ISY994 Series – Network Security Configuration Guide

Requires firmware version 4.5.4+

Requires Java 1.8+

Introduction

Universal Devices, Inc. takes ISY security extremely seriously. As such, all ISY994 Series are equipped with network security features.

	ISY994 PRO Series
TLS/SSL Level	*User selectable:* TLS 1.0 TLS 1.1 TLS 1.2 (default)
Cipher Suites	*User selectable*: Ciphers are offered in the order listed below. **Low Strength:** TLS_RSA_WITH_AES_128_SHA, **Medium Strength:** TLS_RSA_WITH_AES_128_SHA, TLS_RSA_WITH_AES_256_SHA, **High Strength:** TLS_RSA_WITH_AES_128_SHA2 TLS_RSA_WITH_AES_256_SHA2 TLS_RSA_WITH_AES_GCM_128_SHA2 **All (default):** TLS_RSA_WITH_AES_GCM_128_SHA2 TLS_RSA_WITH_AES_256_SHA2 TLS_RSA_WITH_AES_256_SHA TLS_RSA_WITH_AES_128_SHA2 TLS_RSA_WITH_AES_128_SHA
Server Certificates	✓ Self Signed ✓ Signed by a CA ✓ PKCS12 (.pfx) Import (can be used for wildcard certificates)
Client Certificates	✓ Self Signed ✓ Signed by a CA ✓ PKCS12 (.pfx) Import (can be used for wildcard certificates)
Client Authentication	Yes: *User selectable*
Server Authentication	Yes: *User selectable*
Import CA Certs for Authentication	Yes

Table 1. Features

Logging into ISY dashboard

a) If you do not have Java installed, please install the latest for your platform. You may find the latest Java downloads at **http://www.java.com/getjava.** Please choose the latest JRE for your platform.
Note: you need Java 1.8 and above

a) Follow these instructions to install ISY Finder/Launcher app (Figure 1) on your desktop which should be used here on out. Click on your ISY on the list which brings up the launch menu

   a. Click on the **Dashboard** menu item to perform the rest of the setup in this document
   b. In either case, when prompted to authenticate, enter **admin** for both username and password

