Inception Server SSL Setup

When you require secure communication between client computers and your Inception server, you can configure the Inception Server to use Secure Sockets Layer (SSL). After configuring your Inception Server to use SSL, client computers must use an https:// URL to connect to the server.

Configure the Web Server for SSL

By default, the web server on the Inception Server is not configured to use SSL. The http.conf file on your Inception Server computer contains the settings that control SSL.

To configure the Inception Server web server to use SSL

1. Log in to the **Inception Server** computer as **Inception**.
2. Locate the `http.conf` file in the following folder.

   `C:\Program Files\Ross Video\Inception\configuration`
3. Use the **Notepad** text editor to open and edit the `http.conf` file.
4. In the **HTTPS Configuration** section of the `http.conf` file, configure the following settings:

```
#*********************#
# HTTPS Configuration #
#*********************#
wrapper.java.additional.50=-Dorg.eclipse.equinox.http.jetty.https.enabled=true
wrapper.java.additional.51=-Dorg.eclipse.equinox.http.jetty.https.port=443
***This file should be stored in a location that will not change during upgrades***
wrapper.java.additional.52=-Dorg.eclipse.equinox.http.jetty.ssl.keystore=C:\Inception.keystore
wrapper.java.additional.53=-Dorg.eclipse.equinox.http.jetty.ssl.password=password
wrapper.java.additional.54=-Dorg.eclipse.equinox.http.jetty.ssl.keypassword=password
wrapper.java.additional.55=-Dorg.eclipse.equinox.http.jetty.ssl.needclientauth=false
wrapper.java.additional.56=-Dorg.eclipse.equinox.http.jetty.ssl.wantclientauth=true
wrapper.java.additional.57=-Dorg.eclipse.equinox.http.jetty.ssl.protocol=TLS
wrapper.java.additional.58=-Dorg.eclipse.equinox.http.jetty.ssl.algorithm=RSA
wrapper.java.additional.59=-Dorg.eclipse.equinox.http.jetty.ssl.keystoretype=JKS
```

5. Save the updated `http.conf` file and exit the **Notepad** text editor.

Generate or Import a Signed Certificate for the Inception Server

After you configure the Inception Server web server to use SSL, you need to generate a self-signed certificate or import an existing CA-signed certificate.

Generate a Self-Signed Certificate

You can use the Keytool or the OpenSSL command to generate a self-signed certificate.

- Self-signed certificates do not work for iPads. When iPads require secure communication with your Inception Server, you must import a CA-signed certificate.

When asked for your first and last name enter the Inception Server name to which you will connect, for example: inception.rossvideo.com.

Keytool Command

Self-Signed certificates generated using the Keytool command are valid for 10 years.

To use Keytool to generate a self-signed certificate

1. On the **Inception Server** computer, open a **Command** window.
2. In the **Command** window, enter the following command to change to the `C:\` folder:

   ```
   cd C:\
   ```

3. In the **Command** window, enter the following command to generate a private key file:

   ```
   keytool -genkey -keyalg RSA -alias inception -keystore inception.keystore -storepass password -validity 3800 -keysize 2048
   ```

4. Restart the **Ross Inception Service**.
5. Add the generated self-signed certificate to your trusted root certificate list to enable all browsers on your system to use the certificate, refer to the section "**Add a Self-Signed Certificate to Your Trusted Root Certificate List**" on page 4–3.

Openssl Command

You may need to install Openssl on your system before you can use the Openssl command to generate a self-signed certificate.

To use OpenSSL to generate a self-signed certificate

1. On the **Inception Server** computer, open a **Command** window.
2. In the **Command** window, enter the following command to generate a private key file:

   ```
   openssl genrsa -des3 -out inception.key 2048
   ```

3. To generate a Certificate Signing Request (CSR) file, enter the following command:

   ```
   openssl req -new -key inception.key -out inception.csr
   ```

4. To strip the password from the generated key file, enter the following commands:

   ```
   copy inception.key inception.key.org
   ```

   ```
   openssl rsa -in inception.key.org -out inception.key
   ```

5. To create self-signed certificate file (10 year), enter the following command:

```
openssl x509 -req -days 3650 -in inception.csr -signkey inception.key -out inception.crt
```

6. To combine the certificate and key files, enter the following command:

```
openssl pkcs12 -inkey inception.key -in inception.crt -export -out inception.pkcs12
```

7. To import into the key file, enter the following command:

```
keytool -importkeystore -srckeystore inception.pkcs12 -srcstoretype PKCS12
-destkeystore inception.keystore -deststoretype JKS
```

8. Restart the **Ross Inception Service**.

Import a CA-Signed Certificate

✶ The .crt file must be in PEM format. You can use the openSSL command to convert the .crt file to PEM format.

