Technical Notes for Ocularis 5.7

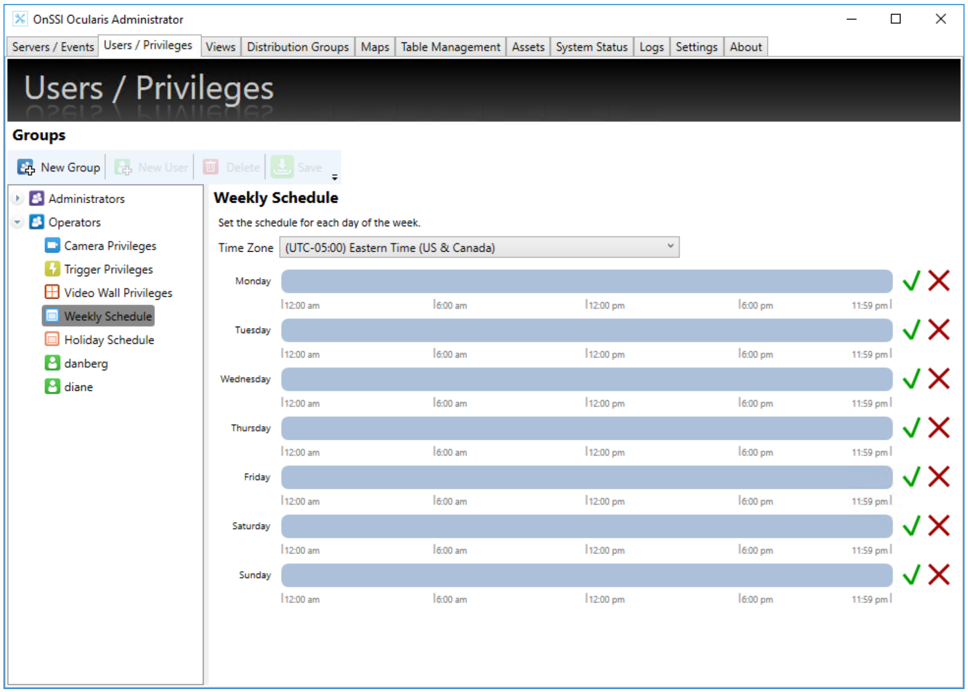
The purpose of this document is to provide technical details for various new features in the Ocularis 5.7 release.

Topics in this Document

Login Restrictions Based on a Schedule

The system administrator can now implement added security and control when an Ocularis user can log in to Ocularis using Ocularis Client, Ocularis Web or Ocularis Mobile. Using Ocularis Administrator, Weekly Schedules can be configured on a user group basis. By default, all users have 24 / 7 / 365 access but administrators can reduce this time period to only when the operator's shift takes place. There is also a Holiday calendar to further define acceptable login times for each user group.

This is configured in the **Weekly Schedule** module of the *Users / Privileges* tab within *Ocularis Administrator*.



Set the schedule for each day of the week.

Time Zone (UTC-05:00) Eastern Time (US & Canada)

Figure 1 Weekly Schedule

By default, a user group's access is all the time (24 x 7 x 365). Administrators can establish approved login hours for each group based on their work schedule. Then, if a user attempts to log in with Ocularis Client, Ocularis Web, Ocularis Mobile or the Ocularis SDK, the system will deny access. Also, for Group Administrators, the schedule also controls their access to Ocularis Administrator.

> ***Note**: If a user is logged in past their configured end time, the system will not log the user out.*

To Modify the Login Schedule for a User Group

Use these steps to restrict the acceptable login times for a user group. Members of the 'Administrators' user group may modify schedules for any group and Group Administrators may modify the schedules for their own user group.

1. In the **Users / Privileges** Tab of *Ocularis Administrator*, select the group whose schedule you wish to configure.
2. Select the **Weekly Schedule** node.

