   To reset the LDAP Connector:

1. Navigate to **Admin** > **Devices** > **Source Devices and LDAP Connectors**.
2. Select **Reset Connector Sync** in the **Actions** drop-down of the LDAP Connector you want to reset.
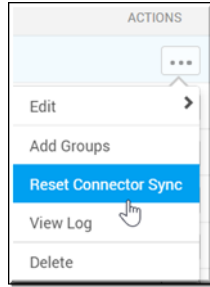
Disable LDAP Authentication for Users

When you first add your LDAP Connector, you can specify if LDAP authentication is to be used for users (either as a direct connection or through a connector). This functionality is enabled by default.

If disabled, however, this means that users and groups will still use LDAP sync while users will be *authenticated* through SAML.

▼   To disable LDAP authentication for users:

1.   Navigate to **Admin** > **Devices** > **Source Devices and LDAP Connectors**.
2.   Select the LDAP Connector to edit.
3.   Deselect the **Allow LDAP Authentication for Users** checkbox.
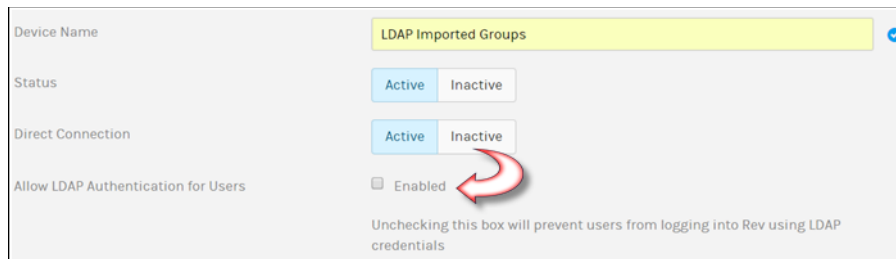
Keep in mind:

• When checked, users must use LDAP credentials to log in to Rev.
• When disabled, if a user attempts to login using LDAP credentials, an error message will appear.

Rev Technical Requirements

This section contains topics that deal with Rev technical requirements and supported formats. It will be updated frequently and will always refer to the latest version of Rev.

Supported Video and Audio File Formats

The following file types are supported when uploading video and audio in Rev:
- MP3
- MP4
- FLV
- F4V
- MKV
- MOV*
- WMV (VC-1)
- MPEG-1
- MPEG-2
- MTS*
- OGV*

* These files must be transcoded first as the original files will not be playable within Rev.

Transcoding Preset Default Settings

Supported Vbrick Devices

Rev Version	DME Version	Encoder Versions	LDAP Connector Versions	VBM Agent
Current Rev Cloud Release - v7.37	• DME 3.24.0 • DME 3.23.0 - Includes all patches	• Encoder 4.9	• 7.37 • 7.36	• 1.3
Current Rev On-Premises Release - v7.34	• DME 3.23.0 • DME 3.22.0 - Includes all patches	• Encoder 4.9	• NA	• 1.2

Rev Version	DME Version	Encoder Versions	LDAP Connector Versions	VBM Agent
Previous Rev On-Premises Release - v7.28	• DME 3.21.0 • DME 3.20.2 • DME 3.19.1 • DME 3.19.0	• Encoder 4.9	• NA	• 1.1.4 • 1.1.3

Add a Distributed Media Engine (DME)

Add a Distributed Media Engine (DME)

View the Status of a Device

Supported Player and Stream Compatibility

Stream Type	IE11 (Win7)	IE11 (Win8)	Edge (Legacy)	Edge Chromium	Chrome	Firefox	Safari	iOS	Android
Flash Multicast*	Flash	Flash		Flash	Flash	Flash	Flash		
Vbrick Multicast+		HTML5	HTML5	HTML5	HTML5	HTML5	HTML5		
Rev Connect**				HTML5	HTML5	HTML5	HTML5 **		
HLS***	Flash	HTML5	HTML5	HTML5	HTML5	HTML5	HTML5	HTML5	HTML5
RTMP Unicast	Flash	Flash	Flash	Flash	Flash	Flash	Flash		
RTP Multicast	Vbrick	Vbrick							
RTP Unicast	Vbrick	Vbrick							
MP4 Progressive Download	HTML5	HTML5	HTML5	HTML5	HTML5	HTML5	HTML5	HTML5	HTML5

* Flash Multicast takes priority for live streaming events.

