MOTOROLA SOLUTIONS Unity Video Privilege Management User Guide

Contents

Unity Video Privilege Management

Avigilon Unity Video
Privilege Management User Guide

© 2023, Avigilon Corporation. All rights reserved. MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. Unless stated explicitly and in writing, no license is granted with respect to any copyright, industrial design, trademark, patent or other intellectual property rights of Avigilon Corporation or its licensors.

This document has been compiled and published using product descriptions and specifications available at the time of publication. The contents of this document and the specifications of the products discussed herein are subject to change without notice. Avigilon Corporation reserves the right to make any such changes without notice. Neither Avigilon Corporation nor any of its affiliated companies: (1) guarantees the completeness or accuracy of the information contained in this document; or (2) is responsible for your use of, or reliance on, the information. Avigilon Corporation shall not be responsible for any losses or damages (including consequential damages) caused by reliance on the information presented herein.

Avigilon Corporation avigilon.com
PDF-UNITY-VIDEO-PRIVILEGE-MANAGEMENT-H
Revision: 1 – EN
20231127

Privilege Management

Privilege Management lets large organizations achieve better global monitoring and control of user access and permissions from one screen in the cloud. Changes made to user access in the cloud are automatically synchronized with the Avigilon Unity sites. Administrators can give users access only to the areas they need, and specify what users can do.

NOTE

Privilege Management is only available for organizations using Avigilon Unity 8.0.4 or newer.

User Privileges and Access Management

Managing user privileges and permission will always involve users, user groups, roles and policies. These elements are essential for managing user accounts, limiting access and preventing users from accessing or performing actions outside of the scope of their job. Regular review of policies and user groups will ensure that user access is properly managed across your organization.

Menu	Main Tasks
Users Tab	Manually add users and then add them to one or more groups. Users inherit the roles assigned to a group.
User groups Tab	Add new groups and assign users to groups.
Roles Tab	Create a role (define a set of privileges) based on job responsibility.
Policies Tab	Create a policy that grants a User Group a Role for a set of sites or devices within a s ite.

IMPORTANT
User access takes effect only when a policy is defined with one or more user groups, one role and one or more sites.

Managing Users

Users are granted access to specific sites or devices or granted the ability to perform certain tasks through group membership. This way, users inherit the same permissions and privileges assigned to their group. Users can belong to more than one group depending on the access and permissions they require. Time is saved by updating users at the group level, removing the need to update individual user accounts.
Tasks that you can perform include:

- Adding a User
- Adding a User to More Groups
- Searching for a User
- Updating a User Profile
- Removing a User from a Group
- Deleting a User from Your System
- Verifying Group Membership and Associated Group Policies

Adding a User

After manually adding a user, you must assign each user to one or more groups.

1. Select the Users tab.
2. Select New user.
3. In the Create user pop-up, enter the user’s name and email address.
4. Click Create user.
   If the user:
   Does not exist in the system, they will receive an email inviting them to register their user account to access the organization.
   NOTE
   If the user has not received an invitation email, you can click the Resend invite button to resend the invitation.

Already exists in the system as a user in another organization, they will receive an email indicating that they have been added to a new organization, and to click the link in the email to sign in and view their account.

You will notice that the user is added to the Users page. In the User Groups column, a ⚠ None warning icon indicates the user has not been added to a group.

5. To add the user to a group, click the user row to display the User details page.
6. Click the User details drop-down.
7. Use the search box to find user groups that are not listed.
8. Select one or more check boxes.
9. Click Add to group.

The selected user groups are added to the User Groups area on the User details page. On the Users page, the user's name is displayed alongside the group.

Adding a User to More Groups

When a user needs more permissions and privileges due to a change in job responsibility or promotion, identify one or more groups that have the necessary permissions. Then you can add the user to those groups.

1. Click the 👤 Users tab.
2. If the user is not listed, enter the user name or email address in the search box.
3. In the user list, select the user.
4. In the User Groups area, select the Add groups drop-down.
5. In the list of user groups, select one or more user group check boxes to add the user to the groups.
6. Click Add to groups.

Searching a User

When there are many users in the system, you can search for a user by first or last name, or by email address.

