Channel Partner User Groups Permissions

OpenEye Web Services (OWS) employs User Groups to make it easy to make changes, streamline setup and ensure that no one gets left out of updates or changes. Users in a User Group will have access to all permissions enabled in the User Group settings. User Groups created at a Channel Partner level will have permissions pertaining to the Customer Accounts controlled by the Channel Partner.

Channel Partner accounts have an Administrator User Group created by default. These default groups cannot be edited, and it will be necessary to create a new User Group to customize permissions.

To view and make changes to a User Group (other than a default one), click **Edit** next to the desired User Group under the **Management** tab: **Management > User Groups**.

This section will review the different menus and settings for the new or selected Channel Partner User Group.

Table of Contents

Channel Partner Users

Within this section, you can view Users in the User Group or add Users to the group by clicking **Add User** and checking the box next to each name to be included. Remove Users by clicking the **X** next to their names. Alternatively, check the box labeled **Automatically include all users in this User Group** to include everyone; adding Users to a group in this manner automatically includes future users.

Channel Partner Permissions

This section manages User Group permissions for Channel Partner users, and the features and functions they are allowed to see and/or modify. Check the permissions you want to assign to the User Group. Click **Save** to preserve any changes.

Channel Partner

Manage Accounts: Allows the ability to create, edit, and disable accounts. Also provides the ability to edit Global Default settings.

Manage Unassigned Recorders: Allows users to assign recorders from the Unassigned Recorders section to an End User Customer Accounts.

Manage Channel Partner Users and Groups: Allows adding, editing, and deleting Channel Partner users and groups.

System Design Tool: Allows users to access System Design Tool.

View All Designs: Allows access to view designs by all users.

Alerts

View Alerts: Allows users to view alerts that they have been previously added to. Users will only be able to see alerts on recorders/cameras from companies added to this user group.

Create/Edit Health Alert Rules: Provides the ability to create, edit, and delete health and storage retention alert rules. Permissions can also be enabled individually.

Create/Edit Non-Health Alert Rules: Provides the ability to create, edit, and delete non-health alert rules. Permissions can also be enabled individually.

Alert Administrator: Allows users to create any alert rule type. Users will be able to see all alert rules, even if they are not a member.

Allow Third-Party Integration Access: Allows users to configure Alert Rules to send to third party integrations. This option also provides access to the alerts generated by the alert rule using the Web Services SDK.

Reports

View Reports: Allows users to view reports that they have been previously added to. Users will only be able to see reports from companies added to this user group.

Create/Edit Reports: Allows users to create and edit reports. Users can only edit reports they have been previously added to.

Report Administrator: Users will be able to see all Reports, even if they are not added to the Reports as a user. Users will be able to create, edit, and delete reports, including Shared Reports.

Operations

Order & Shipping Report: Allows users to view a report that contains details on orders placed with OpenEye.

Channel Partner 2-Step Verification

Enable 2-Step Verification

Using 2-step verification will help prevent unauthorized users from accessing an account with just a stolen password. When users sign in using a new device, 2-step verification will require them to enter both their password and a unique code that they receive on their phones. 2-step verification is highly recommended.

Check the box to Enable 2-Step Verification.

Once enabled, the User will be prompted to enter a phone number the next time they log in. This phone number will be used to send verification codes whenever the user logs in on a new device.

Force Disable 2-Step Verification Requirement

In some cases, there may be users who are unable to use 2-Step Verification (users who do not have access to a phone, etc.). When this happens, they may need to be exempted from 2-Step Verification.

To exempt users from 2-step verification, follow these steps:

1. Create a new user group (optionally called '2-Step opt out') and add the users who should be exempted.
2. Enable the 'Disable 2-Step Verification Requirement' option on this page.

It is not necessary to add additional permissions to this group if the Users exist in other groups with these permissions already configured.

Customer Account Access

Use this section to add or remove Customer Accounts to the User Group. All members of this User Group will have the ability to view and access all Customer Accounts added to this list. Customer Accounts not on this list will be invisible to members of this User Group.

1. Click **Add Account**.
2. Check the boxes next to each account to be included in the **User Group**. To include all existing and future accounts in the User Group, check the box **Include all accounts in this User Group**.

3. Click **Add** when finished.

Web Services Permissions

Use the Web Services Permissions section to enable or disable User Group permissions pertaining to managing Web Services settings on the recorder, managing other Users and User Group permissions, and management of video clips, alerts and reports. Check the permissions you want to assign to the User Group. Click **Save** after checking permissions.

Administration

Administrative Access: Allows full administrative control of Customer Accounts specified in Account Access section.

User Management

Enable **Manage User and User Groups** to give Users management permissions over Users and User Groups.

Manage Built-in User Groups: Allows Users to view, add, and remove other users from the Built-In User Groups.

Edit Auto Include: Allows enabling and disabling auto include devices and cameras in User Groups.

Manage Access by External IP Address: Allows Users to edit the External IP Address settings under the Remote Client Permissions page.

Recorders

Allows Users to connect to recorders and add, edit or delete recorders and recorder groups.

Recorder Access: Allows connecting to recorders that are specified in the Recorders section with the permissions defined in the Recorder Permissions section.

Manage Recorders and Recorder Groups: Allows Users to add, edit and delete recorders and recorder groups that are specified in the Recorder Management section.

Video Clip Management

Allows access to view and manage video clips uploaded by other Users, as well as Edit, Delete, Share or View Video Clips.

Access Other Users' Video Clips: Allows access to view and manage video clips uploaded by other users based on the Video Clip Permissions enabled.