** Rev Connect can only be utilized from within Vbrick Rev using the Vbrick Rev HTML5 player. While it is supported on Mac Safari, it is NOT supported on iOS Safari.

*** Flash player is used for HLS if account is not on DME 3.8+. This is due to a cross domain HLS issue. DME 3.8 solves this within the Vbrick solution but it could exist from external HLS sources.

+ Vbrick Multicast playback requires the installation of the Vbrick Multicast (agent) for Windows or Mac to be installed from the Support Download Portal.

> **Tip**: "Vbrick" in the table above refers to browser plug-ins that will be used to play the stream type. To use these plug-ins, users may need to grant permission for them to run within the browser.

> **Note**: Vbrick currently does not support video-only or audio-only Live streams. Audio-only VOD streams are currently supported. Note that Vbrick encoders can be set up to add silent audio if the source does not have audio.

Supported Browser, Operating System, and Device Compatibility

> **Note**: Operating Systems are always updated to the latest versions whenever updates are made available for each version in use. Vbrick updates and tests with the latest version(s) of Firefox and Chrome. To ensure that you are consistent, please make sure you also have the latest version of each OS and browser you use.

Device	OS	Browser
PC	• Windows 10 Enterprise • Windows 10 Pro • Windows 8 and 8.1 Pro • Windows 7 Pro	• IE 11+ • Firefox 70+ • Chrome 78+ • Edge (Windows 10 only) • Edge Chromium
Mac	• macOS 10.13: High Sierra • macOS 10.14: Mojave • macOS 10.15: Catalina	• Safari 13+ • Firefox 70+ • Chrome 78+* • Edge Chromium
iPhone, iPad	iOS 13.0+	Native Browser
Android	Android 7.0+	Chrome only
Chromebook	Chrome OS	Chrome only

* The Mac Chrome Browser video decoder has displayed some instabilities when playing HLS streams with identified data loss. This is a rare occurring issue that manifests as a "stall" or stopping of the playback. Disabling Chrome Hardware Acceleration will fix the issue. You can disable this from within Chrome by visiting the URL "chrome://settings", then navigating to Advanced > System > "Use hardware acceleration when available" and toggling as necessary. This issue only effects Mac Chrome users and does not affect Windows users.

Allowed Lists and Required Rev URLs

> **Note**: This is in reference to Rev Cloud only.

Accessing Rev Cloud requires that end user's browsers are able to access certain Rev URLs. Some customers leverage browser, proxy, or firewall lists to restrict URLs that can be accessed from an end user's browser. For those customers, along with adding your main Rev URL to the listed sites, it is important to add the data center URLs below to the Allowed List

sites (or preferably add a more generic *.us.vbrickrev.com, *.eu.vbrickrev.com, *.au.vbrickrev.com allowed listing rule).

Note that your welcome e-mail will contain the main Rev URL that you use to access Rev or it may be a custom URL that you requested. Those accessing our cloud-based CDN will use something similar to *.akamai.net. Contact Vbrick Support if you have any questions.

Note which data center you are hosted in to add the sites below in addition to your main Rev URL:

North American Data Center

- https://media.us.vbrickrev.com
- https://static.us.vbrickrev.com
- https://dme-update.us.vbrick.com
- https://media-alt.us.vbrickrev.com
- https://northamerica.rev.vbrick.com
- https://webexlive.rev.vbrick.com

EU Data Center

- https://media.eu.vbrickrev.com
- https://static.eu.vbrickrev.com
- https://dme-update.eu.vbrickrev.com
- https://media-alt.eu.vbrickrev.com
- https://europe.eu.vbrickrev.com
- https://webexlive.eu.vbrickrev.com

AU Data Center

- https://media.au.vbrickrev.com
- https://static.au.vbrickrev.com
- https://dme-update.au.vbrickrev.com
- https://media-alt.au.vbrickrev.com
- https://asiapacific.au.vbrickrev.com
- https://webexlive.au.vbrickrev.com

Rev Connect

You should only list outbound connections of the following URLs if you are using Rev Connect. Otherwise, this is not required.
- https://rev-connect.us.vbrickrev.com
- https://rev-connect.eu.vbrickrev.com
- https://rev-connect.au.vbrickrev.com

