



# USING A MULTI-DOMAIN SSL CERTIFICATE WITH A 3-SERIES PROCESSOR

RESIDENTIAL APPLICATION

Crestron Electronics, Inc.

---

## REVISION HISTORY

---

Version	Date	Comments	Author
1.1	8/22/2018	Updated to reflect new information.	AS

Crestron and the Crestron logo are either trademarks or registered trademarks of Crestron Electronics, Inc. in the United States and/or other countries. Other trademarks, registered trademarks, and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Crestron disclaims any proprietary interest in the marks and names of others. Crestron is not responsible for errors in typography or photography.

## TABLE OF CONTENTS

1	Introduction .....	4
2	Control System Ethernet Configuration .....	5
3	Register Control System With MyCrestron DNS.....	5
4	Using Gandi.NET.....	8
4.1	Register the Domain.....	8
4.2	Create Subdomain Records .....	8
4.3	Create Certificate Signing Request (CSR) .....	12
4.4	Create SSL Certificate.....	12
4.5	Download the SSL Certificate.....	15
5	Creating a Certificate Signing Request (CSR).....	17
6	Uploading Certificates to the Control System .....	20
7	Enable SSL Certificate and Encrypted Communication For Web Xpanel.....	21
8	Configure Ports in Router Firewall.....	24
9	Basic SSL Testing.....	25
9.1	Internal Network .....	25
9.2	External Network.....	26
10	Crestron App.....	26
11	Xpanel Web .....	27
11.1	Connection Properties .....	27
11.2	Core3 Xpanel Web .....	27
11.3	Internal Network .....	27
11.4	External Network.....	28
12	Appendix.....	29
12.1	Domain Registrar .....	29

# 1 INTRODUCTION

This guide will provide step-by-step instructions for installing a multi-site SSL certificate in a Crestron 3-Series control system. Specific domain registrars were selected to reduce confusion and provide the exact steps needed. The following registrars were selected for this guide:

- gandi.net

The purpose of using a multi-domain certificate in a residence is to provide support for multiple encrypted connections to more than one hostname, but utilize a single SSL certificate.

I.E. With a registered domain of "JohnsHome.com", multiple subdomains can be secured: "AVInside.JohnsHome.com", "AVOutside.JohnsHome.com", "Security.JohnsHome.com", "CameraDVR.JohnsHome.com", etc.

Since the Crestron App supports multiple connection configurations, one subdomain can be used for inside the residence and another for outside.

The following are requirements with this guide:

1. Control system must use a static IP address (can be a reserved DHCP address).
2. Domain(s) must be registered with a public DNS provider. (I.E. gandi.net)
3. 3-Series control system must be running firmware 1.010.0060 and above.

The control system must be registered with the MyCrestron DNS service.

## 2 CONTROL SYSTEM ETHERNET CONFIGURATION

If the home router supports DHCP Address Reservation, it is highly recommended that it be used and that the control system Ethernet configuration be set to DHCP.

**Note:** Since the public domain registrar will be used to resolve the fully qualified hostname of the control system, the “Domain Name” field cannot contain the registered domain. Use anything other than the domain registered with the public registrar or simply leave it blank.

If the home router does not support DHCP Reservation, manually configure the Ethernet port of the control system and set a static IP address. Do not forget to configure the DNS server(s).

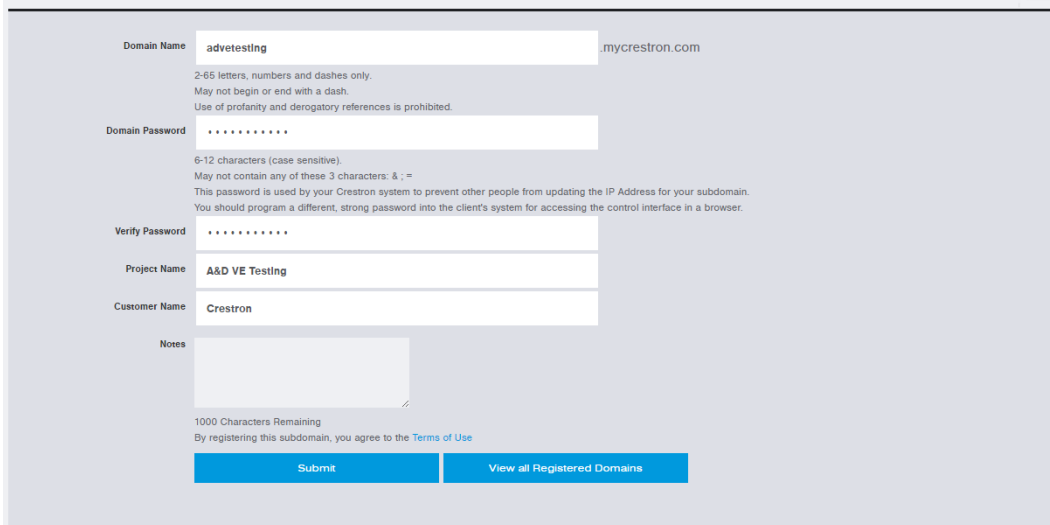
In either case, note the IP address of the control system. For the purpose of this guide, the IP address of the control system is 192.168.1.35 and this was set in the DHCP Address Reservation list of the home router.

## 3 REGISTER CONTROL SYSTEM WITH MYCRESTRON DNS

The control system needs to be registered with the MyCrestron DNS service. This service will be used to resolve the public facing home router to a DNS name that can be used with the SSL certificate.

1. Before configuring the control system, log into the Crestron website and register a domain for the control system here: <http://www.crestron.com/resources/design-install-tools/my-crestron-dynamic-dns-ddns>.

For the purpose of this guide, the following information was registered:



The screenshot shows a registration form for a subdomain. The form fields are as follows:

- Domain Name:**  .mycrestron.com. Below the field, it says: "2-65 letters, numbers and dashes only. May not begin or end with a dash. Use of profanity and derogatory references is prohibited."
- Domain Password:** . Below the field, it says: "6-12 characters (case sensitive). May not contain any of these 3 characters: & ; =. This password is used by your Crestron system to prevent other people from updating the IP Address for your subdomain. You should program a different, strong password into the client's system for accessing the control interface in a browser."
- Verify Password:**
- Project Name:**
- Customer Name:**
- Notes:**

