

Ocularis OpenSight™ enables disparate Ocularis systems to be monitored within a single interface.

## **Who Should Read This Document**

Ocularis OpenSight works between two parties: a host and a viewer (remote monitor). Both parties require a minor amount of configuration in order to implement Ocularis OpenSight. Both the host and remote monitor entities should read this document.

## **What is Ocularis OpenSight?**

Ocularis OpenSight is designed to let users consolidate and share information from video surveillance and other security systems that are not within a single entity. For example, a school may wish to allow the local police department to monitor selected cameras of the school's security system. With OpenSight, the police can now view the school's designated cameras within the police department's own Ocularis map without the need for a separate login into the school's system. What's more, many other schools can be added to the same view at the police department.

When implementing OpenSight in this example, the school, or host, would grant the police department the user privileges and access rights the school feels is necessary for proper monitoring by the police. These rights and privileges can be different from the school's own internal personal use. If this school has multiple locations (such as a university) it may wish to share information between each in one integrated map.

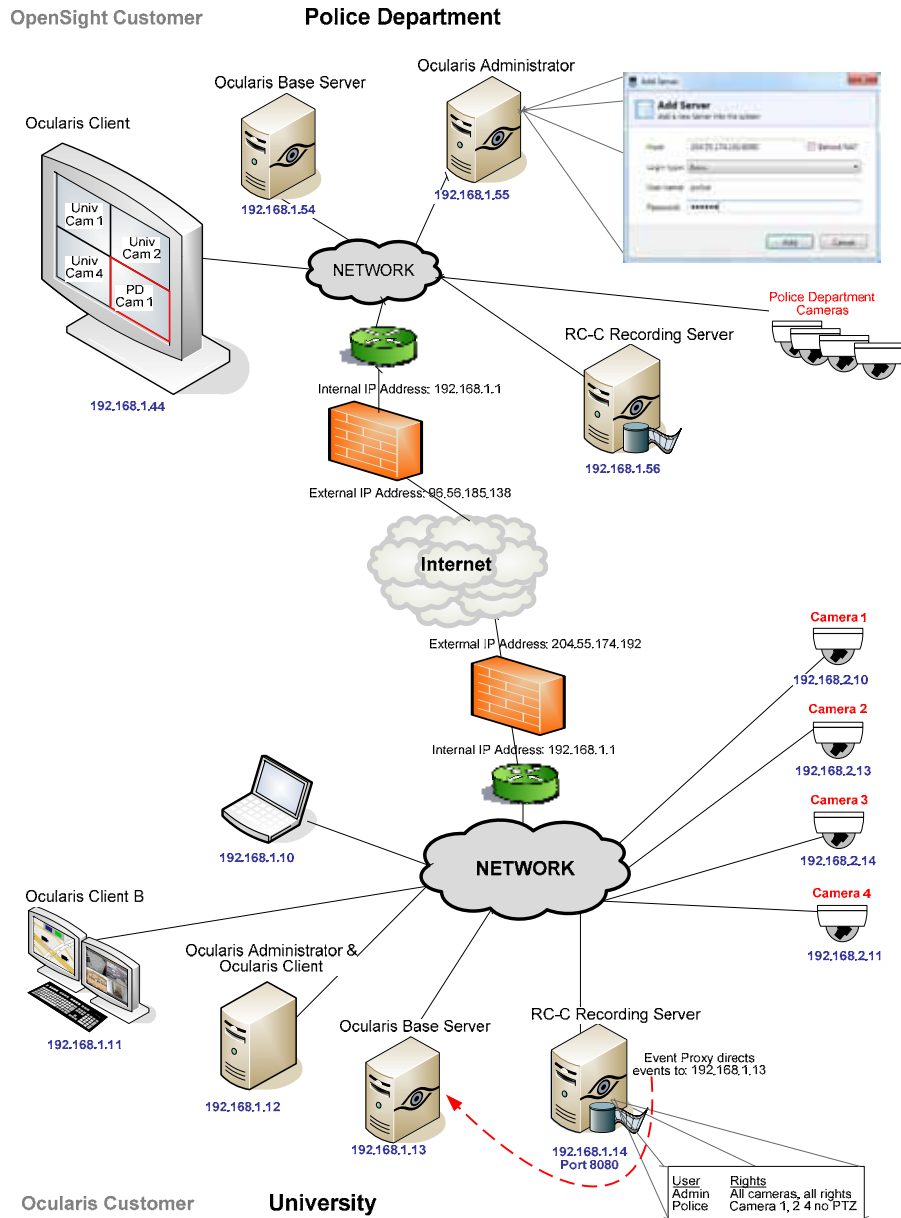


Figure 1 OpenSight Layout (Sample)

## OpenSight Entities

As depicted in Figure 1 above, there are typically two parties or entities involved when using OpenSight. These are: the *Host* and the *Remote Monitor*.

### Host

The *Host* entity in an OpenSight environment, is the party who wishes to share their cameras with someone else. Cameras may be shared across the same organization or with different companies. To use OpenSight, the Host must possess either Ocularis ES or Ocularis CS using recorders such as RC-C or RC-E. In the earlier example, the host is the University.