Supported Browser Closed Captions by Stream Type

Stream Type	IE11 (Win7)	IE11 (Win8)	Edge	Chrome	Firefox	Safari	iOS	Android
Flash Multicast	Yes	Yes		Yes	Flash	Yes		
HLS	Yes	Yes	Yes	Yes	HTML5	Yes	Yes	Yes

Stream Type	IE11 (Win7)	IE11 (Win8)	Edge	Chrome	Firefox	Safari	iOS	Android
RTMP Unicast	Yes	Yes		Yes	Flash	Yes		

Support for displaying closed captions has been checked in accordance to the table above. Please note that even if the video stream type and browser support closed captioning, the video asset itself must also contain captions in order for the captions to be visible in the player. RTP Multicast, RTP Unicast and MP4 stream types do not support closed captions.

Enable Closed Captions on a Video

Browser Settings and Device Configurations

Some supported browsers require specific configurations or settings when used with Rev and are detailed below.

Microsoft Edge

The Rev URL should be added to your "Local Intranet" so that Rev can play http-based HLS/RTMP streams from DME via Flash. This has been tested and confirmed.

▼ To add Rev's URL to Local Intranet:

1. In Internet Explorer, click **Tools > Internet Options**. (You may also type **inetcpl.cpl** in the **Start** menu).
2. On the **Security** tab, click **Local Intranet > Sites**.
3. Click **Advanced** and add your Rev URL in the **Add this Web site to the zone** box.
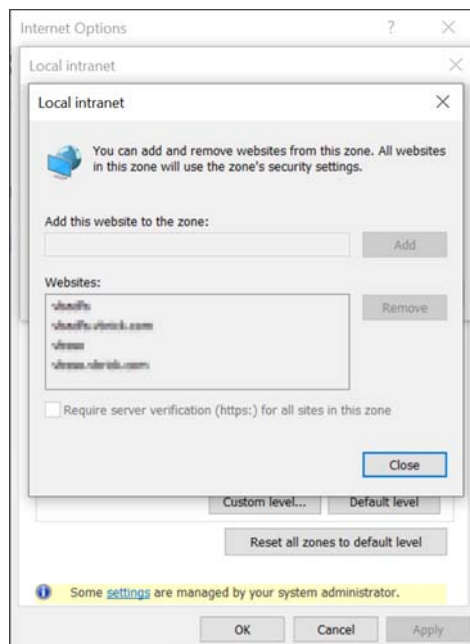
4. Click **Add** then close the form by clicking **Close** and then **Ok** and **Apply** as needed.
5. Restart your computer.

> **Note**: Some organizations manage Local Intranet sites through Group policy and do not allow direct editing. This means you will need to request this update through your IT department. However, you may test this environment setting by temporarily adding it for a given user.
>
> See: https://www.isunshare.com/windows-10/add-trusted-site-to-group-policy-in-windows-10.html

Citrix BCR Requirements

Citrix Flash Offloading

| Citrix Version	Rev Version	Citrix VDA/VDI OS Version	Browser	Stream/Playback Type
Citrix XenApp/ XenDesktop 7.6 and above that supports Flash offloading	Rev 7.15 and above	Windows 7 and Windows 2008 Server	IE11	Flash-based unicast and multicast

Citrix Browser Content Redirection (BCR) Software Requirements

Citrix Version	Rev Version	Citrix VDA/VDI OS Version	Citrix Receiver OS Version	Browser	Stream/Playback Type
Citrix XenApp/ XenDesktop 7.15 LTSR CU3 Citrix XenApp/ XenDesktop 7.16 and above **More Info**: Citrix Blogs - Maximize Multimedia w/ BCR 2.0 BCR 2.0 Configuration	Rev 7.25 and above	Windows 10	Windows 10 and 8	IE11 and Chrome	HTML5 HLS based multicast and unicast Multicast requires Vbrick Multicast agent to be installed on the Citrix receiver

Citrix Browser Content (BCR) Redirection

Browser Content Redirection (BCR) 2.0 is a new feature introduced in Citrix XenApp/ XenDesktop v7.16. It allows seamless redirection of the entire browser content area (a.k.a. viewport) to the Citrix client (known as the receiver) for selected webpages or domains. Previous versions of Citrix (such as Flash redirection) allowed only the video element of the page redirected to the client.

