VideoManager 12.0 Admin Guide

This document is intended to be a reference guide for system administrators when utilising advanced VideoManager features.

Intended purpose

This document is intended to be a reference guide for system administrators when utilising advanced VideoManager features.

Conventions

This document uses the following conventions:

Convention	Description
▸ For more information...	A cross-reference to a related or more detailed topic.
[ ]	Text enclosed in square brackets indicates optional qualifiers, arguments or data.
<>	Text enclosed in angle brackets indicates mandatory arguments or data.

Contact address

Edesix Limited
16 Forth Street
Edinburgh
EH1 3LH
United Kingdom

Safety notices

Caution — *Indicates a hazardous situation which, if not avoided, could result in moderate injury, damage the product, or lead to loss of data.*

Additional information relating to the current section.

Notice — *Indicates a hazardous situation which, if not avoided, may seriously impair operations.*

9 Admin

The ***Admin*** tab provides access to system administration functions.

These functions include:

- ***People*** (***Users*** and ***Roles***).

>> For more information, see People on page 134

- ***Devices*** (***Device Profiles***, ***Device Settings***, and ***Access Control Key Management***).

>> For more information, see Devices on page 145

- ***Connectivity*** (***WiFi Profiles***, ***Bandwidth Rules***, ***Auto Fetch***, and ***Site Manager***).

>> For more information, see Connectivity on page 153

- ***Policies*** (***Deletion Policy***, ***Incident Exports***, ***File Exports***, ***Password Complexity***, ***Reports***, ***User-defined Fields***, and ***Import Profiles***).

>> For more information, see Policies on page 165

- ***User Interface*** (***Login Settings***, ***Dashboard***, ***Messages***, ***Theme Resources***, ***Player***, ***Language***, ***Maps***, and ***Thumbnails***).

>> For more information, see User Interface on page 193

- ***Firmware*** (***Auto Upgrade Settings***, ***Device Images***, ***DockController Images***, and ***EdgeController Images***).

>> For more information, see Firmware on page 212

- **System** (***Storage***, ***Web Server***, ***Backup Databases***, ***Licences***, ***Advanced Settings File***, and ***Server Controls***).

>> For more information, see System on page 221

- **⚖ Legal**

>> For more information, see View Legal Information on page 235

9.1 People

In the ***People*** tab, users can edit aspects of VideoManager related to users and roles.

To access the ***People*** tab:

1. Navigate to the ***Admin*** tab.
2. Click the ***People*** pane.

From here, users can access:

- ***Users***

Create, edit, reassign, and delete users.

>> For more information, see Create, Edit, Reassign and Delete Users on page 135

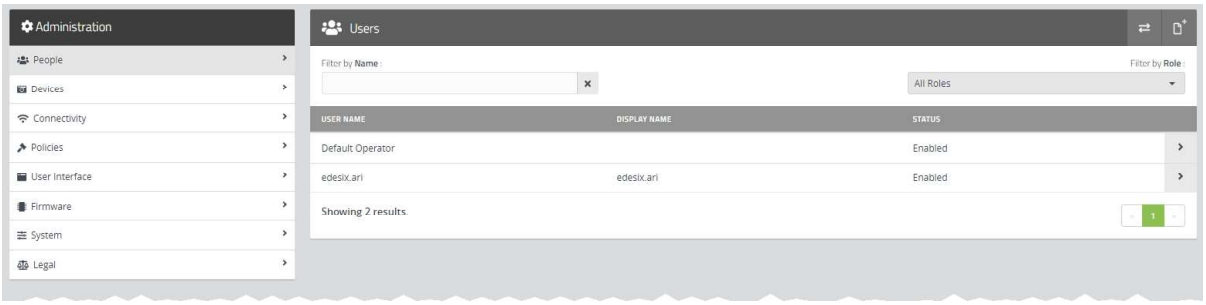
- ***Roles***

Create, edit, and delete roles.

>> For more information, see Create, Edit, Copy and Delete Roles on page 138

9.1.1 Create, Edit, Reassign and Delete Users

A user is assigned to every person wishing to access VideoManager. Different users have varying levels of control over the system, depending on how they have been configured. This is done from the ***Users*** section of the ***People*** pane, in the ***Admin*** tab.



From the appropriate pane, sufficiently privileged users can perform a range of actions. These actions are:

- Create, edit, and delete users.
- Reassign users.

To create a user:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Users*** section.
4. Click ***Create User***. The ***New User*** screen opens.
5. Enter the following information for the new user:
    - **User Name -** enter a name for this user. No two users can have the same name on one VideoManager system. This **cannot** be changed later.
    - **Password -** enter a password for the user.
    - **Confirm Password -** enter the password again to confirm it.
    - **Display Name -** enter a display name for this user. This can be changed later.
    - **Touch Assign ID -** enter the ID the user uses for assignment of devices with RFID if Touch Assign is being used for VideoBadge assignment.

To find the RFID value of a tag, swipe it and then click the question mark at the right hand end of this text box. This will show a list of failed Touch Assign assignments the most recent entry will be for that failed scan, from which can copy the value from the entry to the textbox. Alternatively, if Touch Assign is not being used, leave this field blank.