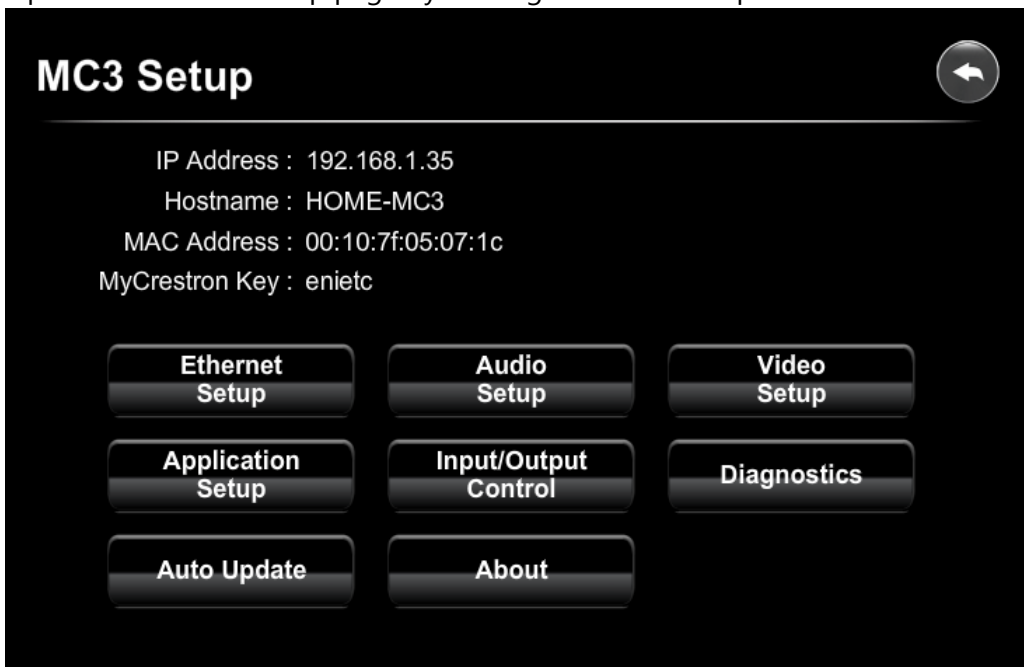
At the bottom of the form, it says "1000 Characters Remaining" and "By registering this subdomain, you agree to the Terms of Use". There are two buttons: "Submit" and "View all Registered Domains".

Make sure the password used for registration is noted, as it will be required in the control system registration page.

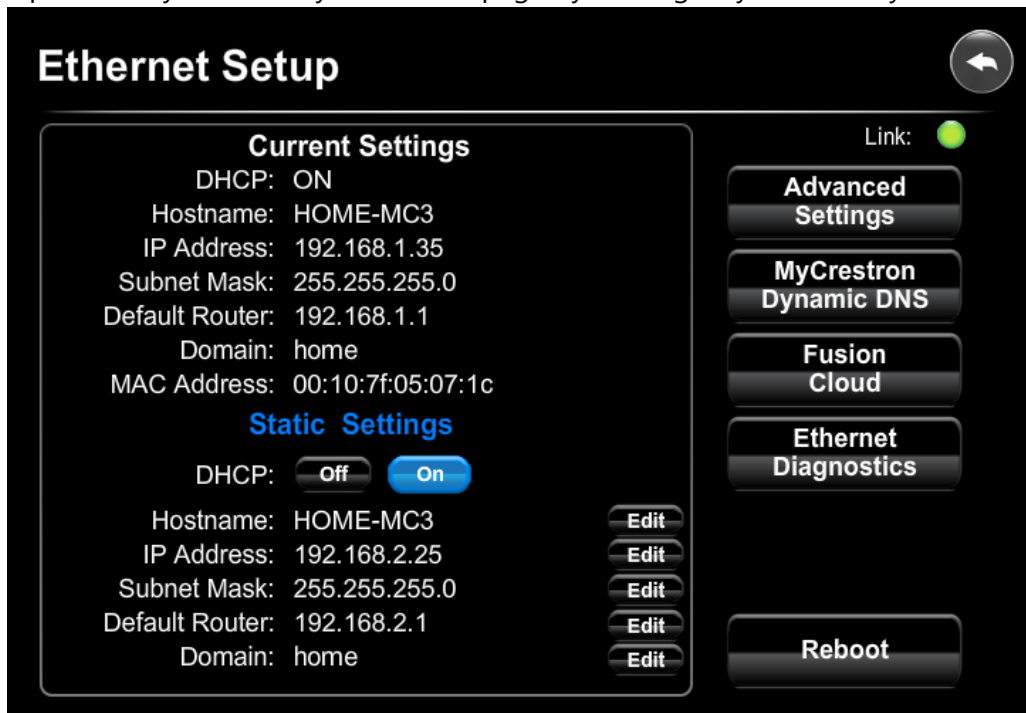
2. After a domain is registered at the Crestron website, use a web browser and open the control system configuration interface using [http://<control\\_system\\_ip>/setup](http://<control_system_ip>/setup). Click "Setup".



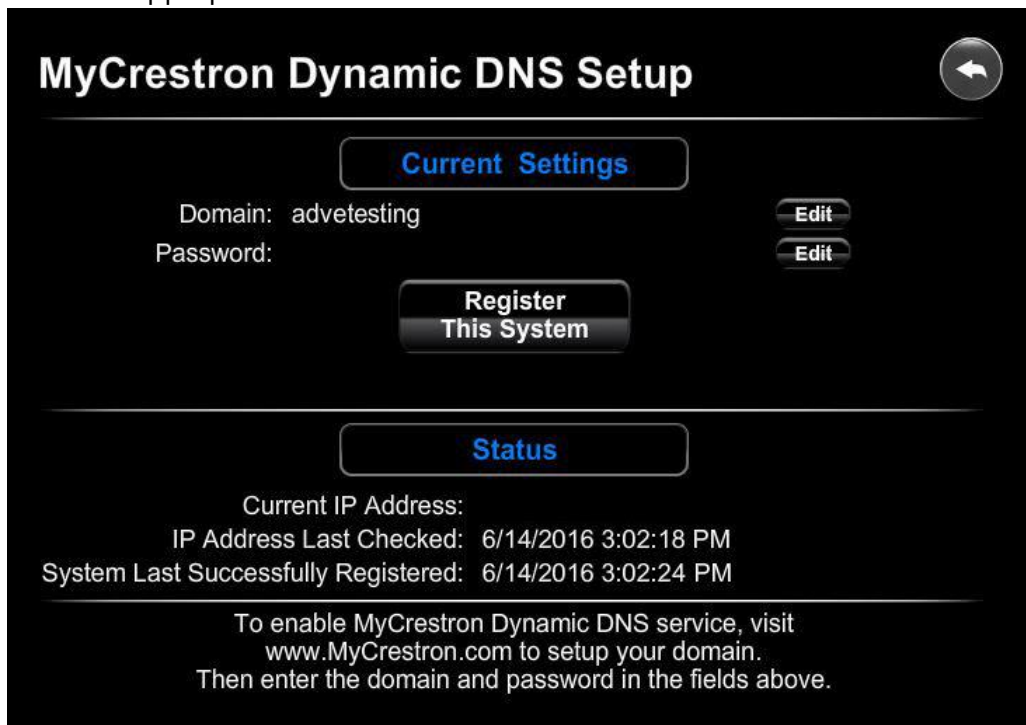
3. Open the Ethernet Setup page by clicking "Ethernet Setup".



4. Open the MyCrestron Dynamic DNS page by clicking "MyCrestron Dynamic DNS".



5. Enter the appropriate data.



- Edit the domain and enter the registered MyCrestron domain (from Step 1).
- Edit the password and enter the password used for registration (from Step 1).
- Click "Register This System".

## 4 USING GANDI.NET

This section will provide detailed instructions using gandi.net as the domain registrar, as well as the SSL certificate provider.

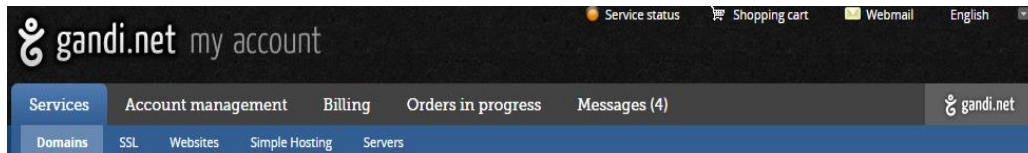
### 4.1 REGISTER THE DOMAIN

Using the domain search page: <https://www.gandi.net/domain> find an available domain and register it. During the registration process, an account will be created.

