Cockpit HTTPS Connection

Cockpit enables you to use a web user interface to manage your Caprica Server through a secure HTTPS connection. Cockpit provides a self-signed certificate to enable web browser HTTPS access. Most modern web browsers flag the provided self-signed certificate as unsecured. To guarantee an HTTPS connection between your web browser and Cockpit, Ross Video recommends using a signed certificate.

The steps to set up a signed certificate depend on your web browser platform, your IT policies, and your Certificate Authority (CA). Ross Video recommends using an external CA to simplify certificate creation, deployment, and maintenance. You can also create your own internal CA and sign your own server certificate.

✶ Since each IT department and external CA has unique requirements that cannot be covered in this document, you should gather requirements from your IT department and CA before you proceed with the procedures in this application note.

Independent of using an internal or external CA, you must create a Certificate Signing Request (CSR) and a private key for each Caprica server in your system. The CA uses the CSR to create a signed certificate. You must copy the signed certificate and private key to the Caprica Server for the Cockpit to use.

✶ Due to the various customer security environments, this application note provides the basic steps to configure a secure HTTPS connection for Cockpit.

The following topics are discussed in this application note:

- Creating an Internal Certificate Authority
- Registering Your Certificate Authority with Your Web Browser
- Creating a Certificate Signing Request
- Signing a Server Certificate
- Preparing and Loading a Signed Certificate
- Disabling HTTPS Secure Connections

Creating an Internal Certificate Authority

✶ When you already have a CA on another server, your IT department provides you a CA, or your company uses an external CA, skip this section and continue with the section "**Registering Your Certificate Authority with Your Web Browser**" on page 4–2.

To create an internal Certificate Authority

1. Log in to your Caprica Server.
2. Create a folder to store certification files; for example: `ca_files`.
3. Change into your certification files folder.
4. Use a text editor to create a file named `ca.cfg`.
5. Enter the text below it the open `ca.cfg` file. Do not copy and paste the text below into the `ca.cfg` file as this may cause formatting errors in the file.

```
HOME            = .
RANDFILE        = $ENV::HOME/.rnd

[ ca ]
default_ca      = CA_default

[ CA_default ]
default_days     = 1000
default_crl_days = 365
default_md       = sha256
preserve         = no
x509_extensions  = ca_extensions
email_in_dn      = no
copy_extensions  = copy
certificate      = ./cacert.pem
private_key      = ./cakey.pem
new_certs_dir    = .
database         = ./index.txt
serial           = ./serial.txt

[ req ]
prompt  = no
default_keyfile    = cakey.pem
distinguished_name = ca_distinguished_name
x509_extensions    = ca_extensions
string_mask        = utf8only

[ ca_distinguished_name ]
countryName          = <country_name>
stateOrProvinceName = <state_province_name>
localityName         = <city_name>
organizationName     = <company_name>
commonName           = <common_name>
emailAddress         = <email_address>

[ ca_extensions ]
subjectKeyIdentifier   = hash
authorityKeyIdentifier = keyid:always, issuer
basicConstraints       = critical, CA:true
keyUsage               = keyCertSign, cRLSign

[ signing_policy ]
countryName            = optional
stateOrProvinceName    = optional
localityName           = optional
organizationName       = optional
organizationalUnitName = optional
commonName             = supplied
emailAddress           = optional

[ signing_req ]
subjectKeyIdentifier   = hash
authorityKeyIdentifier = keyid,issuer
basicConstraints       = CA:FALSE
keyUsage               = digitalSignature,
keyEncipherment
```

6. In the **[ca_distinguished_name]** section of the `ca.cfg` file, replace the text **<country_name>** with a two character abbreviation for the country in which your Caprica Server resides.
7. Replace the text **<state_province_name>** with the name of the state or province in which your Caprica Server resides.
8. Replace the text **<city_name>** with the name of the city in which your Caprica Server resides.
9. Replace the text **<company_name>** with the name of the company that owns your Caprica Server.
10. Replace the text **<common_name>** with the host name of your Caprica Server.
11. Replace the text **<email_address>** with the email address for the Caprica Server administrator.
12. Save and close the `ca.cfg` file.
13. In the folder that contains your `ca.cfg` file, run the following command to generate a CA certificate and a corresponding key:

    ```
    openssl req -x509 -config ca.cfg -newkey rsa:4096 -sha256 -out cacert.pem -outform PEM
    ```

14. At the `Enter PEM pass phrase:` prompt, enter a pass phrase for the CA certificate.

✶ Ross Video does not recommend creating a CA without a pass phrase.