6. Set additional options for the new user using the following toggles:

   - ***User must change password*** **-** if set to ***On***, the new user must change their password the first time they log in.

   This makes it possible to assign a predetermined password to a user and then force them to change it for security purposes. Users should configure when the password will expire from the ***Password Complexity*** *section.*

   - ***Enabled*** **-** if set to ***On***, the user can log in to VideoManager. If set to ***Off***, the user cannot log in.

7. In the ***Roles*** panel, select the roles to be assigned to the user. The user's roles can be altered later.

8. In the + ***Sharing*** panel, select the sharing options required for the user:

   - **Auto Share With -** if the videos captured by this user should be automatically shared with other users on the system, enter the names of these users and click ***Add***.

   Users cannot see who their videos are auto-shared with, or if they are auto-shared at all.

   - **Supervised Users -** if the new user should supervise other users on the system, enter the names of these users and click ***Add***. The supervising user will be able to view all supervised videos under the ***Supervised Videos*** pane of the ***Videos*** tab.

9. If required, add ***user-specific WiFi networks***. These are networks which only appear on the user's account, and are not viewable by other on the system.

>> For more information, see Create, Edit and Delete User-Specific WiFi Networks on page 239.

To edit a user:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Users*** section.
4. Next to the user to be edited, click ***Edit User***.

   The ***Edit User*** window opens.
5. Make the necessary changes.

It is also possible to reassign a user. This is necessary if a user has left an organisation and they should no longer have access to VideoManager. Reassigning them will transfer all of their videos and incidents to another user. To do so:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Users*** section.
4. Click ***Reassign User*** in the top right-hand corner.
5. When prompted, enter the names of the user which is redundant, and the user which their information will be transferred to.

To delete a user:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Users*** section.
4. Click ***Delete User***.

   A confirmation window will open.
5. Click ***Yes***.

9.1.2 Create, Edit, Copy and Delete Roles

A role is a collection of permissions within VideoManager, which can then be assigned to users. Because of this, roles dictate what actions users can take on VideoManager, and what aspects of the UI they can see. Each user can have several roles assigned to them. This is done from the ***Roles*** section of the ***People*** pane, in the ***Admin*** tab.

VideoManager provides the following default roles:

- ***System Administrator*** - users assigned to this role can access all aspects of the VideoManager UI (e.g. deleting incidents, creating other users, etc.).
- ***Device Operator*** - users assigned to this role can record videos. They cannot perform any other actions on VideoManager, and do not have the ability to log in.
- ***System User*** - users assigned to this role can view their own videos, and videos shared with them. They cannot operate devices, or access the ***Admin*** tab.
- ***System Supervisor*** - users assigned to this role can view own videos and those recorded by users they are supervising. They cannot operate devices, or access the ***Admin*** tab.
- ***System Manager*** - users assigned to this role can view own, supervised and system-wide videos. They can, however, assign devices and perform actions on incidents.

*Every default role except **System Administrator** can be edited manually.*

However, users may sometimes find it necessary to create their own roles, tailored to their workflow. Creating unique roles is a simple process.

To create a role:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Roles*** section.
4. Click ***Create Role***.

5. Configure role properties.

>> For more information, see Configure Role Properties on the next page

6. Configure permissions for the role.

>> For more information, see Enabled and Disable Permissions on page 142

7. Click ***Create Role*** to save the role.

Roles can also be copied.

1. Next to the role to be copied, click Copy Role.

   The ***New Role*** window opens.

2. Click ***Copy Role***.

   The role will be copied and opened for editing.

To edit a role:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Roles*** section.
4. Next to the role to be edited, click > ***Go To Role***.

   The ***Edit Role*** window opens.

To delete a role:

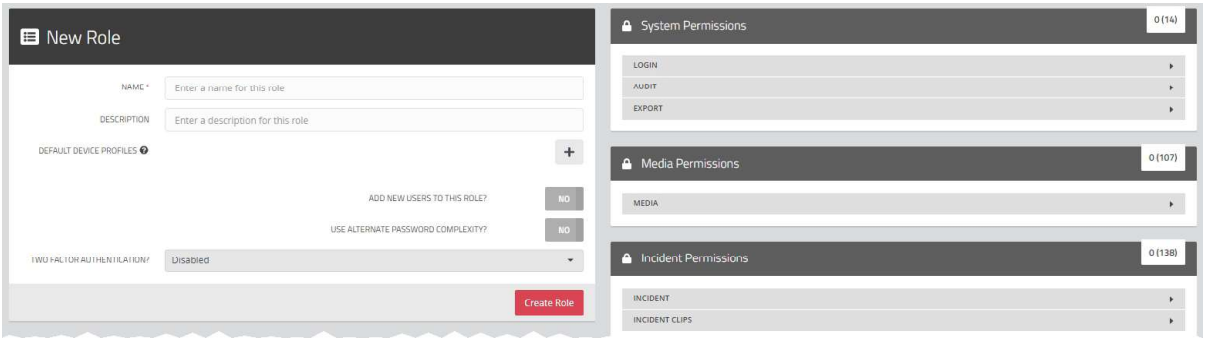
1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Roles*** section.
4. Click ***Delete Role***.

   A confirmation window will open.