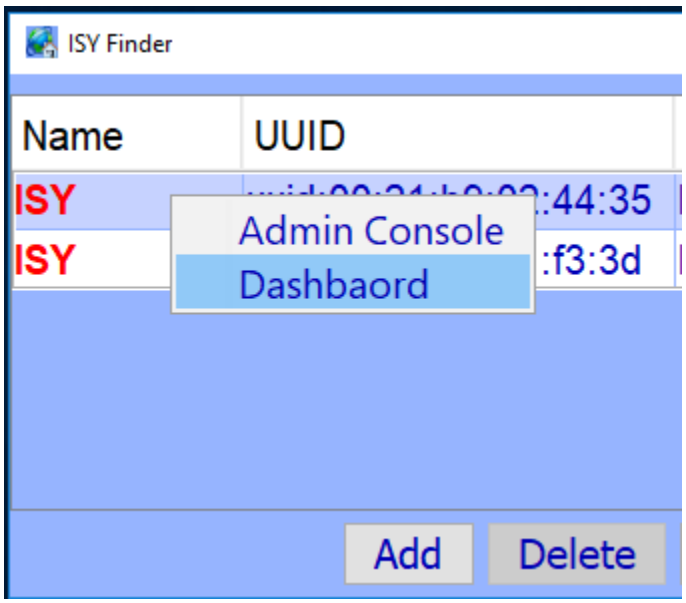
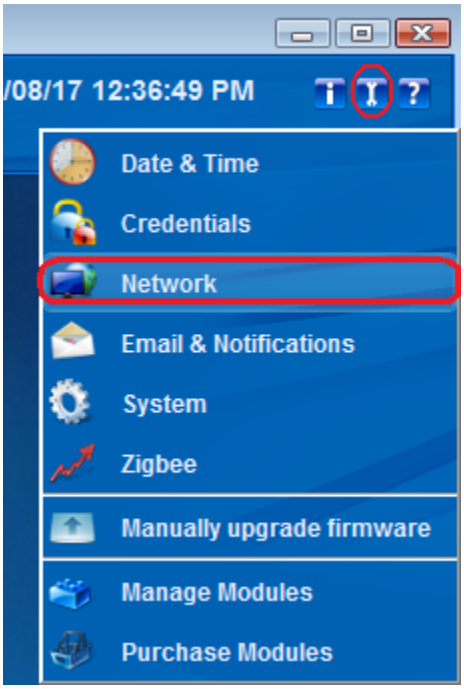
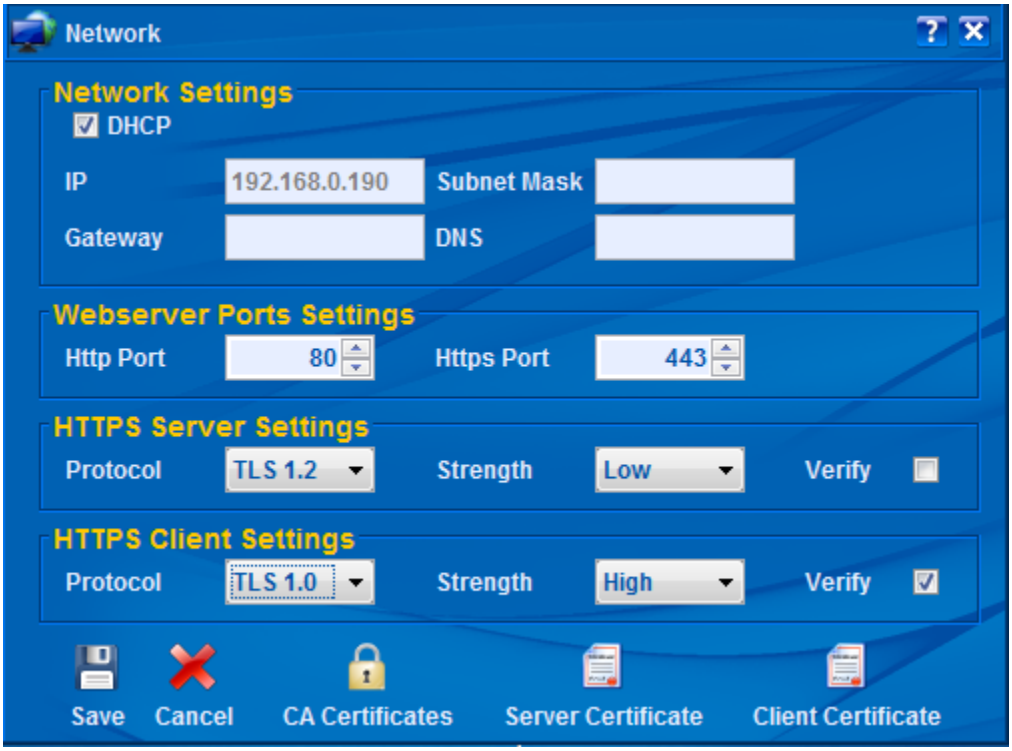


Figure 1 – ISY Finder/Launcher

Configure Network Security





a. Protocol

A maximum protocol level supported by client or server. Please note that if you use TLS 1.2 and if the peer is requesting TLS 1.0, then ISY will downgrade to TLS 1.0.

b. Strength

The symmetric key strengths. Each cipher suites strength has an ordered/priority list of cipher suites that ISY will use to determine its operations. The priority is from high to low (top to bottom):