See [Host Configuration](#) below for further instructions.

**REMOTE MONITOR**

The *Remote Monitor* entity in an OpenSight environment, is the party who wishes to view the cameras of someone else. It can be across the same organization or with different companies. To use OpenSight, the Remote Monitor must possess a valid installation of Ocularis Base with corresponding OpenSight licenses. In the earlier example, the Remote Monitor is the Police Department.

See [Remote Monitor Configuration](#) below for further instructions.

**Configuring OpenSight**

This section reviews the steps necessary for OpenSight configuration.

- Host Configuration
- Remote Monitor Configuration

**HOST CONFIGURATION**

The following steps should be performed by the Host when preparing their system for OpenSight use.

1. Determine which cameras you wish to be monitored by the Remote Monitor organization.
2. Create a user account on the NVR with the privileges you wish to provide to the Remote entity.
3. Provide the Remote Monitoring entity with the user account ID, password, public IP address and port number for the NVR.

Proceed with the following instructions based on the NVR used:

- For NetDVMS 6.5x Recorders see page 4.
- For RC-C 7.0x Recorders see page 5.
- For NetEVS 3.1x and RC-E 4.0x Recorders see page 6.

**FOR NETDVMS 6.5X RECORDERS**

1. On the NVR responsible for those cameras you wish to share, create a new basic user account in the *NetDVMS Image Server Administrator* to be used by the Remote Monitoring entity. If the cameras are located on more than one NVR, this process must be repeated for each NVR. In the case of a master-slave, create the user account on the master NVR.

**How To....**

- a. In the User Administration section of the *NetDVMS Image Server Administrator*, click the **User Setup** button.
  - b. Click the **Add a Basic User** button.
  - c. Enter a **Username** to be given to the Remote Monitoring entity.
  - d. Enter a **Password** for this account.
  - e. Click **OK** and then click **Close**.
2. Restrict the access for this new user account for only those cameras you wish to be monitored.

**How To....**

- a. In the User Administration section of the Image Server Administrator, select the **Restrict user access** radio button.
  - b. Click the **User Access** button.
  - c. Select the new user account from the User drop-down list.
  - d. Select the Global User Rights you wish to provide to the Remote Entity.
  - e. Select the cameras you wish to enable for the Remote Entity.
  - f. Select or remove additional privileges for the cameras (Browse rights, Export, etc.)  
Restrict the account privileges to only those which you want the Remote Monitoring entity to have. You may be as broad or as granular as you like. Consider, however, that you may not want to provide privileges to a feature that may interfere with your own operators (such as controlling PTZ).
  - g. When finished, click **Close**.
3. If it is not already configured, outside access must be enabled in order to allow the Remote Monitoring entity to gain access to the NVR video.

**How To....**

- a. In the Server Configuration section of the Image Server Administrator, check the **Enable Outside Access** checkbox.
- b. In the **Outside Address** field, enter the public IP address assigned to your firewall.
- c. In the **Outside Port** field, enter the port used by the public IP address to gain access via the firewall.
- d. Click the **Local IP Ranges** button to identify local address ranges used internally. This will enable the Image server to recognize login requests originating from these IP addresses as coming from a local network and provide access locally.

**Note:** when using outside access, the router or firewall used must be configured so that requests sent to the outside (public) IP address and port are forwarded to the inside (local) IP address and port of the server running the Image Server service.

- e. When done adding local IP ranges, click **Close**.
- f. Click **OK** to save settings and close the NetDVMS Image Server Administrator.

**FOR RC-C 7.0x RECORDERS**

1. On the NVR responsible for those cameras you wish to share, create a new basic user account in the *RC-C Management Application* to be used by the Remote Monitoring entity. If the cameras are located on more than one NVR, this process must be repeated for each NVR. In the case of a master-slave, create the user account on the master NVR.

*How To....*

- a. In the *RC-C Management Application*, expand the *Advanced Configuration* node of the Navigation Pane.
  - b. Right-click the **Users** node.
  - c. Select **Add New Basic User**.
  - d. Enter a **Username** to be given to the Remote Monitoring entity.
  - e. Enter a **Password** for this account.
  - f. Click **OK**.
2. Restrict the access for this new user account for only those cameras you wish to be monitored.

*How To....*

- a. In the *User Properties* screen, accessed by double-clicking the username if not already open.
  - b. Click the **General Access Properties** tab.
  - c. Select which general settings you would like to grant to this user account.
  - d. Select the **Camera Access** tab
  - e. Select the cameras you wish to enable for the Remote Entity.
  - f. Select or remove additional privileges for the cameras (Browse rights, Export, etc.)  
Restrict the account privileges to only those which you want the Remote Monitoring entity to have. You may be as broad or as granular as you like. Consider, however, that you may not want to provide privileges to a feature that may interfere with your own operators (such as controlling PTZ).
  - g. When finished, click **OK**.
3. If it is not already configured, outside access must be enabled in order to allow the Remote Monitoring entity to gain access to the NVR video.