💡 **TIP**

You can also filter the columns on the page by clicking the small arrow on the column headers.

1. Select the 👤 Users tab.
2. In the search box, enter a name or email address.

Updating a User Profile

You can update a user's first and last name. Note that the profiles of federated users cannot be modified in Avigilon Unity Privilege Management.

1. Click the 👤 Users tab.
2. If the user is not listed, enter the user name in the search box.
3. In the list of users, select the user row.
4. In the Users details area, update the name.
5. Click Save changes.

Removing a User from a Group
Sometimes a user’s job responsibilities change in the organization. If the user no longer requires the privileges and permissions of a group they are a member of, you can remove them from the group.

1. Click the👤 Users tab.
2. If the user is not listed, enter the user name or email address of the user in the search box.
3. In the user list, select the user.
4. In the User Groups area, select the drop-down of the group that you want to remove the user from.
5. Click Remove from group.
6. To confirm, click Remove user to remove the user.

Deleting a User from Your System
You can permanently remove the user account of an employee who has left your organization.

1. Click the 👤Users tab.
2. If the user is not listed, enter the user name or email address in the search box.
3. In the user list, select the user that you want to remove.
4. On the User details page, click 🗑next to the user’s name.
5. To remove the user, click Delete user.

Now, the user will be unable to sign in again.

Verifying Group Membership and Associated Group Policies
Before adding a user to a group, you can verify a group’s policy and membership to confirm that the group’s access
corresponds to the access requirements of the user.

1. In the 👤Users tab, select the user to display the Users details page.
2. Click the More 3 dots context menu, and then click ↗ Manage user groups.
3. Select the group to view the User Groups details page.

- The Group policies area lists policies associated with the group.
- Members of the group are listed below.

Managing User Groups

A group is assigned access rights via a policy. When users are added to one or more groups, they inherit the access rights assigned to those groups. For example, if a user needs access to view live video, they can be added to a group assigned with the privilege to view live video.
The Organization Administrators group is the only predefined user group reserved for administrators responsible for managing user access for the organization, and cannot be deleted. When a new organization is created in the system, it automatically assigns the primary administrator to this group. The primary administrator can then add other administrators who can also view and manage user access for the organization.
Tasks that you can perform include:

- Creating a Group
- Updating a Group
- Searching for a Group
- Adding a Group to a Policy
- Adding Users to a Group
- Removing a Policy or Users from a Group
- Removing a Group from the System

Creating a Group
After you create a user group, you can add more than one policy to a group to grant privileges to the group.

1. Click the User groups tab.
2. On the User Groups page, click New user group.
3. On the Create a User Group pop-up, enter a group name.
4. Click Create User Group.

A User groups details page appears. Depending on your workflow, you can either add policies or users to the group.

If you navigate away from the User groups page and then return, note that the new group’s Policy column displays a None warning icon to indicate that the group has not yet been assigned a policy.

Updating a Group Name
You can modify the name of a user group.

1. Select the User groups tab.
2. From the list of user groups, select the group to display the User Groupsdetails page.
3. In the Group name box, modify the group name.
4. Click Save changes.

Searching a Group
To avoid scrolling through pages of groups if your organization is large, use the search box to obtain faster results.

1. Select the User groups tab.
2. In the search box, begin entering the group name to auto-populate with user group matches.

Adding a Group to a Policy

If you previously created a group, and did not associate it with a policy, a None warning icon is displayed in the
Policy column of the group on the User groups page. You can quickly associate a group to a policy.

1. Click the User groups tab.
2. On the User groups page, select a user group to display the User Groups details page.
3. Click the Add policy drop-down, and select the check boxes of one or more policies.

4. Click Add to group.
5. On the pop-up, click Add to group.

Adding Users to a Group

If you identify users that should be members of a specific group, you can easily add them.

1. Select the 👥 User groups tab.
2. From the list of user groups, select the group to display the User group details page.
3. In the Group members area, select the Add members drop-down to expand a list of members.

   TIP

   To find a user who is not listed, enter the user name in the search box.
4. Click one or more check boxes of users in the list, and then click Add to group.
5. To confirm, click Add to group to add users to the user group.