The **viewport** displays the content outlined in the rectangular area of your browser seen in the image below. It does not include things like the address bar, Favorites toolbar, or the status bar.
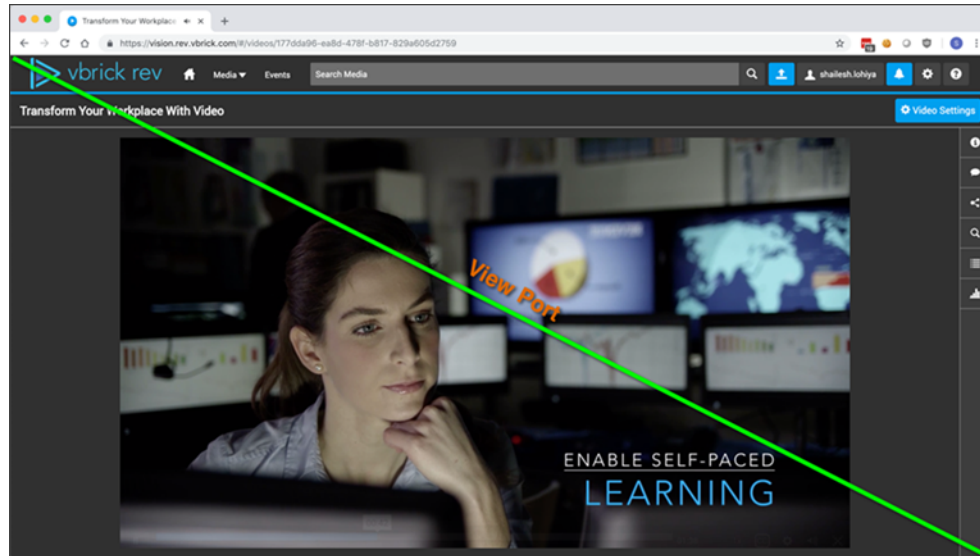
BCR 2.0 provides Vbrick complete control of Rev's content display using HTML5 technology including the HTML5 video player. It allows Vbrick to serve multi-bit rate HLS video directly on the receiver.

Vbrick Multicast

Browser Content Redirection is also supported for **Vbrick Multicast** that provides support for multicast using the HTML5 player. This requires the Vbrick Multicast agent to be installed on the Citrix receiver.

Vbrick Rev Zoning

With Browser Content Redirection enabled, Rev receives the IP of the receiver and Rev applies the zoning using the IP of the receiver. If the **User Location IP Service (ULS)** is enabled, Rev will use the DME ULS URL to get the client IP of the receiver and Rev will use the IP returned by DME ULS for zoning.

Software Requirements

Proper configuration and use requires the following software versions:

Citrix

• Current Release: Citrix XenApp/XenDesktop 7.16 and above
• LTSR Release: Citrix XenApp/XenDesktop 7.15 LTSR CU3
• VDA Operating System: Windows 10
• Receiver: 18.9 and above
• Receiver Operating System: Windows 10 and 8
• Browsers: IE 11 and Chrome

Vbrick Rev

• Rev 7.25 (Oct 2018) and above

BCR Configuration

1. Install the **Browser Content Redirection Chrome Extension** on the VDA for each user that will login to the receiver. This can be pushed as a policy by the Citrix Admin.

    a. Find it here: https://chrome.google.com/webstore/detail/browser-content-redirecti/hdppkjifljbdpckfajcmlblbchhledln?utm_source=chrome-ntp-icon