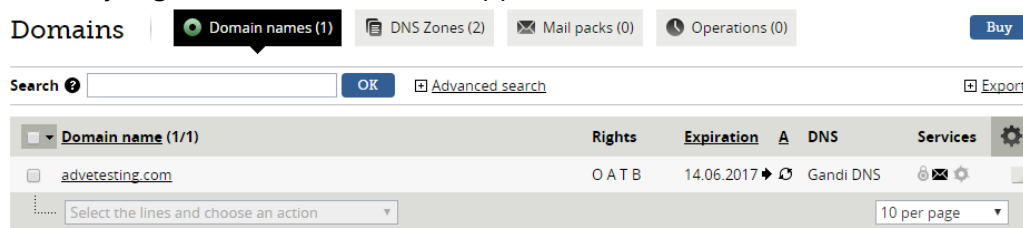
For the purpose of this guide, “advetesting.com” was registered.

### 4.2 CREATE SUBDOMAIN RECORDS

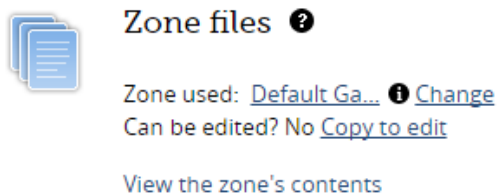
1. In the “Services” tab of the main menu, select “Domains”.



2. The newly registered domain should appear in the interface. Click the domain to edit it.

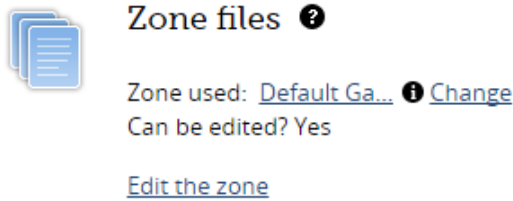


3. To add a new subdomain, the zone file must be edited. However, a zone file that is currently in use cannot be edited. A copy of an “in-use” zone file must be made first.
4. If this is the first time editing the zone file, the interface will provide a link to create a copy. Click the “Copy to edit” link.

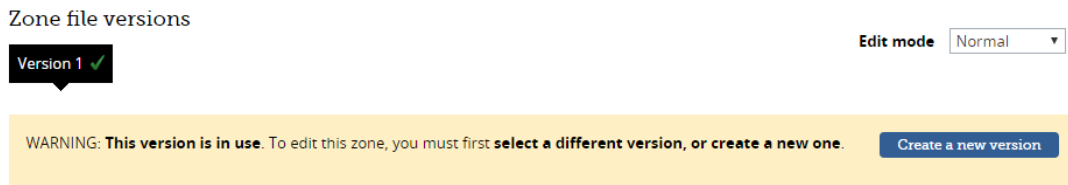




5. Once a copy is made, the zone file can be edited. Click the "Edit the zone" link.

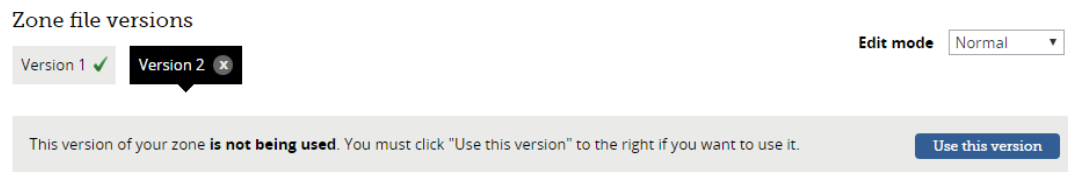


6. If this was the first copy made, it will have already been put "in-use". A notice will be displayed in the interface.



Click "Create a new version".

7. The new version of the zone file can now be edited. The interface will provide a message stating that this version of the zone file is not "in-use".



**DO NOT click "Use this version" until all subdomain records have been added.**

8. First, a subdomain record needs to be created that will be used for connections inside the residence. Click the "Add" button to create a new record. Leave the "Type" as "A" and set the "TTL" to "1 hour". Enter the desired name for the subdomain in the "Name" field. Do not include the registered domain value in this field. It will automatically be appended in the actual server.

I.E. If "myinsideconnection" is entered in the field, and the registered domain is "cooldomain.com", the full subdomain will be "myinsideconnection.cooldomain.com".

Enter the inside IP address of the control system into the "Value" field.

For our example domain (advetesting.com), it was decided to use "avinside" for the internal connection. This means the entire subdomain will be "avinside.advetesting.com". Since the internal IP address of the control system is 192.168.1.35, that was entered into the "Value" field. The following values were entered in the dialog:

**Add a record**

The screenshot shows a web form titled "Add a record". It has the following fields and values:

- Type: A (dropdown menu)
- TTL: 1 (input field) hours (dropdown menu)
- Name: avinside (input field)
- Value: 192.168.1.35 (input field)
- MX priority: (empty input field)

Below the MX priority field is a small text note: "Enter a number between 0 and 65535".

On the right side of the form, there is a warning message: "Use a Gandi service: Warning for some services, you will need to go to the service's interface to activate it." Below this is a bullet point: "• [Web forwarding service](#)".

At the bottom right of the form are two buttons: "Back" and "Submit".

9. Next, a subdomain record needs to be created that will be used for connections outside the residence. Click the "Add" button to create a new record. This time, set the "Type" as "CNAME" and set the "TTL" to "1 hour". Enter the desired name for the subdomain in the "Name" field. As with Step 8, do not include the registered domain value in this field. It will automatically be appended in the actual server.

I.E. If "myoutsideconnection" is entered in the field, and the registered domain is "cooldomain.com", the full subdomain will be "myoutsideconnection.cooldomain.com".

Enter the full MyCrestron registered domain into the "Value" field.

I.E. If "johnshome" was registered with MyCrestron, the full name that should be entered is "johnshome.mycrestron.com".

For our example domain (advetesting.com), it was decided to use "avoutside" for the external connection. This means the entire subdomain will be "avoutside.advetesting.com". From earlier in this guide, the MyCrestron value for our example domain was "advetesting" making the field value "advetesting.mycrestron.com". The following values were entered in the dialog:

## Add a record

Type \*

TTL \*

Name \*

Value \*

MX priority \*

Enter a number between 0 and 65535

Use a Gandi service:  
**Warning** for some services, you will need to go to the service's interface to activate it.

- [GandiBlog service](#)
- [POP/IMAP service](#)
- [POP/IMAP service](#)
- [mail forwarding service](#)
- [webmail.gandi.net](#)
- [web forwarding subdomain](#)
- [fr.sitemakerlive.com](#)
- [Gandi Site](#)

10. Now that the subdomain records have been created in the zone file, the file needs to be set "in-use".

Zone file versions

Version 1 ✓ Version 2 ✗

Edit mode

This version of your zone is **not being used**. You must click "Use this version" to the right if you want to use it.

Click "Use this version".

11. It will take some time for these records to become live. Please verify that the DNS records are "live" before continuing with this guide.