High:

```
TLS_RSA_WITH_AES_128_SHA2
TLS_RSA_WITH_AES_256_SHA2
TLS_RSA_WITH_AES_GCM_128_SHA2
```

Medium:

```
TLS_RSA_WITH_AES_128_SHA,
TLS_RSA_WITH_AES_256_SHA,
```

Low:

```
TLS_RSA_WITH_AES_128_SHA,
```

All:

```
TLS_RSA_WITH_AES_GCM_128_SHA2,
TLS_RSA_WITH_AES_256_SHA2,
TLS_RSA_WITH_AES_256_SHA,
TLS_RSA_WITH_AES_128_SHA2,
TLS_RSA_WITH_AES_128_SHA,
```

c. Verify

Whether or not client/server authentication should be performed on the peer:

i. The certificate must be valid
ii. The certificate must be signed by a CA (see #d. CA Certificates), through a certificate path, which is known to ISY

Care should be taken when Verify is checked for *Server Settings*. In this case, all clients (including browsers and mobile devices) must provide ISY with a valid certificate. This might not be optimal in normal operations since most browsers/mobile devices do not offer any certificates and thus ISY may ***not*** be reachable over HTTPS.

Care should also be taken when Verify is checked for *Client Settings***.** In this case all communications initiated from ISY to external HTTPS resources shall be validated. This might cause problems with Portals (such as MobiLinc) and Network resources which communicate with devices that do not have valid certificates. This may also interfere with SMTP operations that require TLS.

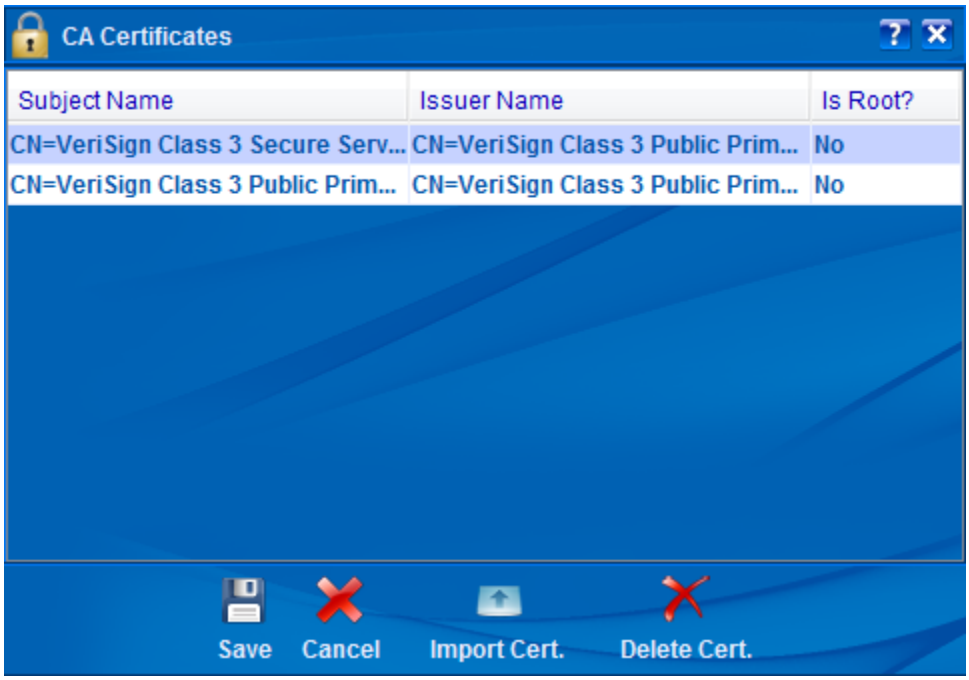
In short – and unless you have explicit requirements, such as OpenADR – then it's best to keep Verify unchecked.

d. CA Certificates

In order for Verify (Client/Server Authentication) to work, you will need to import Certificate Authority signing certificates into ISY.

Please note that if you would like to support a certificate that goes through a chain to reach the root signing certificate, then you ***must*** import all the certificates in the chain and all the way up to the root.

To import CA Certificates, click on the **CA Certificates** button and then click on **Import** to import CA certificates (see below).



You can always use the trusted certificates in your browser to export (in PEM format) and then import into ISY.