Removing a Policy or Users from a Group

You can restrict a group's access to a policy.

1. Select 👥 User groups.
2. On the User Groups page, select the group.
3. To remove a policy from the group:

   a. In the Group policies area, select the policy drop-down.

   b. Click Remove from group.

   c. To confirm, click Remove from group to remove the policy from the group.
4. To remove a user from the group:

   a. In the list of users below, Click 🗑 in a user row.

   b. To confirm, click Remove user from group.

Deleting a Group from the System

IMPORTANT

Deleting a group from the system may impact a number of policies.

1. Select 👥 Add to group.
2. On the User Groups page, select the group.
3. Beside the Group name, click 🗑.
4. To confirm, click Delete group to remove the user group.

Managing Roles

Roles restrict access to ensure that only authorized users are able to perform specific tasks. Create roles to represent various job responsibilities; for example, organization administrator, IT manager, and security officer. As the only predefined role, the Organization Administrator role has the unique privilege of managing users across the entire organization, and cannot be deleted from the system.

Tasks that can be performed in the Roles tab include:

- Creating a Role
- Updating a Role
- Searching for a Role
- Removing a Role

Creating a Role

You can create a role to match the job responsibilities and position of a specific group of users.

1. Click the Roles tab.
2. Click New role.
3. In the Role name box, enter a name.

   Next, you will define the privileges of a role.
4. For each category, select the check boxes of the privileges that will apply to the role.
5. Click Create role.

The role can now be associated with one or more policies.

Updating a Role

When a role changes in your organization, you can update the name or adjust the privileges of the role.

IMPORTANT

Be aware that modifying a role will affect all policies with the same role.

1. Select the Roles tab.
2. Select the role.
3. On the Roles page, make changes to the privileges by selecting or clearing the check boxes, as needed.
4. Select Save changes.

Searching a Role

1. Click the Roles tab.
2. In the search box, enter the name of the role.

Removing a Role

IMPORTANT

Removing a role from the system may impact a number of policies.

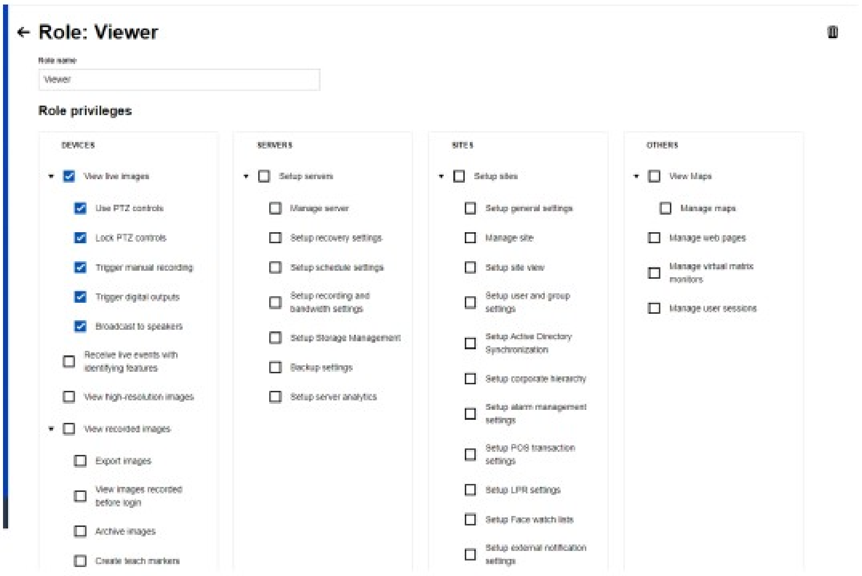
1. Click the Roles tab.
2. In the list of roles, select the role.

3. Click 🗑.
4. To confirm that you want to delete the role, click Delete role.

Managing Policies

With policies, you can set up rules that give a group of users access and the ability to perform specific actions across multiple sites in an organization. For a policy to take effect, it must consist of one or more groups that specify whocan perform actions, and a role that specifies what users can do on one or more sites and devices. As the only predefined policy, Organization Management Policy consists of the Organization Administrators group, the Organization Administrators role and access to all sites and devices in the organization.