The records can be verified by using a simple PING command in a DOS prompt.

For our example domain (advetesting.com), using the subdomains that were just created, the following pings were issued:

- "ping avinside.advetesting.com"

This ping will only return a valid result if it is issued from inside the residence. If it is issued outside the residence, the request will timeout, but the registered IP address should be shown in the first line:

```
Pinging avinside.advetesting.com [192.168.1.35] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

This at least validates that the subdomain is using the correct IP address.

- "ping avoutside.advetesting.com"

This ping should return the IP address of the home router, registered by the control system using the MyCrestron DNS.

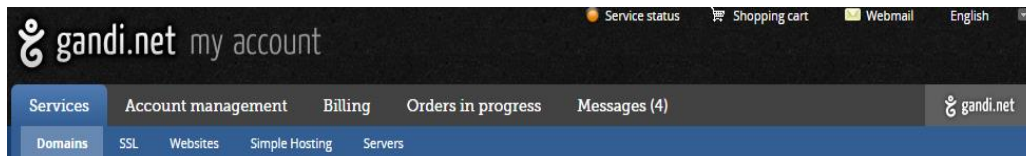
### 4.3 CREATE CERTIFICATE SIGNING REQUEST (CSR)

Follow the directions in **Section 5 - Creating a Certificate Signing Request (CSR)**.

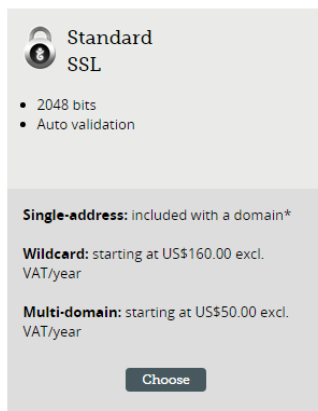
### 4.4 CREATE SSL CERTIFICATE

Once the CSR has been generated, an SSL certificate can now be created.

1. Log back into gandi.net.
2. In the "Services" tab of the main menu, select "Domains".



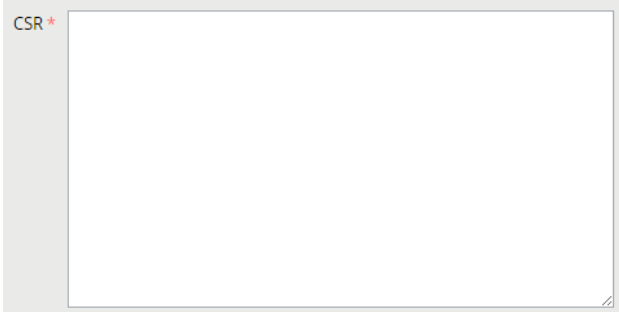
3. Click the padlock icon (in the "Services" column) to add an SSL certificate to the domain.
4. Click the **Get an SSL certificate** button.
5. Select the "Standard SSL" certificate.



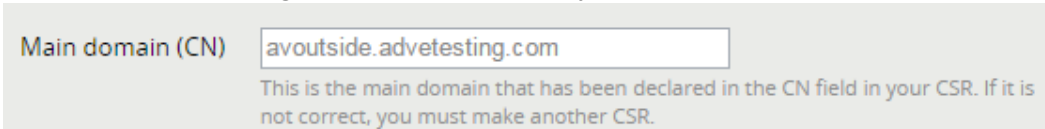
6. Select "Multi-Domain".



- Using a text editor (like Notepad++), open the CSR file generated in **Section 4.3 - Create Certificate Signing Request (CSR)** and paste the contents, including the "BEGIN" and "END" tags, into the CSR data field.

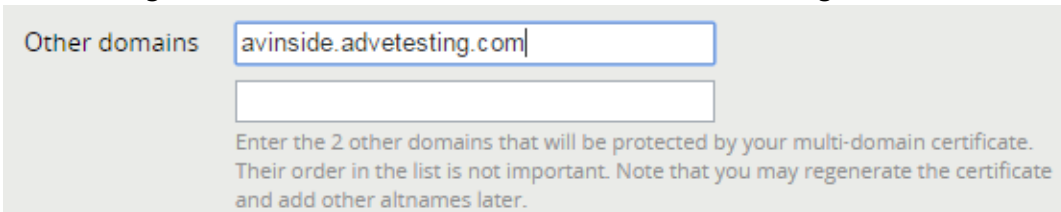
A screenshot of a web form showing a large, empty text area for pasting CSR data. The label "CSR \*" is visible in the top left corner of the form.

- The CSR main domain will be shown in the "Main domain (CN)" field. For our example domain (advetesting.com), we created the CSR using the subdomain "avoutside.advetesting.com". The field displayed this:

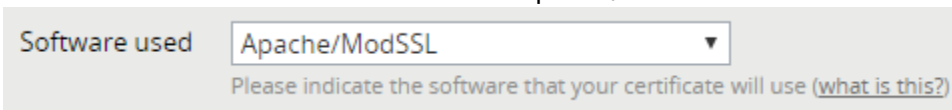
A screenshot of a web form showing the "Main domain (CN)" field. The text "avoutside.advetesting.com" is entered in the input box. Below the input box, there is a note: "This is the main domain that has been declared in the CN field in your CSR. If it is not correct, you must make another CSR."

This correctly matches the registered subdomain.

- Next, enter the inside subdomain that was registered earlier. For our example domain (advetesting.com), the inside subdomain is "avinside.advetesting.com".

A screenshot of a web form showing the "Other domains" field. The text "avinside.advetesting.com" is entered in the first of two input boxes. Below the input boxes, there is a note: "Enter the 2 other domains that will be protected by your multi-domain certificate. Their order in the list is not important. Note that you may regenerate the certificate and add other altnames later."

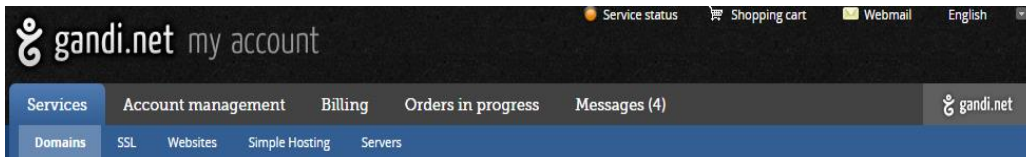
- Leave the "Software used" value set to "Apache/ModSSL".


A screenshot of a web form showing the "Software used" field. The dropdown menu is set to "Apache/ModSSL". Below the dropdown, there is a note: "Please indicate the software that your certificate will use ([what is this?](#))"

- Finalize the purchase of the certificate.
- Once payment is approved, an email will be provided with a link to complete the SSL certificate validation process. **DO NOT click the link.** By default, the validation rights to the domain uses a DNS record to validate each subdomain. Since gandi.net provides 5 free email addresses with the domain purchase, it is actually easier to use Gandi mail to validate the subdomains.

13. Log back into gandi.net.

14. In the "Services" tab of the main menu, select "Domains".



15. Click the email  icon (in the "Services" column) to activate the Gandi mail services.

16. Create a new mailbox called "admin".

17. Activate the mail service by clicking the activate link.

**Gandi Mail service:** not activated [activate](#)

18. Open Gandi Webmail by clicking the access link.

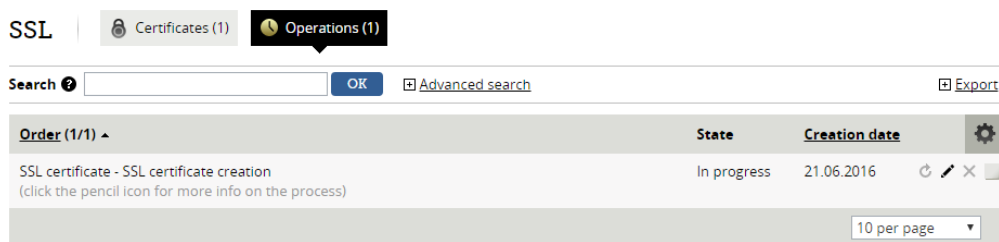
**Gandi Webmail:** [Access](#)

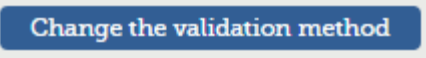
19. Log into the admin mailbox created in Step 16 and leave the interface open.

