ConferenceManager

HD Video Deployment Guide

Software Version 12.0

sonexis™

Trademarks

Disclaimer: This Operator's Guide is meant as a general guide to configuring and administering the conferencing system. Not every configuration or problem can be anticipated given the variations in all hardware and software products. Compunetix, Inc. accepts no responsibility for errors or omissions contained in this Guide.

Compunetix, Inc.
978-640-2000
www.sonexis.com
CustomerCare@sonexis.com

Headquarters:

2420 Mosside Boulevard
Pittsburgh, PA 15146

Technology Center:

50 High Street, Suite 27
North Andover, MA 01845

Contents

Deploying Webcam Support

ConferenceManager provides webcam (HD Video) services via a customized Red5 server and video application. Webcam services can be installed on the ConferenceManager server itself, or on a remote server that may or not be providing conferencing services. Webcam services may also be supported by multiple servers, which are automatically load-balanced. Please contact Sonexis Customer Care to discuss best practices for your specific environment.

Webcam services can use one or both Real Time Messaging Protocol (RTMP) flavors:

- RTMP over port 1935 provides the best performance; note that many firewalls block incoming WAN traffic on port 1935 by default.
- RTMPS over port 443 supports secure client connections, but requires that the webcam server is configured with an SSL certificate [that is trusted by the client].

If both RTMP and RTMPS are enabled, clients will first attempt to connect via RTMP, and then RTMPS.

To configure ConferenceManager for webcam support:

Step 1. Install the Java Runtime Environment on each server that will provide webcam services (version 7u67 or higher; see www.java.com).

Step 2. Contact Sonexis Customer Care for the webcam installer package.

Step 3. Run the webcam installer.

Note that the following Windows firewall rules are created automatically upon install:

- **Webcam Admin 5080:** Allows Administration of the server. Access is limited to the local subnet by default; if the webcam software is installed on a ConferenceManager server itself then this rule can be disabled.
- **Webcam User 1935:** Allows unsecure webcam client access via RTMP on port 1935.
- **Webcam User 443:** Allows secure webcam client access via RTMPS on port 443.

Step 4. If you plan to use offer secure access via RTMPS, you must install a client-trusted SSL certificate on each webcam server:

- If you have an existing wildcard SSL certificate, see "Configuring SSL for RTMPS (Existing Certificate)" on page 5
- If you do not have an SSL certificate, see "Configuring SSL for RTMPS (New Certificate)" on page 3

Step 5. Add and Configure each server from ConferenceManager's **Webcam** tab.

If the ConferenceManager server itself is providing webcam services, it must also be added.

Step 6. Enable webcam for one or more Classes of Service:

a. From the Class of Service page, click the **Edit** link for the Class of Service you wish to modify.

b. Set **Allow Web** > **Allow Webcam** to **Yes**.

c. Click **Save**.

Configuring SSL for RTMPS

Configuring SSL for RTMPS (New Certificate)

This section describes how to configure SSL on a webcam server if you do not currently have a valid SSL certificate.

1. CREATING A KEYSTORE

Step 1. Open a CMD window as Administrator on the Web Server and go to the Java \bin directory:

```
cd C:\Program Files\Java\jre7\bin
```

Step 2. Run the following key generation command:

```
keytool -genkey -alias red5 -keyalg RSA -keypass password -storepass password -keystore c:\Sonexis\Red5\conf\keystore
```

Step 3. Type the new keystore password twice, pressing the Return key after each.

IMPORTANT: You must also use this password later for the `<red5>` key.

Step 4. When prompted to enter your **first and last name**, type the Common Name (CN) of the existing wildcard certificate (e.g., `*.example.com`) and press the Return key.

Step 5. Answer the remaining input prompts for organization and location.

Step 6. When prompted to **Enter key password for <red5>**, press the Return key to use the same password as the keystore.

Step 7. Verify that the file `C:\Sonexis\Red5\conf\keystore` was created.

2. GENERATING A CERTIFICATE REQUEST

After creating your keystore you can request an SSL certificate.

Step 1. Run the following command:

```
keytool -certreq -keyalg RSA -alias red5 -file c:\temp\red5.csr -keystore c:\Sonexis\Red5\conf\keystore
```

Step 2. Type the keystore password when prompted and press the Return key.

Step 3. Verify that the `c:\temp\red5.csr` file was created.