IMPORTANT
User access takes effect only when a policy is defined with one or more user groups, one role and one or more sites.
Example: As part of a policy, the Viewer role could be assigned to a Viewer user group (of security guards) to enable the group to view live video on all cameras in Site 2.



← Role: Viewer

Role name: Viewer

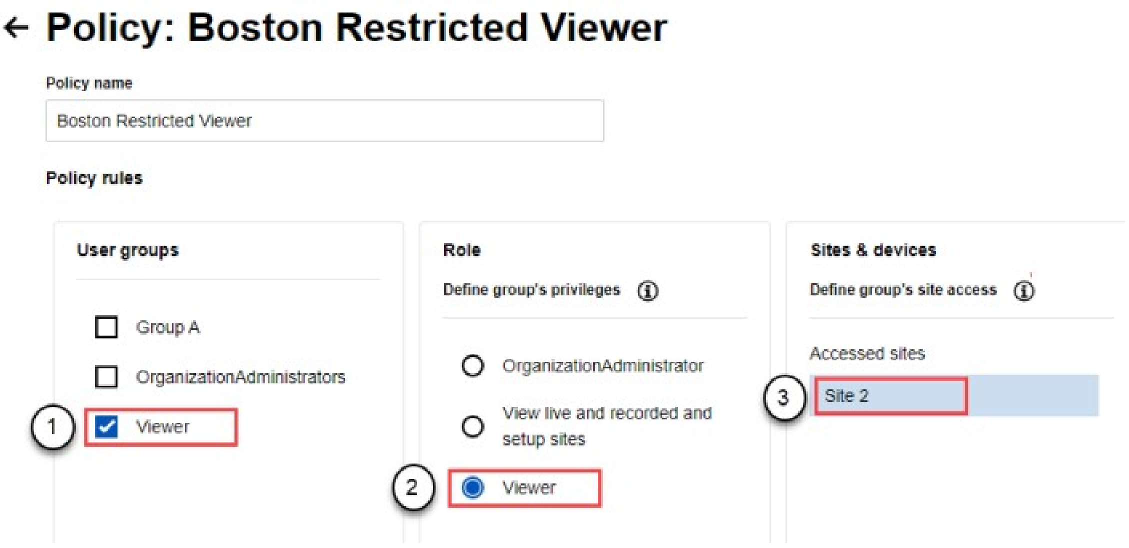
Role privileges

DEVICES
- ☑ View live images
  - ☑ Use PTZ controls
  - ☑ Lock PTZ controls
  - ☑ Trigger manual recording
  - ☑ Trigger digital outputs
  - ☑ Broadcast to speakers
- □ Receive live events with identifying features
- □ View high-resolution images
- □ View recorded images
  - □ Export images
  - □ View images recorded before login
  - □ Archive images
  - □ Create leach markers

SERVERS
- □ Setup servers
  - □ Manage server
  - □ Setup recovery settings
  - □ Setup schedule settings
  - □ Setup recording and bandwidth settings
  - □ Setup Storage Management
  - □ Backup settings
  - □ Setup server analytics

SITES
- □ Setup sites
  - □ Setup general settings
  - □ Manage site
  - □ Setup site view
  - □ Setup user and group settings
  - □ Setup Active Directory Synchronization
  - □ Setup corporate hierarchy
  - □ Setup alarm management settings
  - □ Setup POS transaction settings
  - □ Setup LPR settings
  - □ Setup Face watch lists
  - □ Setup external notification settings

OTHERS
- □ View Maps
  - □ Manage maps
- □ Manage web pages
- □ Manage virtual matrix monitors
- □ Manage user sessions



← Policy: Boston Restricted Viewer

Policy name: Boston Restricted Viewer

Policy rules

User groups
- □ Group A
- □ OrganizationAdministrators
- ☑ Viewer

Role
Define group's privileges
- ○ OrganizationAdministrator
- ○ View live and recorded and setup sites
- ● Viewer