20. In the "Services" tab of the gandi.net main menu, select "SSL".



21. Selection "Operations" and then select the pencil  icon.



22. Click the  button to open the validation configuration dialog. Change the method to “Validation by email”.

Chosen method

Validation by DNS record  
Validation by DNS record implies that you have access to the DNS zone file of your domain, and can add a record to it. If you opt for this method, the record to be inserted into the zone will be displayed on the following page.

Validation by email  
This validation method is simple, though requires that you have an email address available for **for each domain validated**. This email address must be created with the user **admin@** (ex.: if you want to validate the domain **example.com**, you must create the email address **admin@example.com**). If you did not get the validation email, go to your validation status interface and relaunch the sending of the verification emails.

Validation by file  
This validation method requires that you have access to the server that hosts the website that the domain will point to. You are asked to copy a TXT file that contains a verification key, and to place it at the root directory of the website. If you don't have the hosting set up for your site, or if you don't have access to the root directory, then choose another validation method. **Warning: Your .TXT file should only be available through HTTP. The validation will not work with HTTPS redirection.**

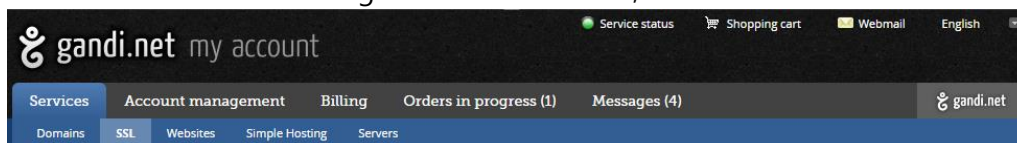
[Back](#) [Submit](#)

23. Two emails will now be sent to the “admin@” mailbox created in Step 16. Follow the instructions to validate the subdomains.

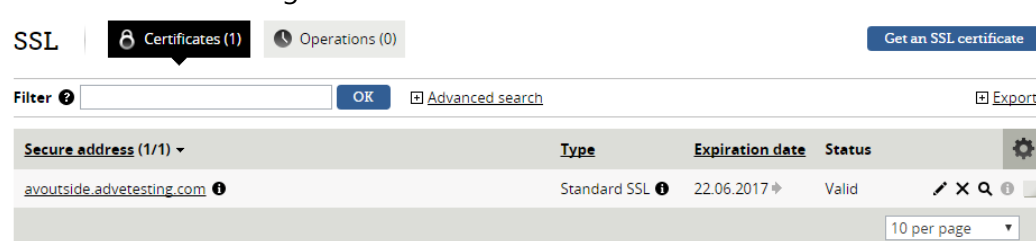
## 4.5 DOWNLOAD THE SSL CERTIFICATE

Once the SSL certificate has been issued, it can be downloaded from your account.

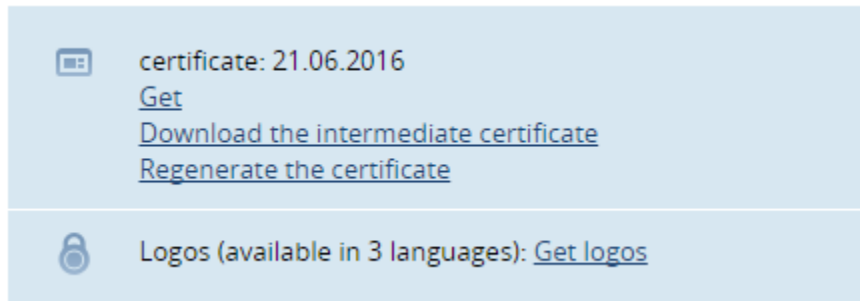
1. Log back into gandi.net.
2. In the “Services” tab of the gandi.net main menu, select “SSL”.



3. The subdomain that just received an SSL certificate should be shown in the list. For our example domain (advetesting.com), the certificate for the subdomain “avoutside.advetesting.com” was in the list. Click the actual subdomain name.



- Download both the actual SSL certificate, as well as the intermediate certificate. Click "Get" for the SSL certificate. Click "Download the intermediate certificate" for the intermediate.



Note: If either of the certificates do not download as files, but display raw data in the browser window, simply select all the data and paste it into a text document (Notepad++ works well for this). Save each file separately with a .cer file extension. Note the filenames to distinguish the SSL from the Intermediate certificate.

- To validate the contents of both the SSL and Intermediate certificates, use one of the free online services.

I.E. <https://www.sslshopper.com/certificate-decoder.html>.

Simply paste the contents of the .cer/.crt files into the decoding window. For the SSL certificate, verify that both registered subdomains are reflected.

For our example domain (advetesting.com), this is what was decoded:

**Certificate Information:**

- ✓ **Common Name:** avoutside.advetesting.com
- ✓ **Subject Alternative Names:** avoutside.advetesting.com, avinside.advetesting.com
- ✓ **Organization Unit:** Domain Control Validated
- ✓ **Valid From:** June 20, 2016
- ✓ **Valid To:** June 21, 2017
- ✓ **Issuer:** Gandi Standard SSL CA 2, Gandi
- ✓ **Serial Number:** 144e13b633e431c578acd5d56824d9f8

This reflects that both of the subdomains are supported with this certificate.

- See **Section 6 – Uploading Certificates to the Control System** for instructions on how to upload the certificates.



## 5 CREATING A CERTIFICATE SIGNING REQUEST (CSR)

A certificate signing request must be created before an SSL certificate can be issued.

**Note:** Once the CSR is generated and submitted to the certificate provider, DO NOT generate another CSR. At the moment the CSR is generated using the control system, a private key file (.pvk) is created. This file is unique to the CSR.

1. Using Toolbox -> System Info, connect to the control system.
2. Select Functions -> SSL Management.
3. Check "Enable SSL". Leave the "Certificate Settings" type as "Self-Signed"  Signed". Click  next to "Certificate Management" and select Generate Certificate Request.