Video Clip Permissions: Allows access to all Video Clip Permissions. Permissions can also be enabled individually: Edit, Delete, Share, View.

Reports

Allows users to view, create or edit reports, along with assigning Report Administrator access to view, edit and delete any report, even those to which they're not added.

View Reports: Allows Users to view reports that they have been previously added to. Users will only be able to see reports from companies added to this User Group.

Create/Edit Reports: Allows Users to create and edit reports. Users can only edit reports they have been previously added to.

Report Administrator: Users will be able to see all Reports, even if they are not added to the Reports as a user. Users will be able to create, edit, and delete reports, including Shared Reports.

Alerts

Customize Alerts Permissions to allow users to view, create, edit, assign Alert Administrator access, and allow third-party integration access.

View Alerts: Allows Users to view alerts that they have been previously added to. Users will only be able to see alerts on recorders/cameras from companies added to this User Group.

Create/Edit Health Alert Rules: Provides the ability to create, edit, and delete health and storage retention alert rules. Permissions can also be enabled individually.

Create/Edit Non-Health Alert Rules: Provides the ability to create, edit, and delete non-health alert rules. Permissions can also be enabled individually.

Alert Administrator: Allows Users to create any alert rule type. Users will be able to see all alert rules, even if they are not a member.

Allow Third-Party Integration Access: This option allows users to configure Alert Rules to send to third party integrations. This option also provides access to the alerts generated by the alert rule using the Web Services SDK.

Remote Client Permissions

These permissions allow administrators to limit the clients a user in a User Group can access. User access to remote clients should be restricted by need and location. Access to clients is managed in User Groups and can be restricted both by client type and by IP range. This gives Administrators the flexibility to enforce policies such as preventing Users from accessing video using the mobile app or accessing clients when not on the corporate network.

Command Station

Allows users to access recorders using the Command Station Desktop Client application.

View Shared Layouts: Allows viewing of shared camera and map layouts.

Manage Shared Layouts: Allows editing of shared camera and map layouts.

Edit Linked Cameras: Allows users to modify cameras in the Linked Cameras feature.

Push to Client: Allows alerts to be sent to users logged into Command Station. The 'Push to Client' option must be enabled for each user in the alert rule in order to receive alerts.

Force Alerts to be Acknowledged: This option forces the alert pane to remain open until all alerts are closed.

Web Browser

Allows users to connect to Web Services and recorders using a web browser.

Local Console

Allows users to connect to the recorder when using a monitor and keyboard / mouse attached to it.

Mobile Applications

Allows users to connect to recorders using iOS devices (iPhone, iPad, etc) and Android devices (phones, tablets, etc).

Restricting Access by External IP Address

External IP Administrators can also restrict access to an External IP Address range. This prevents users from accessing OWS when they are outside of their corporate network. When enabled, the range of external IP addresses entered into the fields will have permission to access OWS. All other external addresses will be restricted.

1. Enable restriction.
2. Enter a range of external IP Addresses that OWS can be accessed from.
3. Select to add additional ranges if necessary.

NOTE: Remote Client permissions are dependent on your OWS license. View the complete list of features by license type for more information.

Recorder Permissions

This section allows you to enable or disable User Group permissions pertaining to Recorders on Customer Accounts

specified in Account Access.

Video

Allows access to all video operations (each permission can also be enabled individually).

View Live Video: Allows viewing of live video.

View Recorded Video: Allows viewing of recorded video.

Export Video Locally: Allows exporting of recorded video to a local storage location.

Export Video to Web Services: Allows exporting of recorded video to Web Services.

Control PTZ: Allows pan, tilt and zoom control.

Set PTZ Presets: Allows setting PTZ presets.

Auto Focus: Allows users to activate the auto focus option on supported cameras.

Audio

Allows access to audio options (each permission can also be enabled individually).

Listen To Audio: Allows listening to live and recorded audio.

2 Way Audio: Allows ability to push audio to an audio device.

Web Services

Allows management of all Web Services settings (each permission can also be enabled individually).

Manage Web Services Registration: Allows adding or removing recorders.

Manage Web Services Uploads: Allows managing video clip uploads to Web Services.

System User Management

Allows management of all local System User Management tasks (each permission can also be enabled individually).

Manage Roles: Allows adding, editing, and deleting of user roles on the local recorder.

Manage System Users: Allows adding, editing, and deleting of system users on the local recorder.

NOTE: OpenEye recommends that any system connected to OpenEye Web Services (OWS) perform all user management through OWS. As such, the System User Management permissions should be rarely used.

Setup

Allows management of all system setup settings (each permission can also be enabled individually).

Access Power Off / Restart Options: Allows access to recorder power options.

Access Support Tools: Allows access to recorder support tools.

Manage Cameras: Allows adding, editing, and deleting of cameras.

Manage Holidays: Allows adding, editing, and deleting holidays.

Manage Intrusion Devices: Allows users to manage Intrusion devices.

Manage Licensing: Allows management of recorder licenses.

Manage Local Data Collection Devices: Allows user to manage local data collection devices such as Point of Sale terminals.

Manage Macros: Allows adding, editing, and deleting system macros.

Manage Network Configuration: Allows management of network settings.

Manage Schedules: Allows adding, editing, and deleting schedules.

Manage Sensor/Relay Settings: Allows management of sensor/relay settings.

General Information

Use this section to edit the Name or Descriptions of the User Group, or to delete the group entirely. Deleting a group cannot be undone and will remove all users from the group.