Sites & devices
Define group's site access
Accessed sites
- Site 2

1. Viewer User Group is for security guard viewers
2. Viewer Role is for viewers of live video
3. Viewer User Group members with the Viewer role can access live video on site 2

Tasks that can be performed in the Policies tab include:

- Creating a Policy
- Searching for a Policy
- Updating a Policy
- Removing a Policy

Creating a Policy

1. Click the 🔑 Policies tab.
2. Click New policy to display the Create policy pop-up.
3. In the Policy name box, enter a name, and then click Create policy.
4. In the User groups column, select the check boxes of one or more user groups.
5. In the Role column, select a role.
6. In the Sites & devices column:

   a. Click + next to a site.
   b. In the Site access panel on the right, click the site drop-down arrow, and clear the check boxes of devices not required as part of the access policy, if any.
   c. Click Add site.
7. Click Save changes.

Searching a Policy

You can search a policy to verify that the correct privileges and resources for the policy are up-to-date.

1. Click the 🔑 Policies tab to view a list of policies.
2. If the policy is not listed, enter the name of the policy in the search box.

💡 **TIP**

Click the arrow in the User groups header to sort groups alphabetically.

Updating a Policy

When updating a policy, you can add or remove user groups, change the role, and grant or deny access to sites and devices.

1. Click the 🔑 Policies tab.
2. In the list of policies, select the policy to display the Policy details page.
3. Select or clear the check boxes in the User groups, as needed.
4. To update access to a site and devices:

   a. In the Sites & devices column, click ✎ next to the site.
   b. On the Site access panel on the right, click the site right arrow to view available devices.
   c. Select or clear the check boxes of the devices.
   d. Click Update site.

5. To remove access to a site:

   a. In the Sites & devices column, click next to the site.

   b. On the Site access panel on the right, click ✎ Remove site access.

   c. To confirm, click Remove site Remove site access to remove access to the site.

6. Click Save changes.

Removing a Policy
IMPORTANT
Removing a policy may impact a number of user groups.

1. Click the Policies tab.
2. In the list of policies, select the policy to display the Policy details page.
3. Click🗑.
4. To confirm, click Delete policy to remove the policy.

Scenarios

In this section, there are simple scenarios that walk through the steps to:
l Give a security guard access to control PTZ cameras for live video, but no access to view recorded video for a specific site.
l Give an Investigator access to recorded and archived video and the ability to export video for a site.
l Give a new user the same access rights as the primary administrator (OrganizationAdministrator), who has full access rights across the organization. This new user will then have the ability to grant user access to anyone in the organization.
Scenario – Security Guard
This section walks through a simple scenario that grants a security guard the ability to move/control the PTZ cameras but not to view recorded video on select cameras in a specific site.

1. First create a user group:

   a. Click the 👥User groups tab.

   b. On the User Groups page, click New user group.

   c. On the User Groups pop-up, enter Security for the group name, and click Create User Group.

   Next, create a user to add to the Security group.

2. To create a user:

   a. Select the👤 Users tab.

   b. Select New user.

   c. In the Create user pop-up, enter a name for the user and an email address (that can be used to register the user below).

   d. Click Create user.

   Now, you will add the user to the Security group.

   e. Select the user.

   f. Click the Add groups drop-down, and select the Security group check box.

   g. Click Add to groups.

   Under User Groups, note the Security group drop-down indicating that the user is now part of the Security group.

Next you will create a security guard role.

3. To create a role:

   a. Click the Roles tab.

   b. Click New role.

   c. In the Role name box, enter Security Guard.

   Now, you will define the privileges of the security guard to allow them to control PTZ cameras for live images on external cameras.

   d. In the Devices column, select the Use PTZ controls check box and the Lock PTZ controls check box.

   By default, the View live images check box is selected.

   e. Click Create role.

   Next, you will create a policy that includes the security group, security role and sites and devices.