5. Click ***Yes***.

Configure Role Properties

Role properties dictate the name, description, default device profile, and two factor authentication settings of the role in question. They can be configured while a role is being created or edited.



To configure role properties:

1. Navigate to the ***Admin*** tab.
2. Select the ***People*** pane.
3. Click the ***Roles*** section.
4. Click ***Create Role*** or ***Go To Role***, if an already-existing role is being edited.

   The ***New Role*** or ***Edit Role*** screen opens.
5. Enter the following information for the new role:
   - **Name -** enter a name for this role.
   - **Description -** enter a description for this role.
   - **Default device profile -** Devices controlled by users in this role will use the device profile selected here. Devices assigned with RFID will use this device profile automatically. Devices assigned manually will give users the option to override this device profile if they have the correct permissions.

   A user should choose a device profile for each device family (VB-400, VB-100 / VB-200 / VB-300, and VideoTag). If they do not, the default device profile will be used.

   If a user belongs to multiple roles, but all of the roles' device profiles are set to the system default except one, the one which is **not** the system default will be used.

If a user belongs to multiple roles, but some of the roles' device profiles aren't set to the system default, the device profile which is **highest** in the device profile list (apart from the default profile) will be used.

*This list can be reordered from the **Device Settings** section of the **Devices** pane, in the **Admin** tab. From here, users can also change the system default device profile.*

6. Set additional options for the new role using the following toggles:

   - ***Add new users to this role?*** - if set ***On***, then any new users added to VideoManager from now onwards will automatically inhabit this role.
   - ***Use alternate password complexity?*** - if enabled, the user must set a password which conforms to the alternate password rules, instead of the normal password rules.
   - ***Two factor authentication*** - Although some aspects of two factor authentication can be configured from this pane, it is a multi-step process.

   >> For more information, see Configure Two Factor Authentication on page 242.

7. Set the permissions for the role using the toggles. These can be changed at any time.

>> For more information, see Enable and Disable Permissions on the next page

8. Click ***Create Role***.

The role is created with the chosen permissions and options.

Enable and Disable Permissions

A permission is an individual rule which dictates the actions users can perform on VideoManager.

There is a comprehensive list of all permissions in the appendix section.

>> For more information, see Appendix A: Permissions on page 298

A user's permissions are the union of their roles. This means that if a user belongs to two roles, one of which has the permission ***Login to VideoManager application*** enabled and one of which does not, that user will still be able to log in.

There are no permissions which deny an action - only the absence of permissions denies actions.

There are eight groups of permissions:

- System permissions - this controls users' abilities to log in to VideoManager, as well as their audit and export abilities.
- Video permissions- this controls users' abilities regarding videos. The permissions are also sorted by four criteria:
  - ***OWNED*** - if enabled, users can perform actions on the videos created by them.
  - ***SHARED*** - if enabled, users can perform actions on the videos that have been shared with them by other users on the system.
  - ***SUPERVISED*** - if enabled, users can perform actions on the videos that have been created by other users on the system that they supervise.
  - ***ANY*** - if enabled, users can perform actions on any videos on the system, regardless of who created them.
- Incident permissions -this controls users' abilities regarding incidents. The permissions are also sorted by four criteria:
  - ***OWNED*** - if enabled, users can perform actions on the incidents created by them.
  - ***SHARED*** - if enabled, users can perform actions on the incidents that have been shared with them by other users on the system.
  - ***SUPERVISED*** - if enabled, users can perform actions on the incidents that have been created by other users on the system that they supervise.

- ***ANY*** - if enabled, users can perform actions on any incidents on the system, regardless of who created them.

In the incident permissions section, it is also possible to determine which access groups users in that role will belong to. Access groups control what user-defined fields and saved searches users can see.

>> For more information, see Export, Import, and Create User-defined Fields on page 178 and Create, Edit and Delete Saved Searches on page 45

- Device permissions - this controls users' abilities regarding devices. The permissions are also sorted by four criteria:
  - ***USER*** - if enabled, users can perform actions on the devices assigned to them.
  - ***SUPERVISED*** - if enabled, users can perform actions on the devices that are assigned to them or other users on the system that they supervise.
  - ***ANY*** - if enabled, users can perform actions on any device on the system.
- User permissions - this controls users' abilities regarding devices. The permissions are also sorted by two criteria:
  - ***SUPERVISED*** - if enabled, users can perform actions on the users on the system that they supervise.
  - ***ANY*** - if enabled, users can perform actions on any user on the system.
- Notification permissions - this controls how notifications work (if they have been licensed).
- Report permissions - this controls users' abilities to create reports and view statistics.
- Advanced permissions - this controls users' abilities regarding advanced aspects of VideoManager. The permissions are also sorted by two criteria:
  - ***View*** - if enabled, users can view certain aspects of VideoManager which would otherwise be inaccessible.

- ***Edit*** - if enabled, users can edit certain aspects of VideoManager.

9.2 Devices

In the ***Devices*** pane, users can edit aspects of VideoManager related to device configuration.

To access the ***Devices*** pane:

1. Navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.

From here, users can access:

- ***Device Profiles***

Import, edit, and delete device profiles.