Step 4. Submit the `red5.csr` file to the Certificate Authority (CA, e.g., Verisign, Digitrust) and request a SSL server certificate.

Note: if the CA you choose is not well-known, you will need to import the CA's own certificate so your new certificate will be trusted.

3. IMPORTING THE NEW CERTIFICATE

Once the CA has issued your server certificate, you must import it into the new keystore.

Step 1. Copy the certificate to the webcam server and use the –file option to specify its directory and file name (in the example below the certificate file is `C:\temp\MyNewServerCert.cer`):

```
keytool -import -alias red5 -keystore c:\Sonexis\Red5\conf\keystore
-trustcacerts -file C:\temp\MyNewServerCert.cer
```

Step 2. Type the keystore password and press the Return key.

Step 3. If necessary, acquire your CA's certificate and copy it to the server and use the –file option to specify its directory and file name (in the example below the certificate file is `C:\temp\MyTrustedCACert.cer`):

```
keytool -import -alias root -keystore c:\Sonexis\Red5\conf\keystore
-trustcacerts -file C:\temp\MyTrustedCACert.cer
```

Step 4. Type the keystore password and press the Return key.

Step 5. Type **yes** and pres the Return key.

Step 6. Open the file `C:\Sonexis\Red5\conf\red5.properties` in a text editor.

Step 7. Find the property definition for `rtmps.keystorepass` and change the password to the keystore password.

This is the same password from Step 3 of "1. Creating a Keystore" on the previous page.

```
# RTMPS Keystore Password
rtmps.keystorepass=password
```

Step 8. Restart the Red5 Service, if it is running.

Configuring SSL for RTMPS (Existing Certificate)

This section describes the three main steps for configuring SSL on a webcam server if you have an existing wildcard SSL certificate (e.g., `www.example.com`).

1. EXPORTING THE EXISTING CERTIFICATE AND PRIVATE KEY

On Windows platforms you can use the MMC Certificates Snap-In to export your wildcard certificate and private key.

Step 1. From the Windows Start menu, run **MMC**.

Step 2. Select **File > Add/Remove Snap In**.

The Add/Remove Snap-ins window appears.

Step 3. Highlight **Certificates** and click **Add**.

The Certificates Snap-in configuration popup appears.

Step 4. Select **Computer Account** and click **Next**.

Step 5. Verify that **Local Computer** is selected and click **Finish**.

Step 6. Click **OK** to close the Add/Remove Snap-ins window.

Certificates can now be selected from the MMC Console Root.

Step 7. Expand the Console Root tree and select **Certificates > Personal > Certificates**.

Step 8. Right-click on the certificate you want to export and select **All Tasks > Export** to launch the Certificate Export Wizard

Step 9. Select **Yes, export the private key** and click **Next**.

Step 10. Select **Include all certificates...** and click **Next**.

Step 11. Enter a password for the exported private key.

IMPORTANT: You must also use this password for the keystore and `<red5>` key when generating the Java keystore.

Step 12. Confirm the password and click **Next**.

Step 13. Enter a filename for the exported key and click **Next**.

Step 14. Click **Finish** to export the certificate and private key to a file.

Step 15. Copy the exported file to the webcam server.

2. GENERATING THE WEBCAM SERVER KEYSTORE

This step establishes the webcam server's identity, creates a keystore, and creates a server private key for the alias `<red5>`. *It is critical that the password used to export the private key of your wildcard certificate, the keystore password, and <red5> password are identical.*

Step 1. Open a CMD window as Administrator on the Web Server and go to the Java \bin directory:

```
cd C:\Program Files\Java\jre7\bin
```

Step 2. Run the following keytool generation command:

```
keytool -genkey -alias red5 -keyalg RSA -keysize 2048 -keystore
c:\Sonexis\Red5\conf\keystore
```

Step 3. Type the new keystore password twice, pressing the Return key after each.

This is the same password from Step 11 of "1. Exporting the Existing Certificate and Private Key" on the previous page, used when exportng the certificate and private key.

Step 4. When prompted to enter your **first and last name**, type the Common Name (CN) of the existing wildcard certificate (e.g., `*.example.com`) and press the Return key.

Step 5. Answer the remaining input prompts for organization and location.

Step 6. When prompted to **Enter key password for <red5>**, press the Return key to use the same password as the keystore.