3. Each day of the week is shown. Blue indicates approved access time.

> **Tip**: *If you position the mouse over the timescale, a balloon appears displaying the Start and End time on the timescale.*

4. At the top of the schedule, a time zone drop-down is available. Select the time zone applicable to the users of the selected group. This restricts the access time based on the local time of the selected time zone.

   For example:

   The time zone selected is Paris time (UTC +01:00) and the schedule for Mondays is 9:00 a.m. to 4:00 p.m.

   A user from this group travels to the NYC office which is in Eastern Time (UTC -05:00). This user will only have access on Mondays from 3:00 a.m. to 10:00 a.m. local NY time.

> **Note**: *The time zone set for the group's Weekly Schedule is shared with the time zone for its Holiday Schedule.*

5. For each day of the week:
   - Click the 'X' to remove all privileges for that day. ✗
   - Click the checkmark to apply privileges for the entire day. ✓
   - To limit the time period, clear the daily schedule with the 'X' icon and then drag and release the mouse across the time period.

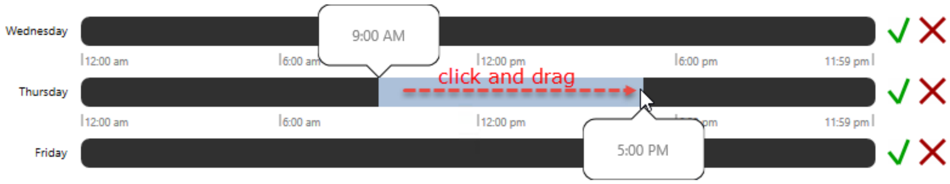
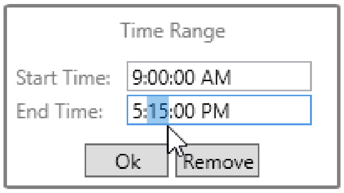


Figure 2 Click and Drag from left to right

6. When you release the mouse, the Time Range pop-up appears.



Time Range

Start Time: 9:00:00 AM

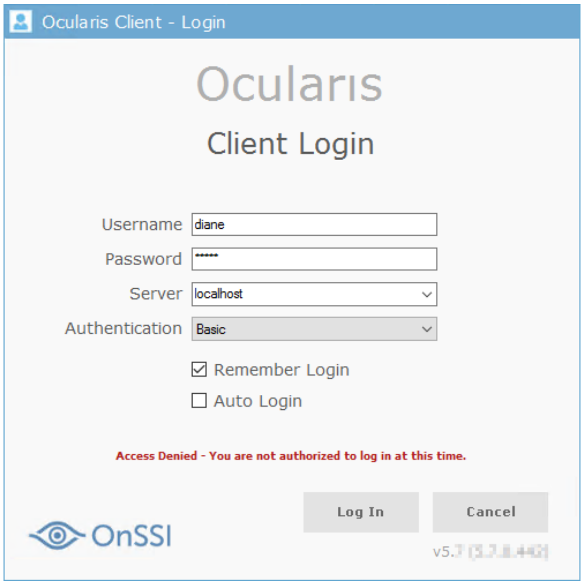
End Time: 5:15:00 PM

Figure 3 Time Range Pop-Up

   You can manually fine tune the time period. Click **Ok** to save the settings.

7. Repeat for each day of the week.

If a user attempts to login to Ocularis Client during their off hours, this message will appear:



Username diane

Password *****

Server localhost

Authentication Basic

☑ Remember Login

☐ Auto Login

Access Denied - You are not authorized to log in at this time.

Figure 4 Access Denied

A similar message is displayed in Ocularis Administrator for Group Administrator logins.

More Information on Schedules

- Schedules apply to the entire user group. If a user requires a different schedule, he or she must be placed in a different user group.
- There may be more than one valid, non-contiguous access time periods set with the same day.
- All login attempts, valid or after hours, are registered in the audit log.
- Access restrictions apply to Ocularis Client, Ocularis Web, Ocularis Mobile, Ocularis Administrator and any 3rd party application using the Ocularis SDK
- The 'Administrators' user group has no time or date restrictions.
- Use a Holiday Schedule to further refine access times for each user group (see below).