4. To create a policy:

   a. Click the Policies tab.

   b. Click New policy to display the Create policy pop-up.

   c. In the Policy name box, enter PTZ Camera Control for the name of the policy, and click Create policy.

   d. In the User groups column, select the Security user group check box.

   e. In the Role column, select the Security Guard role.

   f. In the Sites & devices column:

   i. Click + next to a site.

   ii. In the Site access panel on the right, click to view the cameras for the site, and clear the check boxes of any cameras that the security guard must not have the ability to access.

   iii. Click Add site to confirm access to the selected site and specified cameras.

   g. Select Save changes.

5. Log into Avigilon Unity Video Cloud to verify that the user (security guard) has access only to view live video with the ability to move and control PTZ cameras in the selected site and on select cameras.

Scenario – Investigator

This section walks through a simple scenario that grants an investigator the ability to export video for all external cameras across 2 sites.

1. First create a user group:

   a. Click the User groups tab.

   b. On the User Groups page, click New user group.

   c. On the Create a User Group pop-up, enter Investigator for the group name, and click Create User Group.

   Next, create a user to add to the Investigator group.

2. To create a user:

   a. Select the Users tab.

   b. Select New user.

   c. In the Create user pop-up, enter a name for the user and an email address (that can be used to register the user below).

d. Click Create user.

Now, you will add the user to the Investigator group.

e. Select the user.

f. Click the Add groups drop-down, and select the Investigator group check box.

g. Click Add to groups.

Under User Groups, note the Security group drop-down indicating that the user is now part of the Security group.

Next, you will create a role for investigators.

3. To create a role:

   a. Click the Roles tab.

   b. Click New role.

   c. In the Role name box, enter Investigator.

   Next, you will define the privileges of the Investigator.

   d. In the Devices column, select the Export images check box. By default, the View recorded images check box is selected.

   e. Click Create role.

4. To create a policy:

   a. Click the Policies tab.

   b. Click New policy to display the Create policy pop-up.

   c. In the Policy name box, enter Export Video for the name of the policy, and click Create policy.

   d. In the User Groups column, select the Investigator user group check box.

   e. In the Role column, select the Investigator role.

   f. In the Sites & devices column:

   i. Click + next to a site, and click Add site.

   ii. Click + next to a second site, and click Add site.

   g. Select Save changes.

5. Log into Avigilon Unity Video Cloud to verify that the user (investigator) has access only to recorded video with the ability to export video on cameras in the two selected sites.

Scenario – Organization Administrator

This section walks through a simple scenario of a primary administrator that grants another user membership of the Organization Administrators group. Users in the Organization Administrators group are granted the ability to manage user access across the organization.

1. Select the Users tab.
2. Select the user.
3. On the User details page, select the Add groups drop-down.
4. Select the check box of the Organization Administrators group, and then click Add to groups.

   Note the Organization Administrators drop-down above. If you click this drop-down, this group is part of the Organization Management Policy that gives administrators the ability to manage access across the sites.

5. Log into Avigilon Unity Video Cloud to verify that the user has the ability to manage user access.

More Information & Support

For additional product documentation and software and firmware upgrades, visit **support.avigilon.com**.

Technical Support

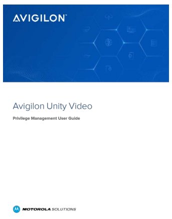
Contact Avigilon Technical Support at **support.avigilon.com/s/contactsupport**.

Third-Party Licenses

help.avigilon.com/avigilon-unity/video/attribution-report/VSA_FixedVideo.html
help.avigilon.com/avigilon-unity/video/attribution-report/VSA_Avigilon_ACC.html

MOTOROLA SOLUTIONS
More Information & Support

Documents / Resources

	**MOTOROLA SOLUTIONS Unity Video Privilege Management** [pdf] User Guide Unity Video Privilege Management, Unity, Video Privilege Management, Privilege Management, Management

References

- **End-to-End Security Solutions \| Avigilon (Openpath & Ava)**
- **help.avigilon.com/avigilon-unity/video/attribution-report/VSA_Avigilon_ACC.html**
- **Avigilon Support Community**
- **Avigilon Support Community**
- **help.avigilon.com/avigilon-unity/video/attribution-report/VSA_Avigilon_ACC.html**
- **Avigilon Support Community**
- **Avigilon Support Community**
- **Solving for Safer - Motorola Solutions**
- **User Manual**