Step 7. Verify that the file `C:\Sonexis\Red5\conf\keystore` was created.

3. INSTALLING THE WEBCAM SERVER CERTIFICATE AND KEYSTORE

The final step is deleting the existing Red5 private key and updating the webcam server with the SSL certificate and new private key.

Step 1. Run the following command to delete the existing private key for Red5:

```
keytool -delete -alias red5 -keystore c:\Sonexis\Red5\conf\keystore
```

Step 2. Run the following command to import the wildcard certificate and private key:

```
keytool -v -importkeystore -srckeystore
C:\Temp\MyWildcardCertExport.pfx -srcstoretype PKCS12 -destkeystore
C:\Sonexis\Red5\conf\keystore -deststoretype JKS
```

Step 3. When prompted, type the destination keystore and source keystore passwords (which are identical), pressing the Return key after each.

Step 4. Type the source keystore password and press the Return key.

This is the same password from Step 11 of "1. Exporting the Existing Certificate and Private Key" on the previous page, used when exportng the certificate and private key.

Step 5. Open the file `C:\Sonexis\Red5\conf\red5.properties` in a text editor.

Step 6. Find the property definition for `rtmps.keystorepass` and change the password to the key store password/exported private key password:

```
# RTMPS Keystore Password
rtmps.keystorepass=password
```

Step 7. Restart the Red5 Service, if it is running.

Managing Servers

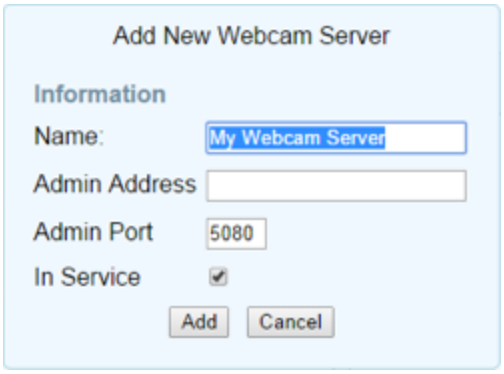
Adding a Webcam Server

You must add and configure webcam servers, even if the ConferenceManager itself is providing webcam services.

Step 1. From the **System** tab, click **Webcam**.

Step 2. Click **Add Webcam Server**.

The Add New Webcam Server dialog appears.



Step 3. Enter a webcam server **Name**.

Each webcam server must have a unique name.

Step 4. Enter an **Admin Address**.

You may use either a DNS name or IP address. The conferencing system must be able to connect to the webcam server on port 5080.

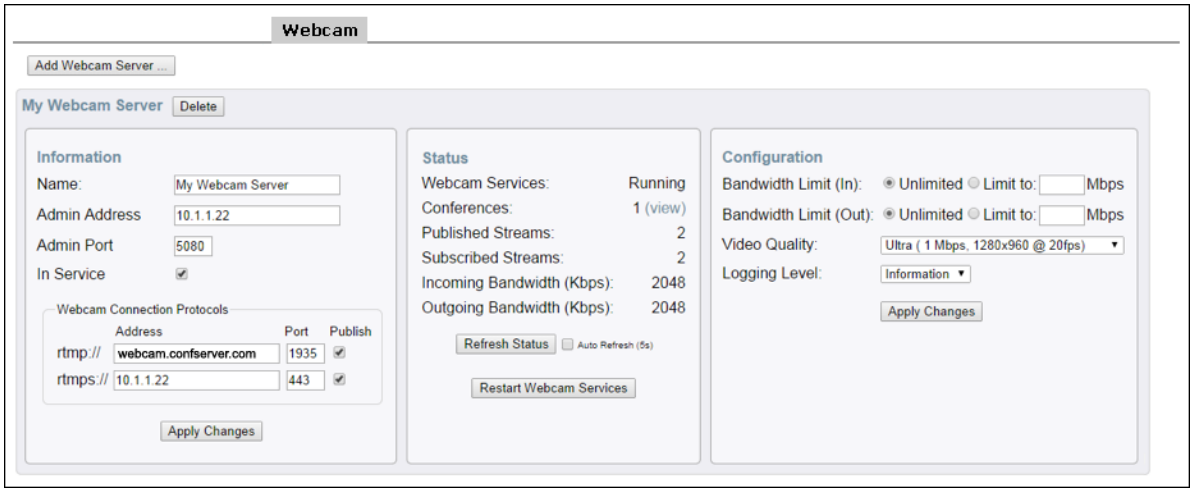
Step 5. If you do not yet want the server to be available for webcam services, uncheck **In Service**.