Holiday Schedule

In conjunction with the Weekly Schedule, administrators can also configure a holiday schedule for the calendar year. This is done on a per group basis.

To Modify the Holiday Schedule for a User Group

Use these steps restrict the acceptable login times for a user group during company holidays.

1. In the **Users / Privileges** Tab, select the group whose schedule you wish to configure.
2. Select the **Holiday Schedule** node. The time zone will be the same as the one set for weekly schedules. If you change the time zone here, it will be changed in the **Weekly Schedules** node.

3. You may select the calendar year from the drop-down on the right.

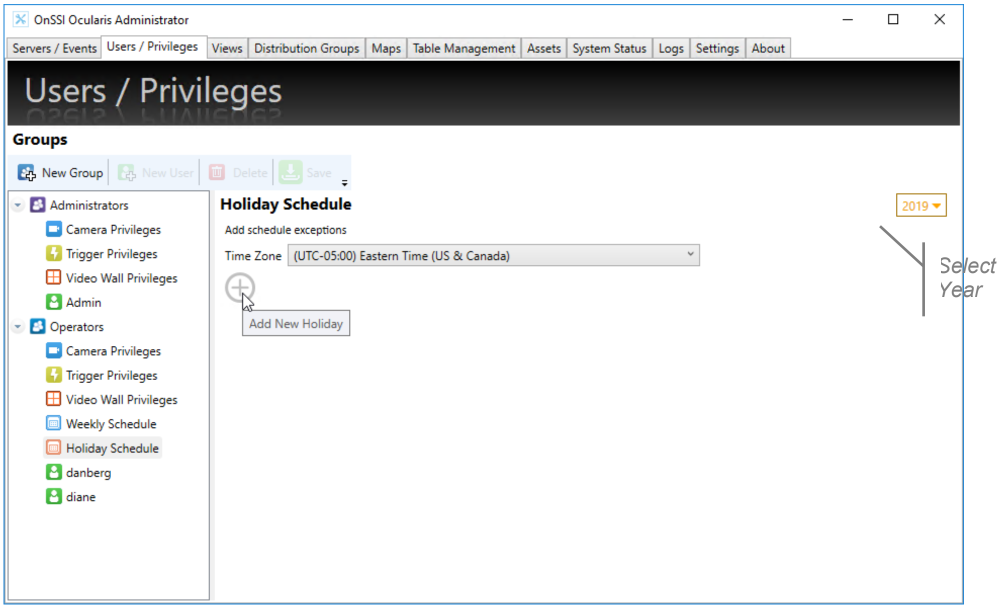


Figure 5 Holiday Schedule

4. Click the ⊕ to add a new holiday. A month calendar appears.

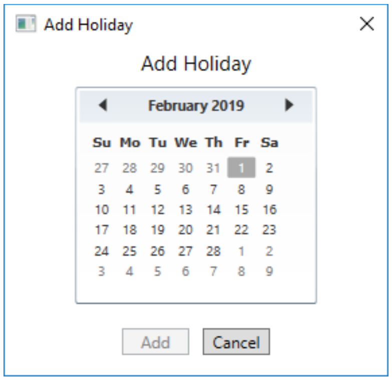


Figure 6 Select Date

5. Navigate to the month for the holiday and select the date. Click **Add**. A day time bar appears with no time selected. This means the group will have no access to the system for the entire day.