>> For more information, see Create, Edit, Reorder and Delete Device Profiles on page 146

- ***Device Settings***

Edit device settings for all devices connected to VideoManager.

>> For more information, see Edit Device Settings on page 149

- ***Access Control Key Management***

Import, edit, and delete access control keys.

>> For more information, see Create, Import, and Export Access Control Keys on page 151

9.2.1 Create, Edit, Reorder and Delete Device Profiles

Device Profiles are used to control the interface between VideoBadges and VideoManager, as well as the recording behaviour and settings. This is done from the ***Device Profiles*** section of the ***Devices*** pane, in the ***Admin*** tab.

To search for already-created device profiles:

1. Navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.
3. Click the ***Device Profiles*** section.
4. In the ***Filter By Family*** dropdown, select one of the following options:
   - **VideoBadge 400 -** this will only show device profiles that are applicable to VB-400s.
   - **VideoBadge 100 / 200 / 300 -** this will only show device profiles that are applicable to VB-300s/VB-200s/VB-100s.
   - **VideoTag 50 / 100 -** this will only show device profiles that are applicable to VideoTags.

> *Device families which are not present on the user's instance of VideoManager will still be an option in the dropdown, even if no device profiles will be returned.*

To create a new device profile:

1. Navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.

3. Click the ***Device Profiles*** section.
4. Click ***Create profile***.
5. In the ***Details*** pane, enter a name for the device profile. Select the device family the device profile will apply to, from the ***Device Family*** dropdown.

Caution *This cannot be changed later.*

The options for the device profile's family are as follows:

- **VideoBadge 400**
- **VideoBadge 100 / 200 / 300**
- **VideoTag 50 / 100**

6. There are 5 areas which sufficiently privileged users can control. Not all areas apply to all device families. These areas are:
   - ***Notifications & Alarms*** - how a VideoBadge utilises its LEDs and sound.
   - ***Power Management*** - how a VideoBadge conserves its battery.
   - ***Recording Behaviour*** - how a VideoBadge records footage.
   - ***Video Settings*** - the quality at which a VideoBadge records footage.
   - ***Controls*** - how a VideoBadge's buttons act when pressed.

>> For more information, see Appendix B: Device Profiles on page 326.

7. Click ***Save Settings*** to save the device profile.

To edit a device profile:

1. Navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.
3. Click the ***Device Profiles*** section.

4. Find the relevant device profile by selecting a device type from the **Filter by family** dropdown.
5. Next to the profile to be edited, click ***Edit profile***.

Users can also reorder device profiles. This is necessary if a user belongs to multiple roles with different assigned device profiles. The device profile which is **highest** in the list here will be the one given to the device. Furthermore, the device profile which is **highest overall** in the list will be the system default. To reorder device profiles:

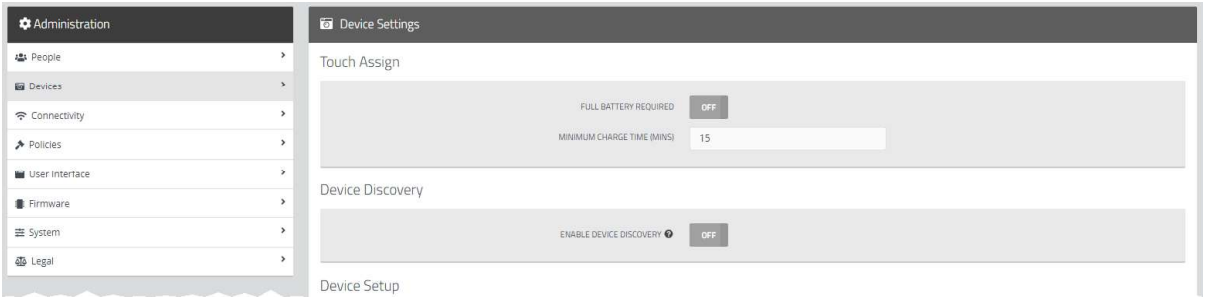
1. Navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.
3. Click the ***Device Profiles*** section.
4. Find the relevant device profiles by selecting a device type from the **Filter by family** dropdown.
5. Click ***Reorder profiles***.

To delete a device profile:

1. Navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.
3. Click the ***Device Profiles*** section.
4. Next to the profile to be edited, click ***Delete profile***.

9.2.2 Edit Device Settings

Any settings configured here will apply to all devices connected to VideoManager. This is done from the ***Device Settings*** section of the ***Devices*** pane, in the ***Admin*** tab.



To reach the ***Device Settings*** section:

1. Navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.
3. Click the ***Device Settings*** section.

There are multiple categories which users can configure:

1. ***Touch Assign*** - this gives users the option to toggle whether Touch Assign is only possible with a full battery. If set to ***Off***, the user will be given an option to enter a minimum charge time, before which the device cannot be assigned by RFID. The exception for this is devices which have been permanently allocated to a user - in this case, they can be tapped out by RFID even when they have not met the minimum charge time.

2. ***Device Discovery*** - this gives users the option to toggle whether device discovery is on or off. If set to ***Off***, VideoManager will only discover VideoBadges and VideoTags which are connected to DockControllers. Any devices connected by USB will **not** appear on the ***Devices*** tab.