To import a CA-signed certificate

1. On the **Inception Server** computer, open a **Command** window.

2. In the **Command** window, enter the following command to generate a private key file:

```
keytool -keystore inception.keystore -alias inception -genkey -keyalg RSA
```

3. To generate a Certificate Signing Request (CSR) file, enter the following command:

```
keytool -certreq -alias inception -keystore inception.keystore -file inception.csr
```

4. To import the certificate into the key file, enter the following command:

```
keytool -keystore inception.keystore -import -alias inception -file inception.crt
-trustcacerts
```

5. Restart the **Ross Inception Service**.

6. Add the generated self-signed certificate to your trusted root certificate list to enable all browsers on your system to use the certificate, refer to the section "**Add a Self-Signed Certificate to Your Trusted Root Certificate List**" on page 4–3.

Add a Self-Signed Certificate to Your Trusted Root Certificate List

After you generate a self-signed certificate for your Inception Server, you can add the certificate to your trusted root certificate list to enable all browsers on your system to use the certificate.

Internet Explorer

To add a self-signed certificate to your trusted root certificate list

1. Log in to a client computer as a user with administrative privileges.
2. Start the **Internet Explorer** web browser.
3. Navigate to the **Inception** web page.
4. Ignore certificate warnings that display and continue to the **Inception** web page.
5. Click the **Certificate error** text at the top of the web browser window.
6. In the **Uninstall Certificate** dialog box, click **View certificates**.
7. In the **Certificate** dialog box, click **Install Certificate**.
8. In the **Store Location** section of the **Certificate Import Wizard**, select the **Local Machine** option.
9. Click **Next**.
10. Select the **Place all certificates in the following store** option.
11. Click **Browse**.
12. In the **Select Certificate Store** dialog box, select the **Show physical stores** check box.
13. Select the **Trusted Root Certificate Authorities** folder.
14. Click **OK**.
15. In the **Certificate Import Wizard**, click **Next**.
16. Click **Finish**.
17. In the **Alert** that displays, click **OK**.
18. In the **Certificate** dialog box, click **OK**.
19. Restart **Internet Explorer**.

Chrome

To add a self-signed certificate to your trusted root certificate list

1. Log in to a client computer as a user with administrative privileges.
2. Start the **Chrome** web browser.
3. Navigate to the **Inception** web page.
4. Click the **Caution** to the left of the **Inception** web page URL.
5. Click **Details** for the **Inception** web page.
6. In the **Certificate Error** section of the **Security Overview** panel, click **View Certificate**.
7. In the **Certificate** dialog box, click the **Details** tab.
8. In the **Details** tab, click **Copy to file**.
9. In the **Certificate Export Wizard**, click **Next**.
10. In the **Export File Format** panel, select the **Cryptographic Message Syntax Standard - PKCS #7 Certificate (.P7B)** option.
11. Click **Next**.
12. In the **File** name box, enter a file name for the certificate.
13. Click **Next**.
14. Click **Finish**.
15. In the **Alert** that displays, click **OK**.
16. In the **Certificate** dialog box, click **OK**.
17. Open the **Settings** page.
18. Click **Show advanced settings** at the bottom of the **Settings** page.
19. In the **HTTPS/SSL** section, click **Manage** certificates.
20. In the **Certificates** dialog box, click the **Trusted Root Certification Authorities** tab.
21. In the **Trusted Root Certification Authorities** tab, click **Import**.
22. In the **Certificate Import Wizard**, click **Next**.
23. In the **File to Import** panel, navigate to and select the certificate file (.cer) you saved in step **12**.

24. Click **Next**.

25. Click **Next**.

26. Click **Finish**.

27. In the **Alert** that displays, click **OK**.

28. In the **Certificates** dialog box, click **Close**.

29. Restart **Chrome**.

Single Sign On Setup with SSL Certificates

When setting up single sign on between Inception and Streamline servers you must import the certification file (.crt) for one server into the other server on both servers. Load the .crt file from the Streamline Server into the Inception Server cacert keystore and then load the .crt file from the Inception Server into the Streamline Server cacert keystore.