2. The Citrix Admin should also configure a studio policy on the controller by selecting the **Policies** menu option then the **Settings** tab.
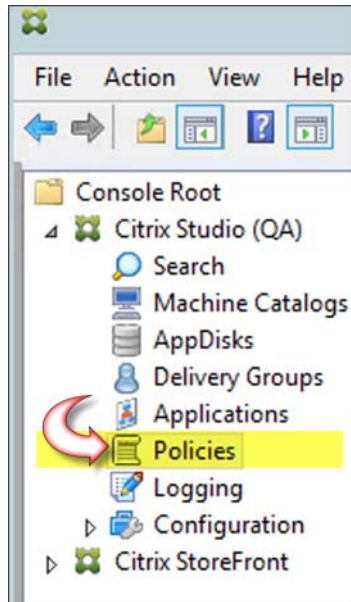
3. This includes whitelisting the Rev URL under **Browser Content Redirection ACL Configuration**, seen below.
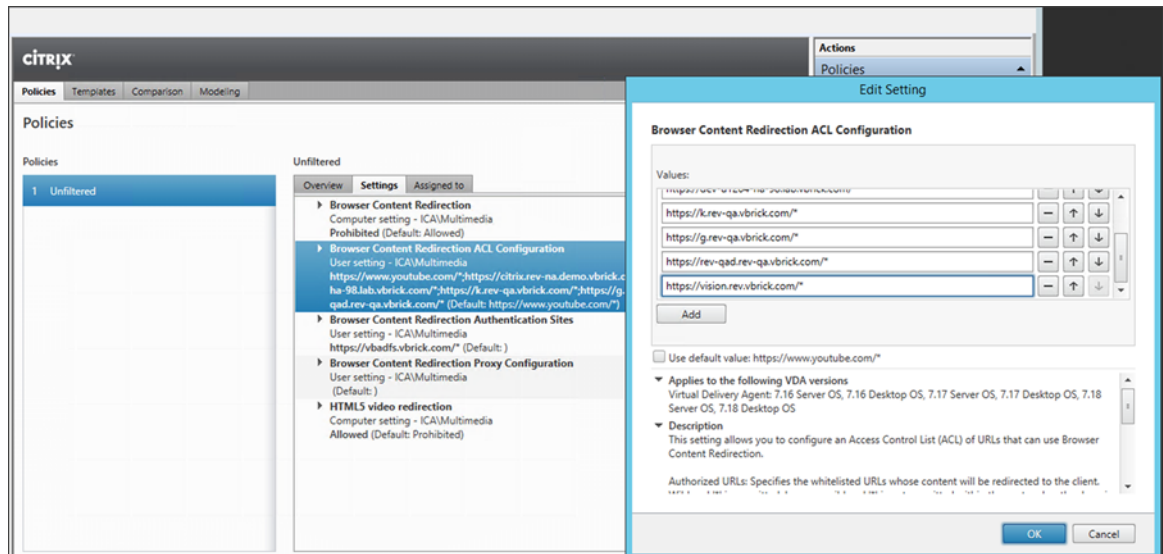
4. If a customer is using SAML SSO with Rev then under **Browser Content Redirection Authentication Sites** the **SAML Identity Provider (IDP) URL** is whitelisted.

    b. See below for sample configuration. You should also refer to https://support.citrix.com/article/CTX238236 for additional details if needed.
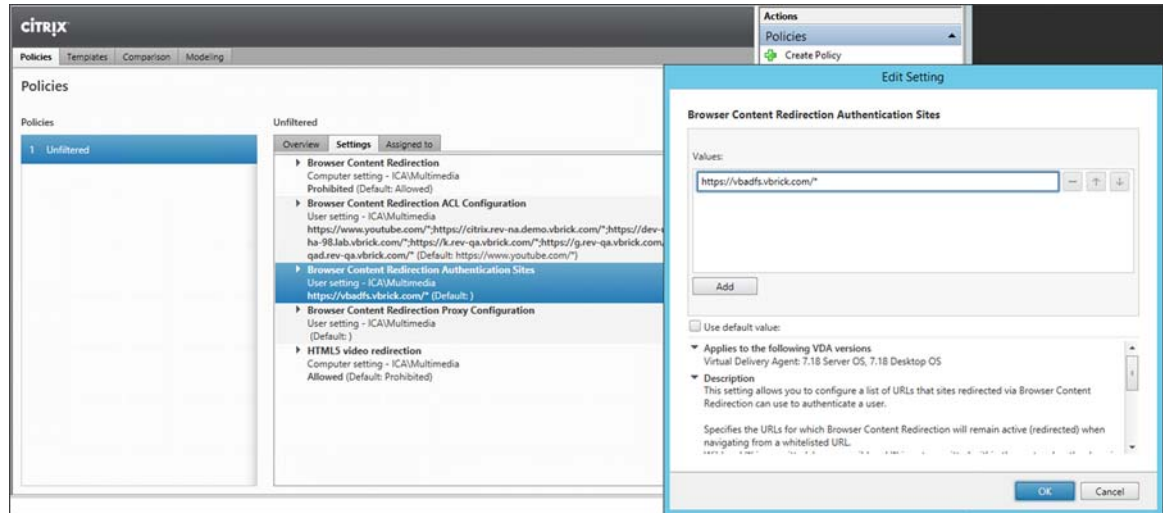
Understanding How the Citrix Receiver Fetches Content