3. ***Device Setup*** - this pane gives users control over three settings:

    - ***Default Device Assignment Mode*** - this dropdown gives users the ability to choose which device assignment mode is the default. They are as follows:

        - **Single Issue** (pool) - the device will be assigned to the user and when it is redocked, it will become unassigned and must be reassigned manually.

        - RFID assignment (pool) - this allows users to undock devices quickly, in case of an emergency. One default user is "assigned"

an entire organisation's devices, which are then tapped out by individual users. When the devices are redocked, all footage is associated with the default user.

>> For more information, see Bulk Touch Assign on page 99

- **Permanent Issue** (personal) - the device will be assigned to the user and when it is redocked, it will stay assigned to the same user.
- **Permanent Allocation** (personal) - the device will be allocated to the user, who must then tap an RFID tag before they can use it in the field. When it is redocked, it will stay assigned to the same user.

In the **Device Field Trip**, **Operator Recorder Summary**, *and* **User Summary** *reports, devices in this mode will be marked as Unassigned if they have been allocated but not tapped out with an RFID tag.*

- ***Show public QR code bootstrap screen***

>> For more information, see Generate Device Config Codes on page 101

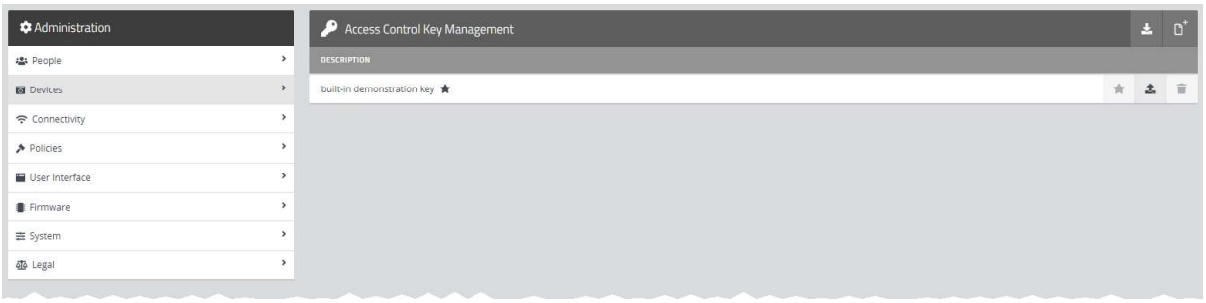
- ***Configure external application credentials*** - this should only be toggled to ***On*** if directed to do so by Edesix support.

4. ***Device Downloads*** - this pane gives users control over two settings:

- ***Limit simultaneous downloads to*** - here, users can set the limit for the number of simultaneous downloads. If the download number is set to 10, then only 10 devices can download footage simultaneously. Once one device finishes downloading, another device will take its place.
- ***Fast Download Recovery*** - this determines whether, when a device's file download is interrupted, the download is suspended and then resumed from the **same point** once connection is reestablished.

9.2.3 Create, Import, and Export Access Control Keys

Access Control Keys are the mechanism that VideoManager uses to encrypt videos and prevent VideoBadges communicating with unauthorised instances of VideoManager. This is done from the ***Access Control Key Management*** section of the ***Devices*** pane, in the ***Admin*** tab.



To create an access control key:

1. Navigate to the ***Admin*** tab.
2. Select the ***Devices*** pane.
3. Click the ***Access Control Key Management*** section.
4. Click ***Create key***.
5. Enter a description for the access control key.
6. Click ***Create key***.
7. Once an access control key has been created, the user can make it the default, by which all new or factory reset VideoBadges are authenticated, by clicking the ***Set as default key*** star.

> *It is recommended that all access control keys are exported upon creation to somewhere secure - in event of a system failure, this will ensure that users can still access footage on their devices that has not been uploaded already.*

If a user wishes to move their device to another instance of VideoManager, they **must** import their access control key into that instance of VideoManager - otherwise, the device will appear as **locked** and they will not be able to access any footage on the device which has not already been downloaded. To do so:

1. In the original VideoManager instance, next to the access control key, click ***Export key***.

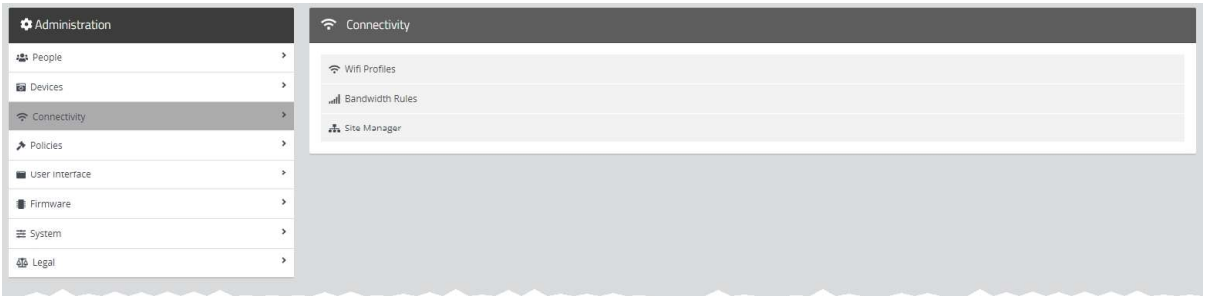
The access control key is downloaded to the user's PC.