Step 6. Click **Add**.

Step 7. Continue with "Configuring Webcam Servers" on the next page.

Configuring Webcam Servers

The **Webcam** tab displays a panel for each webcam server added; there is no limit to the number of webcam servers allowed, and processing loads are automatically load-balanced across servers.



Step 1. Make changes to the **Information** section as necessary:

Parameter	Description	
Name	The webcam server name; must be unique.	
Admin Address	The DNS name or IP address of the server.	
Admin Port	The port over which the webcam server and conferencing server communicate.	
In Service	Enables the webcam service; if checked, the server will publish the selected webcam streams	
Webcam Connection Protocols	ConferenceManager supports two flavors of the Real Time Messaging Protocol, **RTMP** and **RTMPS**. You may enable either or both protocols: ■ If only RTMP is published, only unsecure connections over port 1935 are allowed (note that firewalls typically block port 1935 by default). ■ If only RTMPS is published, only secure connections over port 443 are allowed. ■ If both protocols are published, clients will attempt RTMP before RTMPS connection. Such a configuration would allow intranet clients to use RTMP while forcing WAN users to connect via RTMPS.	
	Address	The service address for each protocol. For best results, use a DNS name that can be resolved by both internal and external clients.
	Port	The service port for each protocol: **1935** for RTMP and **443** for RTMPS.
	Publish	Check the **Publish** check box to allow connections via that protocol.

Step 2. Click **Apply Changes**, if any were made.

Step 3. Make changes to the **Configuration** section as necessary:

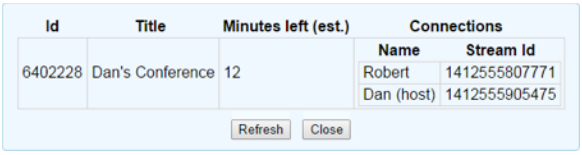
Parameter	Description
Bandwidth Limit (In)	The maximum bandwidth allowed for published video streams. If not **Unlimited** (the default), a Mbps limit can be set, after which no additional webcams can be published.
Bandwidth Limit (Out)	The maximum bandwidth allowed for viewed video streams. If not **Unlimited** (the default), a Mbps limit can be set, after which no additional streams can be viewed.
Video Quality	The video quality that the server will offer. Dividing the available bandwidth by that required for a given quality will give an approximation of how many streams the server can support. ■ **Ultra:** 1 Mbps, 1280 x 960 @ 20 fps ■ **Very High:** 768 Kbps, 640 x 480 @ 20 fps ■ **High:** 384 Kbps, 320 x 240 @ 20 fps ■ **Medium:** 192 Kbps, 320 x 240, 15 fps ■ **Low:** 64 Kbps, 160 x 120 @ 10 fps
Logging Level	The webcam logging level; logs are located in `C:\Sonexis\Red5\log` on each webcam server.

Step 4. Click **Apply Changes**, if any were made.

The **Status** panel allows you to monitor webcam server status.

Monitoring Webcam Servers

Each server panel on the **Webcam** tab includes a **Status** section with the server's current activity.

Item	Description
Webcam Services	Webcam service status (Running or Stopped)
Conferences	The number of conferences using webcams. When there are active conferences, click **View** to display a conference summary. 
Published Streams	The number of users publishing a webcam stream.
Subscribed Streams	The number of webcam streams being viewed.
Incoming Bandwidth	The maximum bandwidth used by all published streams, based upon the number of streams and selected video quality.
Outgoing Bandwidth	The maximum bandwidth used by all viewed streams.

Item	Description
Refresh Status	Click to update the statistics manually, or select the check box to automatically refresh the statistics every 5 seconds.
Restart Webcam Services	Restarts webcam services; this will disconnect any active webcam streams.

Suspending or Removing Webcam Servers

To suspend webcam services, uncheck a server's **In Service** check box and click **Apply Changes.** Conferences in progress will not be affected, but new server connections will not be allowed.

To delete a webcam server configuration altogether, click the **Delete** button next to the server name and confirm the deletion.