Understanding how the Citrix Receiver fetches content is an important configuration consideration.

Client Fetch – Client Rendering: Receiver is contacting Rev directly, therefore it requires Internet access. This offloads all the network usage, CPU, GPU and RAM from VDA to Receiver. All the heavy lifting is done by the Receiver. **This configuration is tested and recommended by Vbrick for Rev**.

Server Fetch – Client Render: Receiver is contacting and fetching content from Rev through the VDA using a virtual channel. This is useful when the client does not have Internet access. Low CPU, GPU and RAM consumption are expected on the VDA but bandwidth will be consumed on the ICA virtual channel.

Server Side Rendering (SSR): No redirection happening, either because the Rev URL is not whitelisted, or the redirection failed and Citrix fallbacks to rendering the webpage on the VDA.

Caution: Note that when Browser Content Redirection is configured, the server fetch is prohibited by default.

Browser Content Redirection Confirmation

Verify that you have successfully configured BCR 2.0 by right-clicking on the Webpage which will show a menu **About HDX Browser Redirection**.

It can also be verified by confirming three processes on the receiver called **HDX Overlay Browser** on Win10 or called **HdxBrowserCef.exe** on Win7.
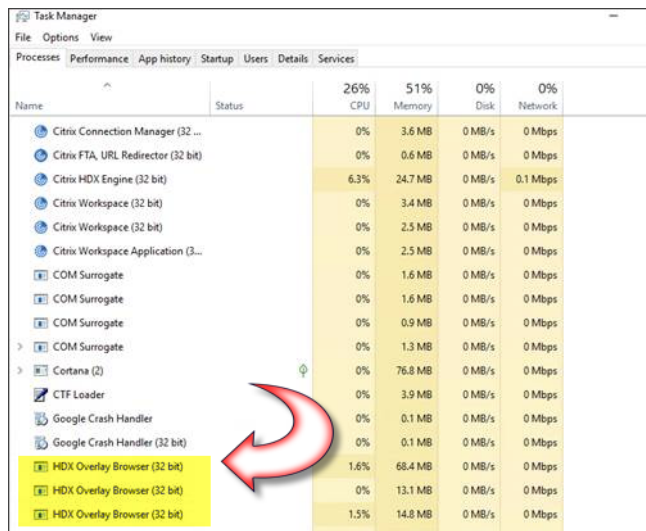
Supported Supplemental File Types and Image Types

The following file types may be attached to a video in Rev. This list also includes the images that may be used in Rev.

File Type
Powerpoint presentations (.ppt, .pptx)
Word documents (.doc, .docx)
Excel documents (.xls, .xlsx, .csv)
PDFs
Zip files (.zip, .rar, .7z)
Text files (.txt)

File Type
Images (.jpg, .png, .gif)

Attach a Supplemental File to a Video

Download a Video File Attachment

Supported System Integrations

Integration Version/ Rev Version Required
WebEx / WebEx v.29 / Rev 7.7
Spark / Spark Cloud & Spark Account / Rev 7.8
TCS / TCS 6.2.1 / Rev 7.5 / DME 3.5.1
VoiceBase / Rev 7.9

Add and Configure a Webex Meetings Site

Enable Webex Teams Integration

Recording

Supported Video Conference (VC) System Integrations

The cloud-version Vbrick Rev system supports live and recorded Webcast events utilizing Video Conferences (VC). When initiated, Vbrick Rev joins a VC call as a SIP participant.

> **Note**: The VC MBR feature has been temporarily disabled for additional tuning with respect to the readability of lower bitrates. VC streaming and recording will continue to create streams using the native VC resolutions and bitrates.
>
> Once Vbrick development and testing have completed the tuning, it will be re-enabled. Thank you for your patience.