2. In the new instance of VideoManager, click ***Import key***.

Select the previously downloaded key.

9.3 Connectivity

In the ***Connectivity*** tab, users can edit aspects of VideoManager related to WiFi and sites.



To access the ***Connectivity*** tab:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.

From here, users can access:

- ***WiFi Profiles***

Create, edit, and delete WiFi profiles.

>> For more information, see Create, Edit and Delete WiFi Profiles on page 154

- ***Bandwidth Rules***

Configure bandwidth rules.

>> For more information, see Create, Edit and Delete Bandwidth Rules on page 158

- ***Auto Fetch***

Configure autofetch if VideoManager is enabled as a Central VideoManager.

>> For more information, see Configure Auto Fetch on page 161

- ***Site Manager***

Configure sites.

>> For more information, see Configure Site Manager on page 164

9.3.1 Create, Edit and Delete WiFi Profiles

VideoManager uses WiFi Profiles to control the connectivity options available. They allow users to quickly and easily configure a large number of VideoBadge VB-300s and VideoTags for deployment. This is done from the ***WiFi Profiles*** section of the ***Connectivity*** pane, in the ***Admin*** tab.

The steps for configuring a VideoBadge and VideoTag are different. This documentation will cover both aspects.

To create a new WiFi profile:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***WiFi Profiles*** section.
4. Click ***Create wifi profile***.

Enter the following information for the WiFi profile (this will apply to all VB-300s and VideoTags which use the profile in question):

- ***Name*** - enter a name for the WiFi profile.
- ***Default profile*** - if this WiFi profile will be the default, toggle this to ***On***.

To add a new network, click ***Add network***. There are many variables which can be changed:

- ***SSID*** - enter the SSID of the WiFi network.
- ***Passphrase*** - enter the WiFi network's passphrase.

These credentials can usually be found on the bottom of the WiFi router.

- Enter the networks that the VB-300 will be required to connect to. The user has a choice of either ***Any***, ***2.4GHz only***, or ***5GHz only***.
- ***Disconnect on low signal*** - determine whether devices will disconnect from the network if it has a low signal.

- ***Hidden network*** - if the VideoBadge is to connect to a mobile hotspot, configure the hotspot as one of the profile's User-specific networks.

If a network is to be used with VideoBadge View, set the ***VideoBadge View*** toggle to **On**.

At this stage, users may also wish to select ***User-specific networks***. If they choose to do so, an option will appear to configure VideoTag settings for all user-specific wifi networks on the user's account.

>> For more information, see Create, Edit and Delete User-Specific WiFi Networks on page 239.

*Prioritise the networks using the arrows next to the **Advanced** control. The first network shown will be the one which devices attempt to connect to first, while the last in the list will only be used if all the others are unavailable.*

Users can also configure VideoBadge-specific settings for an entire profile.

- If WiFi streaming is necessary, ***Enable Streaming*** must be turned on.
- For Video Downloads, ***Download video over Wifi*** must be turned on. If bookmarking is turned on in the Device Profile, only bookmarked videos will be downloaded over WiFi. If it is turned off, all videos will be downloaded over WiFi.

There are multiple choices for configuring a VideoTag as well. Unlike VideoBadge settings, which apply to an entire WiFi profile, VideoTag settings are only specific to a network. For this reason, they must be re-configured for every new network which is added to a WiFi profile.

- Enable streaming - this allows users with appropriate permissions to view live streamed footage over VideoManager from VT-50 devices in the field.
- Enable docking - this makes it possible to administer a VT-50 wirelessly over WiFi.

To edit a WiFi profile:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.

3. Click the ***WiFi Profiles*** section.
4. Next to the profile to be edited, click ***Edit profile***.

To delete a WiFi profile:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***WiFi Profiles*** section.
4. Next to the profile to be deleted, click ***Remove profile***.

To duplicate a WiFi profile:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***WiFi Profiles*** section.
4. Next to the profile to be duplicated, click ***Duplicate***.
5. The ***Create Wifi Profile*** pane opens, with the original WiFi profile's information pre-set.

To export a WiFi profile:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***WiFi Profiles*** section.
4. Next to the profile to be exported, click ***Export wifi profile***.

   The WiFi profile will be exported to the PC's default download location, and can be imported to other instances of VideoManager.