The `openssl` command generates a CA certificate named `cacert.pem` and a corresponding key named `cakey.pem`.

Registering Your Certificate Authority with Your Web Browser

After you register a CA with a web browser, the web browser will trust any certificate signed by the CA. When using an internal CA, copy the generated `cacert.pem` file to each client computer that you use to access your Caprica Server.

✶ When your CA is already registered with your web browser, skip this section and continue with the section "**Creating a Certificate Signing Request**" on page 4–2.

The procedure to register a CA with a web browser depends on the following parameters in your work environment:

- Operating system of your computer.
- Web browser software
- Version of web browser software

Please refer to your web browser documentation for information on how to register your CA with your web browser.

Creating a Certificate Signing Request

Before you can generate a signed certificate, you must create Certificate Signing Request (CSR). A CSR contains information specific to the server. The CA also uses the CSR to generate a signed certificate.

✶ Each CA has different requirements for a CSR. Ross Video recommends checking CSR requirements with your CA provider before proceeding with the procedure in this section

To create a Certificate Signing Request for a Certificate Authority

1. Use a text editor to create a file named `csr.cfg`.
2. Enter the text below it the open `csr.cfg` file. Do not copy and paste the text below into the `csr.cfg` file as this may cause formatting errors in the file.

```
[req]
prompt             = no
default_bits       = 4096
default_md         = sha256
default_keyfile    = serverkey.pem
distinguished_name = dn
req_extensions     = v3_req

[dn]
countryName          = <country_name>
stateOrProvinceName = <state_province_name>
localityName         = <city_name>
organizationName     = <company_name>
commonName           = <common_name>
emailAddress         = <email_address>

[v3_req]
keyUsage = keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth
subjectAltName = @alt_names

[alt_names]
IP.1 = <IP_Address_NIC_1>   # NIC 1 IP address
IP.2 = <IP_Address_Cluster> # Cluster virtual IP address (OPTIONAL)
IP.3 = <IP_Address_NIC_2>   # NIC 2 IP address (OPTIONAL)
```

3. In the [dn] section of the `csr.cfg` file, replace the text **<country_name>** with a two character abbreviation for the country in which your Caprica Server resides.
4. Replace the text **<state_province_name>** with the name of the state or province in which your Caprica Server resides.
5. Replace the text **<city_name>** with the name of the city in which your Caprica Server resides.
6. Replace the text **<company_name>** with the name of the company that owns your Caprica Server.
7. Replace the text **<common_name>** with the host name of your Caprica Server.

8. Replace the text **<email_address>** with the email address for the Caprica Server administrator.
9. In the [alt_names] section, replace the text **<IP_Address_NIC_1>** with the IP address of your Caprica Server NIC 1.
10. Replace the text **<IP_Address_Cluster>** with virtual IP address of your Caprica Server cluster.

✶ If your Caprica system is not configured as a cluster, delete the **IP.2** alternate name from the `csr.cfg` file.

11. Replace the text **<IP_Address_NIC_2>** with the IP address of your Caprica Server NIC 2.

✶ If your Caprica system is not configured to use NIC 2, delete the **IP.3** alternate name from the `csr.cfg` file.