Once connected, Vbrick Rev will receive the individual Speaker and Content Share streams from your VC system. Vbrick Rev then encodes several bitrates for each of the Speaker, Content Share, and (a generated) Switched streams. (Note: The Switched stream is a single stream that will initially display the Speaker and switch into and out of a Content view as content is shared.)

The three streams will then be automatically encoded into three bitrates – High, Medium, and Low. Each bitrate is actually a resolution specification that is encoded within a range of bitrates. These are:

- High: Resolution 720 (HD) Height fixed, Width calculated reserving original aspect ratio; Bitrate targeting 2.6M to 3.6M
- Medium: Resolution 540 (qHD) Height fixed, Width calculated reserving original aspect ratio; Bitrate targeting 1.0M to 2.0M

- Low: Resolution 432 (FWQVGA) Height fixed, Width calculated reserving original aspect ratio; Bitrate targeting 640K to 1.2M
- Note: Vbrick models on 16:9 resolutions and the bitrate may vary below the target based on stream content.

These three streams (Speaker, Content, Switched), with their three bitrates (High, Medium, Low) are then combined into multi-bitrate (MBR) HLS specification for an adaptive playback within our Vbrick Rev player.   (Note: The Switched stream will be provided to native HLS players such as iPhone embedded players.) In this way, viewers that may be on congested or reduced bandwidth lines will automatically optimize for playback.

Please be reminded that as resolution and bitrate are reduced, for example in the Medium and more pointedly in the Low bitrate, the crispness, readability and quality of the video will be challenged. These characteristics are impacted by a number of issues, not the least of which includes the expanse of video (e.g., isolated to a talking-head all the way our to a full landscape view), the degree of motion within the video (e.g., still life to sports footage), and font size when readability is required from the stream. If your use case includes playback at the low setting, please test acceptability of both your Speaker and Content streams at that level.

Also, while Vbrick can capture up to 720p streams, this resolution is negotiated between your VC system and Rev. If you find that your High level streams do not have the 720 resolution, please check the settings within your VC systems.

As always, test for acceptance at all bitrates for each stream against your particular needs, and plan accordingly.

Please see the related help topics below for additional details on these features.

The following list identifies end points that are currently supported in Rev:
- WebEx CMR
- Cisco CMS, DX, SX
- WebEx Teams
- Zoom (Requires at least one Akamai Live device to be configured. See: Add an Akamai Live Device)

For hardware endpoints, Vbrick requires the device to be on the latest firmware/software.

While other systems may work, these are the only systems that Vbrick has qualified and supports through Vbrick Customer Support.

> **Note**: VCI utilizing MBR requires a minimum WAN/LAN bitrate of 700Kbps for dual playback of both Speaker and Content (and less for single stream playback) per viewer. At this available WAN/LAN bitrate, the lowest VCI Speaker and Content will be shown. Playback below this threshold is not guaranteed for VCI MBR streams.

Working with WebEx Teams

WebEx Teams is a cloud based enterprise collaboration suite. Rev can stream/record an existing call that has originated within a WebEx Team space with the following caveats:

1. Vbrick Rev requires that a WebEx Team space must have at least one active video participant before the streaming/recording is initiated from Rev. Starting streaming/recording to an inactive space may produce poor to failed video.

- **Best Practice:** Have at least one participant in the space at least 30 seconds before initiating the streaming/recording on Rev.
2. Vbrick Rev does not support WebEx Team Point to Point calls – these are calls directly to a WebEx Team user. Vbrick Rev supports WebEx Team space calls and direct calls to H/W end points.
3. Webex allows participants to "take over" the content share if another participant is sharing. In rare occurrences, Webex does not forward the new content share.
    - **Best Practice**: When multiple participants utilize content share, each participant should end their content share before the next participant begins sharing.
    - **Note**: If your content share is not showing, stop your content share and then restart it to fix.

Lastly, the WebEx Team SIP address, required to initiate a call from Rev to a WebEx Team space, can be found on the **Schedule a Meeting** page on the WebEx Teams application, under **Join by video system**.

Record a Video Conference

Schedule a Video Conference (VC) Live Webcast Event

Enable Webex Teams Integration