To import a WiFi profile:

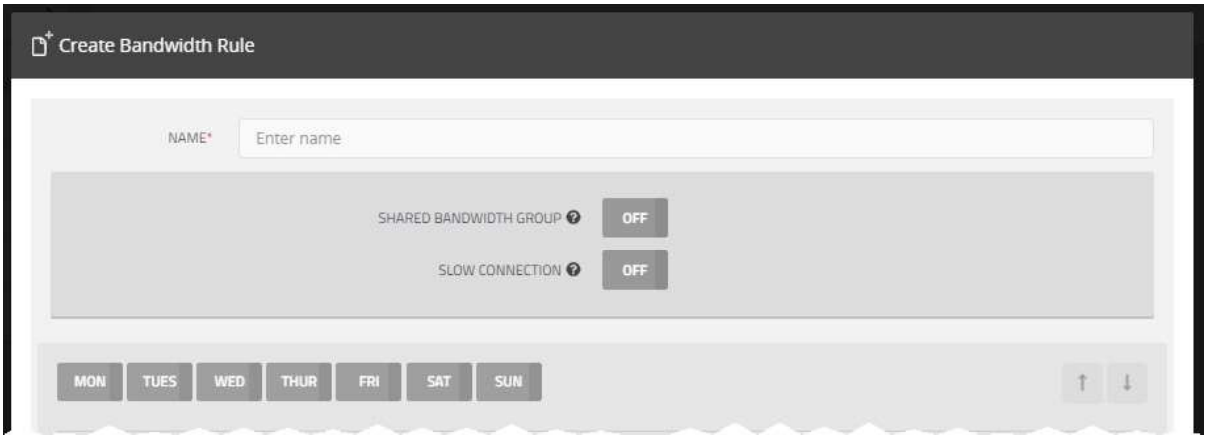
1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.

3. Click the ***WiFi Profiles*** section.
4. Next to the profile to be exported, click ***Import wifi profile***.
5. Select the relevant file from the user's PC.
6. Click ***Import***.

The WiFi profile will now appear on the user's instance of VideoManager.

9.3.2 Create, Edit and Delete Bandwidth Rules

Administrators may wish to configure bandwidth rules, which affect how much bandwidth is used when uploading data from sites to the Central VideoManager. Bandwidth Rules are configured from the Central VideoManager and can then be applied on a per-site basis. Users can add as many restrictions as they want to a bandwidth rule. This is done from the ***Bandwidth Rules*** section of the ***Connectivity*** pane, in the ***Admin*** tab.



To create a bandwidth rule:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***Bandwidth Rules*** section.
4. Click ***Create Bandwidth Rule***.
5. Toggle whether ***Shared Bandwidth Group*** is set to ***On*** or ***Off***.

   This only applies to DockControllers. If set to ***On***, all DockControllers who are added to this rule will be part of the same "group" and will share the same bandwidth limit. This is useful if multiple DockControllers are on the same network connection, and a user wants to stagger the uploads.

6. Toggle whether ***Slow Connection*** is set to ***On*** or ***Off***.

   This only applies to DockControllers. If set to ***On***, all DockControllers who are added to this rule will continuously upload footage to VideoManager, ignoring the overall download limit. This is useful if the DockControllers in question have a slow network connection.

7. Click ***Add rule*** to create an individual rule. This gives users the following configuration options:

1. What day(s) of the week when the rule will occur.
2. The time of day when the rule will occur.
3. The maximum amount of bandwidth that should be used during that period.

Users can create multiple rules within one bandwidth rules, using the ⊕ ***Add rule*** control. This is useful if there are certain "busy" times when footage and other data should not be offloaded, and other "quiet" times when footage and data should be offloaded.

If there are multiple rules within one bandwidth rule, users should order them using the ↑ ↓ controls next to each rule. If there are two overlapping rules (e.g. two rules both applying to Saturday), the rule which is **highest** in the list will take priority.

To apply a bandwidth rule to a DockController:

1. Navigate to the ***Devices*** tab, and select the ***DockControllers*** pane.
2. Find the relevant DockController, and click > ***View details*** next to it.

   Users can filter by **Name**, **Serial**, and **Version**.
3. In the ***Bandwidth Rule*** pane, click the dropdown menu.

   Select the relevant rule.
4. Toggle whether ***High Priority DockController*** is set to ***On*** or ***Off***.

   If set to ***On***, all footage from this DockController will be uploaded as quickly as possible - this means that if the DockController is part of a bandwidth rule that has the ***Shared Bandwidth Group*** setting enabled, it will halt the downloads of other DockControllers in the group until all of its footage has been uploaded.

To copy a bandwidth rule:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***Bandwidth Rules*** section.
4. Click ***Copy Bandwidth Rule***.

   The ***Copy Bandwidth Rule*** window will open.

5. Make any changes which are required.
6. Click ***Save Bandwidth Rule*** to save the rule.

To edit an existing bandwidth rule:

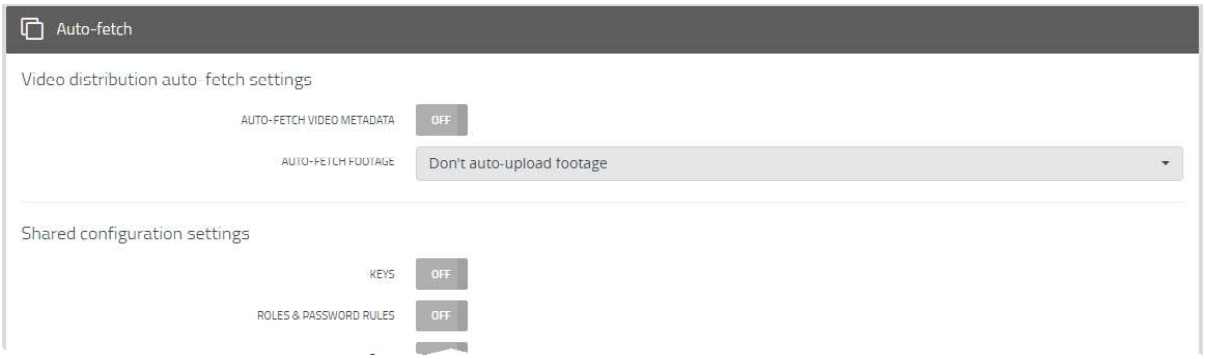
1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***Bandwidth Rules*** section.
4. Click ***Edit Bandwidth Rule***.
5. Make any changes which are required.
6. Click ***Save Bandwidth Rule*** to save the rule.