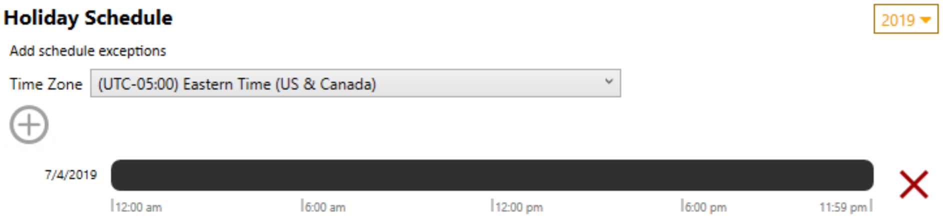
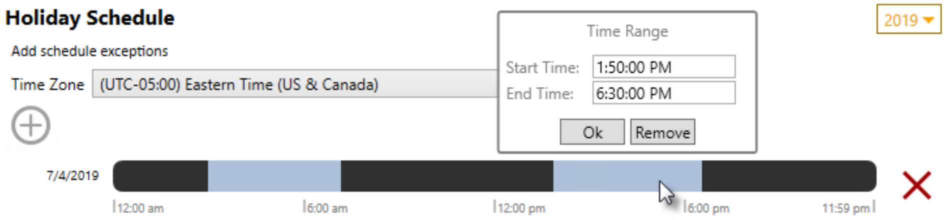


Figure 7 Add a Holiday

6. If you want to grant this user group access for a portion of the day, simply drag and release the mouse on the timeline to identify the time period as you would with the weekly schedule. Fine tune with the Time Range pop-up.



Holiday Schedule

Add schedule exceptions

Time Zone (UTC-05:00) Eastern Time (US & Canada)

Time Range

Start Time: 1:50:00 PM

End Time: 6:30:00 PM

Figure 8 Adjust Access Hours on a Holiday

7. Repeat this process for each holiday, for each user group.

> **Note**: *The Holiday Schedule can grant greater access than the Weekly Schedule. For instance: if a user group has no login access on Mondays and a Holiday that falls on a Monday has a valid login period from 9:00 a.m. to 5:00 p.m., the user group members will be allowed to login even though this is not allowed in their Weekly Schedule.*

Export Alarm Recordings Only

Export Alarm Recording Only

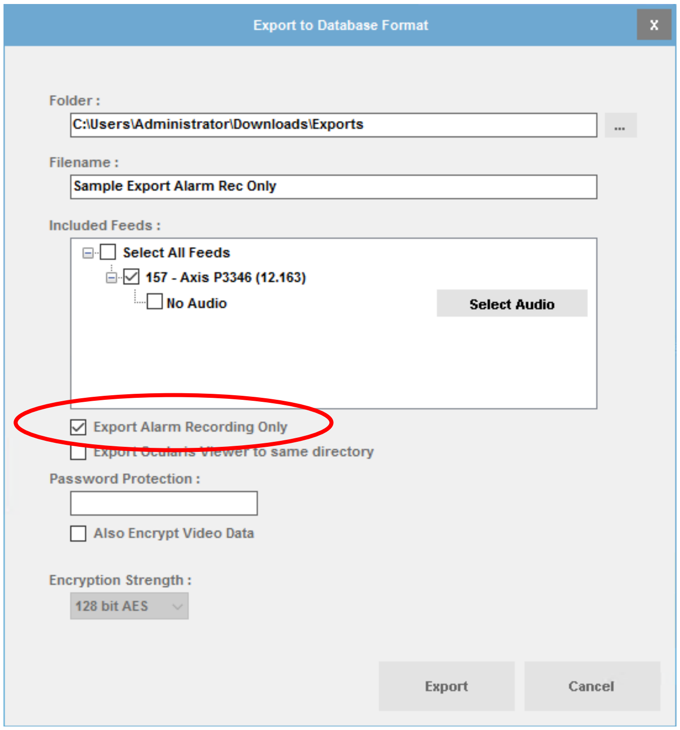
Ocularis supports two types of recordings: Standard and Alarm. Standard recording, also known as continuous recording, is video that is recorded regardless of whether there is motion or another event associated with that video. Standard recording is represented in the color green on the Kinetic Timeline. Alarm recording is video that is recorded due to a configured event, such as motion detection. Alarm recording is represented in the color red on the Kinetic Timeline. If a camera has both Standard and Alarm recording configured, you can export (in Database Format) only the Alarm Recording portion in order to eliminate the Standard Recordings. This saves on export space and time.