SSL Management - auto SGVE-CP3-ARA

Enable SSL

SSL Settings

Secure CIP Port: 41796

Secure CTP Port: 41797

Secure Web Port: 443

Secure Gateway Mode:

SSL Fallback:

Certificate Settings

Certificate Management

Self-Signed  CA-Signed

Password:

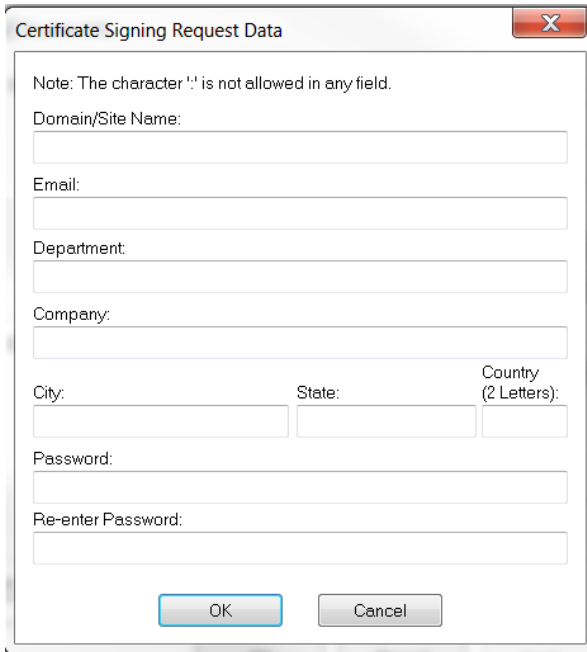
Re-enter Password:

Disable Weak Ciphers

OK Cancel Apply

- Fill in all of the fields, making sure the domain is entered correctly. Since our SSL certificate is a multi-domain type, either of the subdomains can be entered into the "Domain/Site Name" field.

Note: A password is required to generate the CSR and PVK files. **DO NOT forget the password as it is required before you install the SSL certificate.**



Certificate Signing Request Data

Note: The character ':' is not allowed in any field.

Domain/Site Name:

Email:

Department:

Company:

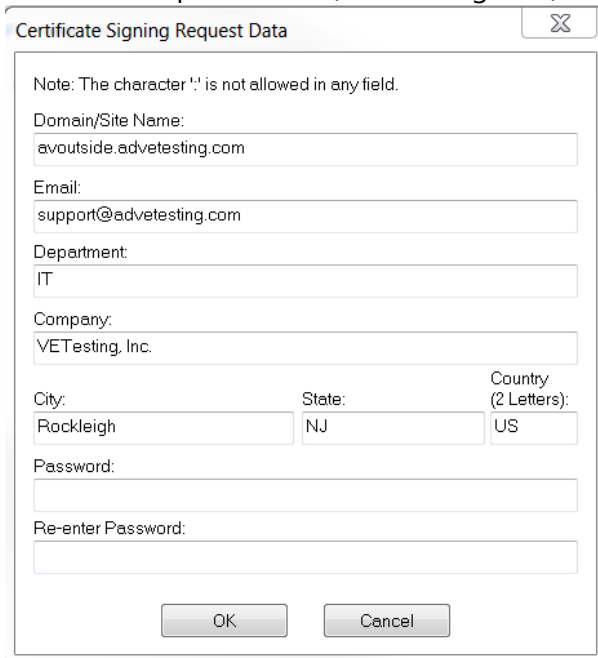
City: State: Country (2 Letters):

Password:

Re-enter Password:

OK Cancel

For our example domain (advetesting.com), the following data was entered:



Certificate Signing Request Data

Note: The character ':' is not allowed in any field.

Domain/Site Name: avoutside.advetesting.com

Email: support@advetesting.com

Department: IT

Company: VETesting, Inc.

City: Rockleigh State: NJ Country (2 Letters): US

Password:

Re-enter Password:

OK Cancel

5. Save the .csr file to an accessible directory on a PC.
6. You can verify the contents of the CSR using an online verification tool.

I.E. <https://www.sslshopper.com/csr-decoder.html>.

Simply copy the contents of the CSR file into the decoding window.

For our example domain (advetesting.com) CSR, the following was revealed:

**CSR Information:**

- ✓ **Common Name:** avoutside.advetesting.com
- ✓ **Organization:** VETesting, Inc.
- ✓ **Organization Unit:** IT
- ✓ **Locality:** Rockleigh
- ✓ **State:** NJ
- ✓ **Country:** US
- ✓ **Email:** support@advetesting.com



7. It is **highly** advisable to store a copy of the .pvk file in a directory on a local PC. Using Toolbox -> File Manager, browse to the "Sys" folder and export a copy of the "srv\_key.pvk" file. This will allow the SSL certificate to be installed again, should the control system need to be replaced.
8. If the SSL certificate is going to be created at a later date or if the creation is going to take some time, the "Enable SSL" checkbox can be cleared so the control system can operate without SSL until the certificate is ready.

## 6 UPLOADING CERTIFICATES TO THE CONTROL SYSTEM

Once the SSL certificate has been issued, two files need to be uploaded to the control system. The first is the Root Certificate and the second is the actual SSL Certificate.

The SSL certificate supplier should have provided an intermediate certificate. This will be used as the RootCA certificate in the control system.

If either of the files do not have a .cer extension, simply copy the files and rename the extension to .cer.

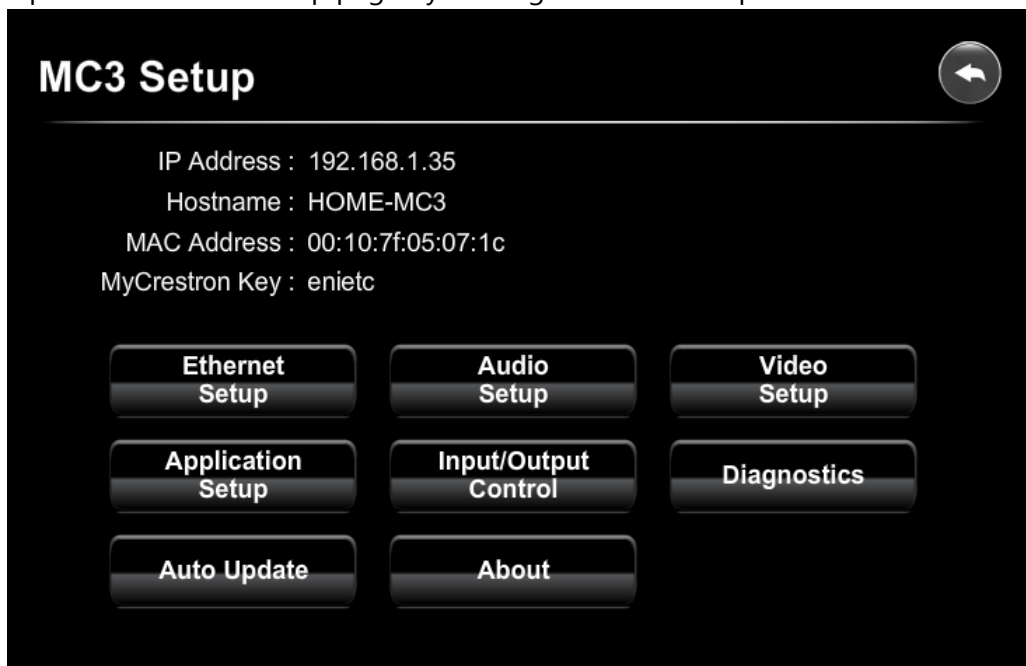
1. Using Toolbox -> System Info, connect to the control system.
2. Select Functions -> SSL Management.
3. Check the "Enable SSL" box if it is unchecked.
4. Select "CA-Signed" if it is not selected.
5. Click  and select Upload Root Certificate.
6. Select the Root Certificate file.
7. Click  and select Upload Signed Certificate.
8. Select the SSL Certificate file.
9. Enter the password used to generate the CSR/PVK before clicking "Apply".

## 7 ENABLE SSL CERTIFICATE AND ENCRYPTED COMMUNICATION FOR WEB XPANEL

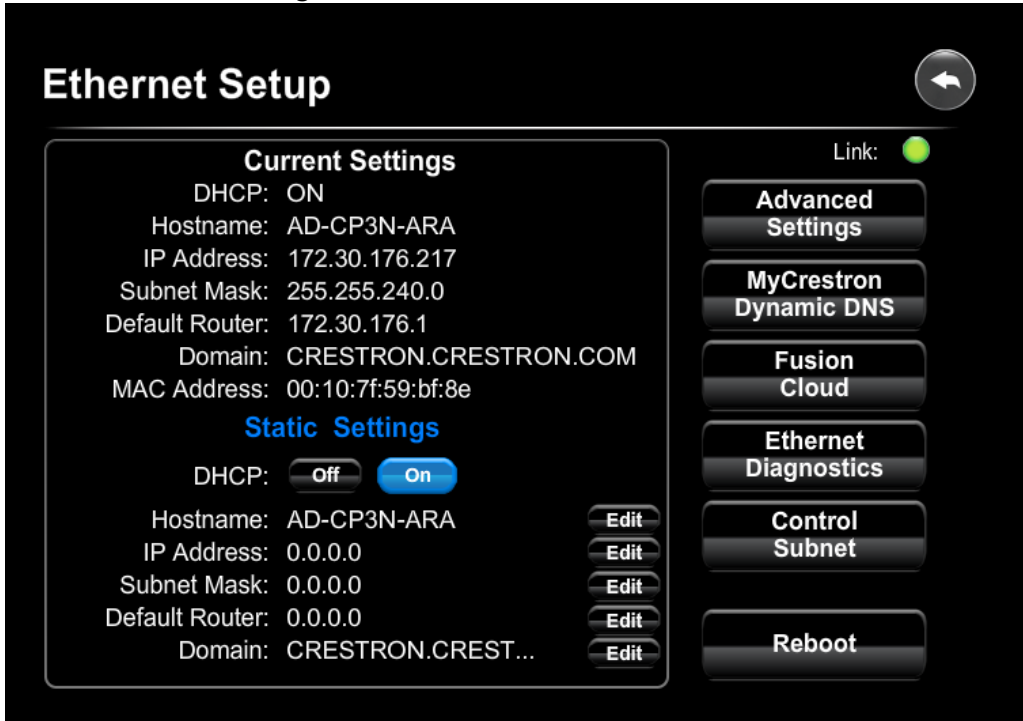
1. Use a web browser and open the control system configuration interface using [http://<control\\_system\\_ip>/setup](http://<control_system_ip>/setup). Click "Setup".



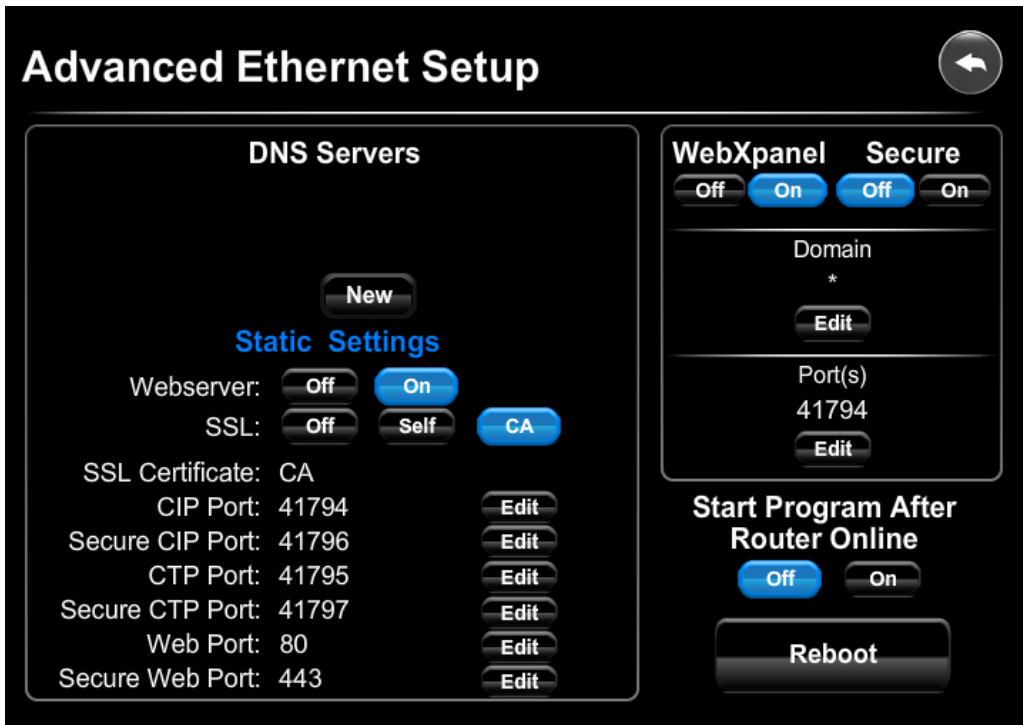
2. Open the Ethernet Setup page by clicking "Ethernet Setup".



3. Click "Advanced Settings".



4. Click SSL "CA".



5. Click "Reboot" to reboot the control system.

6. After the reboot, the control system should now require https to access the web server. The domain name configured for the inside address in **Section: Create Subdomain Records – Step 8** is what should be used.

Use [https://<myinside\\_domain\\_name>/setup](https://<myinside_domain_name>/setup) to open the setup page.

7. Repeat Steps 2 – 3 and click Secure "On". This will enable secure CIP communication (CIPS) for Web Xpanel.