Inception Server

To load the .crt file from the Streamline Server into the Inception Server cacert keystore

1. Copy the `streamline.crt` file generated in step **5** of the **To use OpenSSL to generate a self-signed certificate** from the Streamline Server to the Inception Server.

2. From the Windows Desktop of the **Inception Server**, press **Windows Key+R**.

3. In the **Open** box of the **Run** dialog box, enter `cmd.exe`.

4. Click **OK**.

5. In the **Command Prompt** window, navigate to the `C:\Progrqam Files\Ross Video\inception\jre\bin` folder.

6. Enter the following command to load the .crt file from the Streamline Server into the Inception Server cacert keystore:

   ```
   keytool -keystore "C:\Progrqam Files\Ross Video\inception\jre\lib\security\cacerts"
   keystore -import -alias streamline -file streamline.crt -trustcacerts -storepass
   changeit
   ```

7. Restart the **Inception Server** service.

Streamline Server

To load the .crt file from the Inception Server into the Streamline Server cacert keystore

1. Copy the `inception.crt` file generated in step **5** of the **To use OpenSSL to generate a self-signed certificate** from the Inception Server to the Streamline Server.
2. From the Windows Desktop of the **Streamline Server**, press **Windows Key+R**.
3. In the **Open** box of the **Run** dialog box, enter `cmd.exe`.
4. Click **OK**.
5. In the **Command Prompt** window, navigate to the `C:\Progrqam Files\Ross Video\streamline\jre\bin` folder.
6. Enter the following command to load the .crt file from the Inception Server into the Streamline Server cacert keystore:

```
keytool -keystore "C:\Progrqam Files\Ross Video\streamline\jre\lib\security\cacerts"
keystore -import -alias inception -file inception.crt –trustcacerts –storepass changeit
```

7. Restart the **Streamline Server** service.

Email Server Setup to User Self-signed Certificate

To setup the Inception system email server to use a self-signed certificate

1. Copy the `inception.crt` file generated in step **5** of the **To use OpenSSL to generate a self-signed certificate** from the Streamline Server to the Email Server.
2. From the Windows Desktop of the **Email Server**, press **Windows Key+R**.
3. In the **Open** box of the **Run** dialog box, enter `cmd.exe`.
4. Click **OK**.
5. In the **Command Prompt** window, navigate to the `C:\Progrqam Files\Ross Video\streamline\jre\bin` folder.
6. Enter the following command to load the .crt file from the Inception Server into the Streamline Server cacert keystore:

```
keytool -keystore "C:\Progrqam Files\Ross Video\inception\jre\lib\security\cacerts"
keystore -import -alias inception -file inception.crt –trustcacerts –storepass changeit
```

7. Restart the **Email Server** service.

Renewing Certificates

If you originally used the PKCS 12 method to import your key and certificate files, use an alias of `1` instead of `inception`, to match the alias that the PKCS12 process enters into the keystore command. For example:

```
keytool -keystore inception.keystore -import -alias 1 -file inception.crt -trustcacerts
```

Contacting Technical Support

Technical Support is staffed by a team of experienced specialists ready to assist you with any question or technical issue.

Ross Video has technical support specialists strategically located around the globe to ensure a prompt response to technical inquiries. Our primary technical support center is located in Ottawa, Ontario, Canada. In addition, we have offices in The United Kingdom (London), Australia (Sydney), and Singapore with satellite locations in New York City, The Netherlands, and China. As we expand our presence globally, we are constantly evaluating other key locations to have a local technical support specialist in order to better service our customers.

North America

Our North America center located in Ottawa, Ontario, Canada and is open Monday to Friday 8:30 a.m. to 6:00 p.m. EST, with 24/7/365 on-call service after hours.

Our telephone number is: +1-613-686-1557

Toll free within North America: +1 833-859-0499

EMEA

Our EMEA center is located in Buckinghamshire, England, United Kingdom and is open Monday to Friday 8:30 a.m. to 5:00 p.m. GMT. After hours support is provided by our North America location.

International toll free: +800 3540 3545

Australia

Our Sydney, Australia office is located in Alexandria, NSW.

Our local support telephone number is: 1300 007 677

If the local support specialist is not available, your call will be transferred automatically to our North America center.

Online

E-mail: techsupport@rossvideo.com

Website: use the link https://support.rossvideo.com/ to open a support request.

Copyright