To Export Only Alarm Recordings

1. With the desired camera displayed, enter *Browse* mode.
2. Select the start and end of the video clip.
3. From the menu bar, select ‘Export’.
4. From the **Export Options** screen, select ‘Database Format’.
5. Enter the Folder and Filename for the exported clip.
6. Select the camera feed.

> **Note**: *If audio exists and the Audio box is checked, the audio will still be exported when executing an Alarm Recording Only export. During playback, audio will play during periods where no video is displayed.*

7. Check the box 'Export Alarm Recording Only'.



Export to Database Format

Folder : C:\Users\Administrator\Downloads\Exports

Filename : Sample Export Alarm Rec Only

Included Feeds :

- □ Select All Feeds
  - ☑ 157 - Axis P3346 (12.163)
    - □ No Audio

☑ Export Alarm Recording Only

□ Export Ocularis Viewer to same directory

Password Protection :

□ Also Encrypt Video Data

Encryption Strength : 128 bit AES

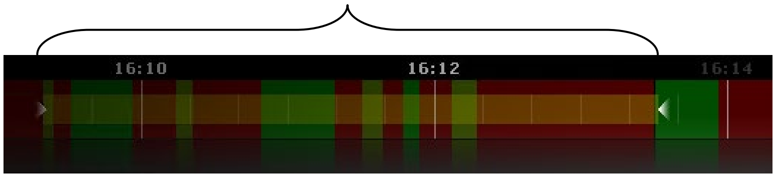
Export Alarm Recording Only

8. Include anything else from the dialog that you want. (e.g. Ocularis Viewer, password, encryption, etc.)

9. Click **Export**.

The exported clip will only contain alarm-based video (i.e. colored in red).

For example, when this camera's video clip is selected, only the video in red (Alarm Recording) will be exported, rather than everything selected.



Export Only Alarm Video

> **Note**: *If audio exists and the Audio box is checked, the audio will still be exported when executing an Alarm Recording Only export. During playback, audio will play during periods where no video is displayed.*

TLS 1.2 Upgrade Information

This release supports TLS 1.2 encryption for stronger security and protection against cyber-attacks. It can be used to secure all logins including Ocularis Administrator, Ocularis Client and Ocularis Media Server. For certain upgrade environments, additional steps may be required.

If you would like to ensure that only TLS 1.2 is used for secure network communication in Ocularis, follow the steps below:

1. If you are using SQL Server Express 2008 as the Ocularis Base database, SQL must be upgraded manually to a version that supports TLS 1.2. SQL Server Express 2008 was included with Ocularis version 5.1 and prior but may also be present if you have upgraded to version v5.2-5.6 from an older Ocularis version. If you are unsure of your version of SQL Server, check with your IT department or contact support@onssi.com.
2. In Windows, disable all security protocols older than TLS 1.2 on all systems that use Ocularis.
3. Install Ocularis 5.7. If Ocularis Base was upgraded to v5.7 prior to disabling the older security protocols (step 2), simply re-run the Base installer (do not uninstall) to enable TLS 1.2 functionality in Ocularis

WebRTC Certificates

WebRTC (Web Real-Time Communication) provides web browsers with real-time communication and improved security via a simple application programming interface. It also provides faster video load times and more responsive PTZ camera control. WebRTC replaces Adobe Flash in Ocularis Web v5.7.

In order to take advantage of this technology, a certificate must be imported into the browser used to view Ocularis Web video. This process need only be done once.

Keep in mind that with WebRTC, TCP Port 8420 must be open as it is now used for live video. Port 1935 is still used when sending M2O video from the Ocularis Mobile App to Ocularis Media Server.

***Note**:* *The Microsoft Internet Explorer browser is no longer supported.*

Refer to the document *Ocularis Web – WebRTC Configuration* for full details on how to import a certificate for each supported browser.

0000002192019-03-1526-5.7.0.455