**Important:** This step only secures the Web Xpanel data communication and also allows a secure Crestron App connection. The original CIP port (41794) is still active and available. To secure the entire control system, please review Crestron's Secure Deployment Guide, Answer ID 5571.

8. Click "Reboot" to reboot the control system.

## 8 CONFIGURE PORTS IN ROUTER FIREWALL

In order to securely access a control system from outside the residence, multiple ports need to be opened/forwarded to the control system processor. Please refer to the actual router manual to determine how to forward ports.

The following are ports that need to be forwarded and what they are used for:

Port	Type	Use
41796	TCP	SSL -> Xpanel Exe, Xpanel Web, Crestron App
41797	TCP	SSL -> Toolbox
443	TCP	SSL -> Xpanel Web, Crestron App
843	TCP	Non-SSL, SSL -> Xpanel Web

Note: Since 443 is a standard web ports, some residential routers do not allow these to be forwarded. Also, those ports may already be in-use by the router remote management web interface. In either case, use a different external port, but forward it to 443 on the control system.

I.E. Forward Port 9443 to Port 443 on the control system IP address. Then, to make a secure web page request from outside the residence, the URL is:

[HTTPS://<external\\_subdomain\\_registered>:9443/<myPage.html>](HTTPS://<external_subdomain_registered>:9443/<myPage.html>)

**See Section 10 - Xpanel Web for specific information about using an Xpanel Web project inside and outside the residence.**

For our example domain (advetesting.com) tests, we configured the following port forwarding rules:

External Port 41796 -> Port 41796 on 192.168.1.35

External Port 41797 -> Port 41797 on 192.168.1.35

External Port 9443 -> Port 443 on 192.168.1.35

External Port 843 -> Port 843 on 192.168.1.35



## 9 BASIC SSL TESTING


### 9.1 INTERNAL NETWORK

A simple web test using the internal (inside residence) network, can be used to verify that the SSL certificate is working correctly.

1. Upload a .jpg image to the HTML folder.
2. Open a web browser and enter [HTTPS://<internal\\_subdomain\\_registered>/<image.jpg>](HTTPS://<internal_subdomain_registered>/<image.jpg>)

For our example domain (advetesting.com), we created a DNS record for the subdomain "avinside" with an IP address of 192.168.1.35. An image "spam.jpg" was uploaded to the HTML folder of the control system. Our test URL while connected to the internal network is: <HTTPS://avinside.advetesting.com/spam.jpg>.

After the image loads in the browser, you can verify the SSL certificate.

I.E. In Chrome, simply right-click the green padlock  <https://avinside.advetesting.com/spam.jpg> and select "Details", then "View certificate". For our example domain (advetesting.com), this is what shown:



## 9.2 EXTERNAL NETWORK

Once the internal test has been completed above, an external test can be done to verify the subdomain registered for use outside the residence is working correctly.

1. Assuming the .jpg image previously placed in the HTML folder of the control system is still there.
2. Open a web browser and enter <HTTPS://<external subdomain registered>/<image.jpg>>

For our example domain (advetesting.com), we created a DNS record for the subdomain "avoutside" with a CNAME reference to our control system MyCrestron hostname. An image "spam.jpg" was uploaded to the HTML folder of the control system. Our test URL while connected to a network outside the residence is:

<HTTPS://avoutside.advetesting.com/spam.jpg>.

## 10 CRESTRON APP

Now that everything has been configured and verified, the internal and external subdomains can be used in the connection details of the Crestron App.

Open the Crestron App and edit/create a new connection. Scroll to the bottom of the dialog and slide "Enable SSL" to ON.

Configure the Address 1 connection:

1. Set the "Host name or IP Address" field to the subdomain registered for the internal connection.

For our example domain (advetesting.com), the internal subdomain is "avinside.advetesting.com".

2. The "HTTP Port" and "CIP" fields should be pre-filled with the correct values of 443 and 41796 respectively, since SSL was enabled in the app.

Configure the Address 2 connection:

1. Slide the "Enabled" to ON.
2. Set the "Host name or IP Address" field to the subdomain registered for the external connection.

For our example domain (advetesting.com), the external subdomain is "avoutside.advetesting.com".