*How To....*

- a. In the Navigation Pane, right-click the *Server Access* node.
- b. Select **Properties**.
- c. In the Server Access tab, check the **Enable Internet Access** checkbox.
- d. In the **Internet Address** field, enter the public IP address assigned to your firewall.
- e. In the **Internet Port** field, enter the port used by the public IP address to gain access via the firewall.

- f. Click the **Local IP Ranges** tab to identify local address ranges used internally. This will enable the Image server to recognize login requests originating from these IP addresses as coming from a local network and provide access locally.

**Note:** when using outside access, the router or firewall used must be configured so that requests sent to the outside (public) IP address and port are forwarded to the inside (local) IP address and port of the server running the Image Server service.

- g. Click **Add** to enter the *Start* and *End* Address for the Local IP Range
- h. When done adding local IP ranges, click **OK**.
- i. Click **Apply** to save settings.

#### FOR NETEVS 3.1X AND RC-E 4.0X RECORDERS

1. On the NetEVS Management Server machine, create a new Windows account to be used by the Remote Monitoring entity. This account is created through the operating system user account utility. Be sure to create a password for this user account.

2. Within NetEVS, create a Role specifically for use by the Remote Monitor.

##### *How To...*

- a. In the NetEVS or RC-E Manager, right-click on *Security > Roles* in the navigation tree.
- b. Select **Add New Role...**
- c. Enter a name to assign to remote monitoring users.
- d. Enter an optional description for this role.
- e. Click **OK**.

3. Add the Windows account created in step 1 to this new role.

##### *How To...*

- a. Select the Role created in step 2 above.
- b. In the **Users & Groups** tab, click the **Add** button.
- c. Verify that the required domain is specified in the *From this location* field. If not, click the **Locations** button to browse for the required domain.
- d. In the *Enter the object names to select* text box, type the user name created in step 1.
- e. Click the **Check Names** button to verify the entry.
- f. If you are prompted for the username and password, enter it and click **OK**. The name should be listed in the *Enter the object names to select* text box.
- g. Click **OK**. The account should be added as a member of this Role.

4. Configure the rights for this Role. Restrict or grant access to devices and functions as needed.

##### *How To...*

- a. Select the Role created in step 2 above.
- b. For each tab, (Device, PTZ, Speech, Application, etc.) grant or restrict access to cameras and privileges for the remote monitor.

5. Save changes.

**REMOTE MONITOR CONFIGURATION**

The following steps should be performed by the Remote Monitor entity when preparing their system for OpenSight use.

**Note:** OpenSight is supported with Ocularis version 1.1 or Ocularis 2.0. If you have an earlier version of Ocularis, we recommend upgrading to version 2.0 prior to completing the configuration steps below.

1. Purchase OpenSight licenses from your OnSSI certified dealer. If necessary, upgrade to Ocularis version 2.0.
2. When you upgrade to Ocularis 2.0 or if you have Ocularis 2.0 and you purchased OpenSight licenses, you will be provided with a new Ocularis SLC and a new .v2c file.
3. Open the *Ocularis License Activation* application located on the Ocularis Base Server.
4. Enter the new/updated SLC and click the **Verify SLC** button.
5. Click the **Update Base License** button, browse to and select the new .v2c file provided to you.
6. When the .v2c import is complete, close the *Ocularis License Activation* application.
7. Obtain the access credentials from the Host.

**You will need:**

- a. The public IP address of their NVR.
    - i. For NetDVMS and RC-C: You need the IP address of the Recording Server machine(s).
    - ii. For NetEVS and RC-E: You need the IP address of the Management Server machine.
  - b. The port number for the corresponding NVR Server(s).
  - c. The user account created for you by the Host.
  - d. The password for this account.
8. In Ocularis, add the Host's NVR(s) using the credentials provided.

**How To....**

- a. Open the *Ocularis Administrator* application.
- b. In the **Servers/Events** tab, click the **Add** button in the Servers pane.
- c. Type in the IP address of the Host's NVR followed by a ":" and the port number.

*For example:*

204.55.174.192:8080

- d. Select **Basic** or **Windows** as the login type as instructed by the Host.
- e. Enter the **User name** provided to you by the Host.
- f. Enter the **Password** provided to you by the Host.
- g. Click the **Add** button.

The NVR should appear in the Servers pane and the authorized cameras are displayed when the NVR is expanded.

Repeat Steps 8 a through g for each NVR to be used with OpenSight licenses.

9. Provide access to the new cameras to those Ocularis users as needed.

*How To...*

- a. In the **Users/Privileges** tab, select the group for which you would like to provide access to the new cameras.
  - b. Drag and drop the camera from the **Devices** list to the **Privileges** pane.
10. Restrict further privileges if necessary.

*How To...*

- a. In the **Users/Privileges** tab, uncheck privileges to the newly acquired cameras (PTZ, Presets, etc.)

**Note:** Despite appearances, you may have fewer privileges than displayed on the Users/Privileges pane. You may further restrict privileges but you may not grant additional privileges to OpenSight licensed cameras.

11. Assign the newly acquired cameras to new or existing views in the **Views** tab.
12. Save your changes.

When viewed in the Ocularis Client, these cameras will appear as any other cameras and the fact that they may belong to another organization is entirely transparent to the operator.