To delete a bandwidth rule:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***Bandwidth Rules*** section.
4. Next to the relevant bandwidth rule, click ***Delete Bandwidth Rule***

9.3.3 Configure Auto Fetch

It is possible to share the configuration of a Central VideoManager with all the sites that connect to it. In a Central VideoManager, these settings can be controlled within the ***Auto Fetch*** section of the ***Connectivity*** pane in the ***Admin*** tab. The ***Auto Fetch*** section is only visible from a Central VideoManager - if VideoManager is configured as a site, it is not visible.



To reach the ***Auto Fetch*** section:

1. Navigate to the ***Admin*** tab.
2. Select the ***Connectivity*** pane.
3. Click the ***Auto Fetch*** section.

There are multiple categories that users can configure.

Auto-fetch

- ***Auto-fetch video metadata*** - if enabled, this will transfer metadata for all site footage. This metadata will be displayed in the the Central VideoManager.
- ***Auto-fetch footage*** - this changes how footage is uploaded from a site to a Central VideoManager.
  - **Don't auto-upload footage** - no footage from a site will be uploaded automatically. This is useful if the user's Central VideoManager does not have a lot of storage.
  - **Auto-upload incident footage** - only footage that is part of an incident will be uploaded automatically (this includes the entire video if the footage has been clipped for the incident), as soon as the incident has been created.
  - **Auto-upload footage from committed incidents** - only footage that is part of an incident when has been **manually** taken control of will be uploaded automatically.

>> For more information, see Commit Incidents on page 87.

- **Auto-upload all footage -** all footage on the site will be uploaded automatically, regardless of whether it is in an incident or not. This is only recommended if the user's Central VideoManager has a lot of storage.

>> For more information, see Create and Edit Sites on page 249.

- ***Replicate Device States and Locations* -** if enabled, this will show all devices connected to sites on the ***Devices*** tab of the Central VideoManager.

***Shared configuration settings* -** settings configured here in the Central VideoManager will be synchronised with all sites connected to it.

- ***Keys* -** this will share access control keys, allowing VideoBadges assigned at one site to be docked at any other, if necessary.
- ***Roles & password rules* -** sharing roles allows users to inhabit the same roles across all devices in an organisation - this is much less time-consuming than manually creating the same role in each individual VideoManager.
- ***Users* -** sharing users avoids the necessity to add each user to each site as required. It should be noted that it is best practice to share both ***Roles & password rules*** and ***Users***, or neither.
- ***Device profiles* -** this shares device profiles configured on the Central VideoManager with its sites.
- ***Deletion policies* -** if enabled, this switch will share all deletion policies across sites to ensure consistency.
- ***User-defined Fields* -** while it is possible to export and import user-defined fields in VideoManager, this option will keep all sites updated without the need to manually copy new or altered fields.
- ***Firmware and Upgrade Policy* -** if enabled, this will synchronise the firmware and upgrade policies configured from the ***Auto Upgrade Settings*** pane.
- ***Synchronise Clocks* -** if enabled, this will synchronise all EdgeControllers with the central VideoManager clock.

> *Users with sufficient permissions can still make changes to these settings on their site (e.g. changing the default device profile). However, the moment the relevant setting is changed in the Central VideoManager, any changes made on the site will be overwritten.*

Video distribution monitor settings **-** these settings govern the upload of footage from sites to the Central VideoManager.

- ***Congestion warning*** **-** if enabled, VideoManager will display a warning if a video takes more than a defined amount of time to upload from a site to the Central VideoManager. The actual length of time, after which the warning will be shown, can be configured once it has been set to ***On***.
- ***Auto-Cancel*** **-** if enabled, VideoManager will automatically cancel an upload if it takes more than a configurable time to upload from a site to the Central VideoManager. The actual length of time, after which the upload will be canceled, can be configured once the it has been set to ***On***.

9.3.4 Configure Site Manager

From the ***Site Manager*** pane, users can toggle whether their instance of VideoManager is acting as a site or not. This will not be available if VideoManager is already acting as a site centre.

If VideoManager is configured to act as a Central VideoManager, this pane will be unavailable.

>> For more information, see Enable and Configure a Central VideoManager on page 248

To enable an instance of VideoManager to act as a site:

1. Toggle ***Connect to a server?*** to ***On***.

   Users will now be given the opportunity to configure the site

2. Enter the ***Server address*** and ***Port***.

3. Enter ***This site's identifier*** and ***This site's password*** - these will have already been set from the central VideoManager.

4. Click ***Save Settings***.

The instance of VideoManager should now be functioning as a site.