3. Set the "HTTP Port" field to the correct value based on the router port configuration set in **Section 7 - Configure Ports in Router Firewall**.

For our example domain (advetesting.com), we configured our router with external port 9443 to forward to 443. So in this field, 9443 was entered.

## 11 XPANEL WEB

Now that everything has been configured and verified, the internal and external subdomains can be used to open an Xpanel Web project.

### 11.1 CONNECTION PROPERTIES

The connection properties of the project need to be modified before it can be used with SSL.

1. Open the project using VTPRO.
2. Select the top node of the project to reveal the project properties.
3. Expand the "Connection Settings" node.
4. Set the "Port" to 41796.
5. Check the "Enable SSL" checkbox.

**Note:** If the "Enable SSL" checkbox is missing from the properties dialog, that parameter will need to be appended to the browser URL as "?enablenessl=1". See below for more details.

### 11.2 CORE3 XPANEL WEB

Before opening the Xpanel Web project, the control system core3 web server needs to be configured for SSL.

1. Using Toolbox -> Text Console, connect to the control system.
2. At the prompt, type "core3xpanelweb" to display the current web server configuration.
3. To configure the server for secure connections, type "core3xpanelweb on \* 41796 secure\_on".

### 11.3 INTERNAL NETWORK

The registered subdomain for the internal network can be used to open the Xpanel Web project.

**Enable SSL Set at Design Time**

URL: [HTTPS://<internal\\_subdomain\\_registered>/core3xpanel.html](HTTPS://<internal_subdomain_registered>/core3xpanel.html)

For our example domain (advetesting.com), the URL is  
[HTTPS://avinside.advetesting.com/core3xpanel.html](https://avinside.advetesting.com/core3xpanel.html)

### **Enable SSL NOT Set at Design Time**

URL: [HTTPS://<internal\\_subdomain\\_registered>/core3xpanel.html?enablesssl=1](https://<internal_subdomain_registered>/core3xpanel.html?enablesssl=1)

For our example domain (advetesting.com), the URL is  
[HTTPS://avinside.advetesting.com/core3xpanel.html?enablesssl=1](https://avinside.advetesting.com/core3xpanel.html?enablesssl=1)

## **11.4 EXTERNAL NETWORK**

The registered subdomain for the external network can be used to open the Xpanel Web project. Unlike the internal network though, the secure web port needs to be specified in the URL, if 443 had to be remapped in **Section 7 - Configure Ports in Router Firewall**.

### **Enable SSL Set at Design Time / 443 Not Remapped**

URL: [HTTPS://<external\\_subdomain\\_registered>/core3xpanel.html](https://<external_subdomain_registered>/core3xpanel.html)

For our example domain (advetesting.com), the URL is:  
[HTTPS://avoutside.advetesting.com/core3xpanel.html](https://avoutside.advetesting.com/core3xpanel.html)

### **Enable SSL Set at Design Time / 443 Is Remapped**

URL: [HTTPS://<external\\_subdomain\\_registered>:external\\_port/core3xpanel.html](https://<external_subdomain_registered>:external_port/core3xpanel.html)

For our example domain (advetesting.com), 443 was remapped to 9443. So the URL is:  
[HTTPS://avoutside.advetesting.com:9443/core3xpanel.html](https://avoutside.advetesting.com:9443/core3xpanel.html)

### **Enable SSL Not Set at Design Time / 443 Not Remapped**

URL: [HTTPS://<external\\_subdomain\\_registered>/core3xpanel.html?enablesssl=1](https://<external_subdomain_registered>/core3xpanel.html?enablesssl=1)

For our example domain (advetesting.com), the URL is:  
[HTTPS://avoutside.advetesting.com/core3xpanel.html?enablesssl=1](https://avoutside.advetesting.com/core3xpanel.html?enablesssl=1)

### **Enable SSL Set at Design Time / 443 Is Remapped**

URL: [HTTPS://<external\\_subdomain\\_registered>:external\\_port/core3xpanel.html?enablesssl=1](https://<external_subdomain_registered>:external_port/core3xpanel.html?enablesssl=1)

For our example domain (advetesting.com), 443 was remapped to 9443. So the URL is:  
[HTTPS://avoutside.advetesting.com:9443/core3xpanel.html?enablesssl=1](https://avoutside.advetesting.com:9443/core3xpanel.html?enablesssl=1)

## 12 APPENDIX

### 12.1 DOMAIN REGISTRAR

The following is a list of domain registrars and common services/pricing

Name	Domain Cost (per Year)	SSL Certificate	Notes
gandi.com	\$15.50 (.com)	\$50 (Multi-Domain)	Account comes with free email.
namecheap.com	\$11 (.com)	\$30 (Multi-Domain)	