12. If you deleted an alternative name from the [alt_names] section, rename the alternate name so that they are sequential starting with **IP.1**.
13. Save and close the `csr.cfg` file.
14. In the folder that contains your `csr.cfg` file, run the following command to generate a CSR file:

    ```
    openssl req -config csr.cfg -newkey
    rsa:4096 -sha256 -nodes -out
    servercert.csr -outform PEM
    ```

    The openssl command generates a CSR file named server.csr and a corresponding key named **serverkey.pem**.

Signing a Server Certificate

IT Department or External CA

If you use a CA managed by your IT department or an external CA, you must sent your CSR file to your IT department or external CA so they can generate a signed certificate for you. Remember to get your IT department or an external CA to return the signed certificate generated from your CSR file to you.

✶ Cockpit expects signed certificates to be PEM encoded x509 certificates.

In the following sections, the signed certificate is refereed to as the **servercert.pem** file.

Internal CA

If you use your own internal CA, you can generate your own signed certificate.

To generate a signed certificate

1. Before signing your first certificate, complete the following steps to create a CA database:
   a. In the folder that contains your `csr.cfg` file, run the following command to create an empty file named `index.txt`:
   b. `touch index.txt`
   c. The **openssl** command updates the `index.txt` file every time you sign a certificate.
   d. Run the following command to create a file named `serial.txt` containing a value of `01`.
   e. `echo '01' > serial.txt`
   f. The `serial.txt` file contains the next available serial number in hex, which the **openssl** command updates every time you sign a certificate.

   With the CA database created, you are ready to sign certificates.
2. In the folder that contains your server.csr, index.txt, and serial.txt files, run the following command to sign your certificate:

   ```
   openssl ca -config ca.cfg -policy
   signing_policy -extensions signing_req
   -out servercert.pem -infiles server.csr
   ```
3. At the Enter pass phrase for /cakey.pem: prompt, enter the pass phrase you set for your CA certificate in step 14 of the procedure "**To create an internal Certificate Authority**" on page 4–1.
4. At the **Sign the certificate? [y/n]:** prompt, enter `y`.

   The openssl command creates a signed certificate file named **servercert.pem**.

Preparing and Loading a Signed Certificate

Your signed certificate `servercert.pem` file and the private key `servercert.pem` file are concatenated to make a `.cert` file. Cockpit loads `.cert` files from the `/etc/cockpit/ws-certs.d` folder on a Caprica Server. When Cockpit loads a certificate, it loads the last file alphabetically with the `.cert` extension.

To prepare and load a signed certificate

1. In your certification files folder, run the following command to create a file named **100-server.cert** and write the contents of your **servercert.pem** to the new file:

   ```
   cat servercert.pem > 100-server.cert
   ```
2. Run the following command to append the content of your **serverkey.pem** file to your **100-server.cert** file:

   ```
   cat serverkey.pem >> 100-server.cert
   ```

3. Run the following command to move your **100-server.cert** file to the **/etc/cockpit/ws-certs.d** folder:

```
sudo mv 100-server.cert
/etc/cockpit/ws-certs.d/100-server.cert
```

4. Run the following command to restart Cockpit and load your signed certificate:

```
sudo systemctl restart cockpit
```

Disabling HTTPS Secure Connections

It is possible to disable HTTPS secure connections for your Caprica system. You should only disabling HTTPS secure connections on a segregated network that is not accessible from the internet.

✶ Ross Video does not recommend disabling HTTPS secure connections for your Caprica system.

To disable HTTPS secure connections for your Caprica system

1. Log in to your Caprica Server.
2. Change into the `/etc/cockpit/` folder.
3. Use a text editor to create a file named `cockpit.conf`.
4. Enter the following text in the open `cockpit.conf` file:

```
[WebService]
AllowUnencrypted = true
```

5. Save and close the `cockpit.conf` file.
6. Run the following command to restart Cockpit:

```
sudo systemctl restart cockpit
```

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: +1 844-652-0645

EMEA

Our EMEA center 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.

Our telephone number is: +44 (0)1189502446

International toll free: +800 3540 3545

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

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: open a support request using the link http://www.rossvideo.com/support/tech-support.html to open a support request.

Copyright