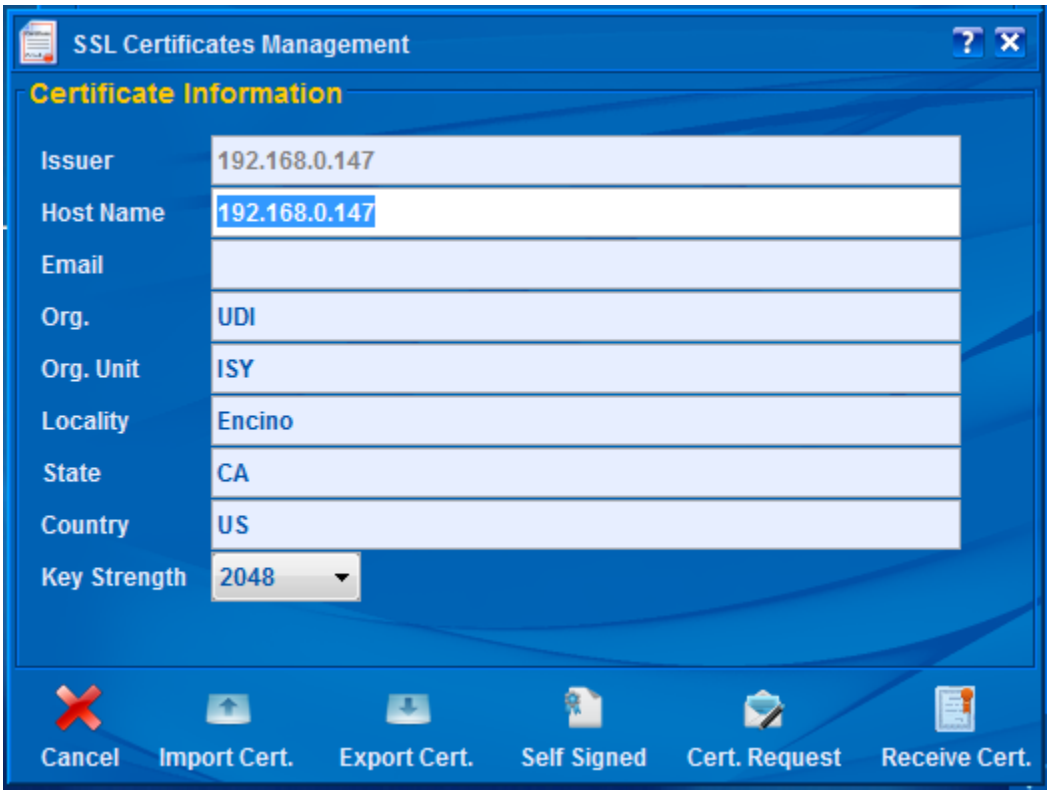
Certificate Management

The operations for Server Certificates and Clients Certificates are identical. As such, in this section only Server Certificates are discussed.

In the Network Dialog (see section 3), click on the Server Certificate. You will be prompted by:

Yes: This will load the certificate store from ISY for which you must have a valid password that you had setup before.

No: This will recreate a new certificate store and overwrites any previous certificate information. The requested password is the password you would like to use to access the store in the future (see Yes).



a. Key Strength

Key Strength is the initial RSA Key Strength which may be 512, 1024, and 2048 bits. The higher the strength, the slower the initial connection with ISY (up to 10 seconds for 2048 bits). Please note that once the initial connection has been established, then this parameter no longer plays a role and communication and cryptographic methods are then based on the strength of the chosen cipher suite's symmetric key.

Note: Although ISY supports 512, 1024, and 2048 bits for self signed certificates, however – and in case of certificate requests – the strength is subject to the approval of the certificate authority. In most cases, the lowest key strength approved by certificate authorities is 2048.

b. Import Cert.

If you have a ***PKCS12 (pfx)*** format file which includes both the Certificate as well as the Private Key, then choose this option to import your certificate/key combination into ISY. You will need to use this feature if you intend to use a preexisting certificate (including wildcard certificates).

Once imported successfully, ISY will reboot for the changes to take effect.

c. Export Cert.

Use this button to export an existing certificate in PEM format. You may want to use this option to import ISY's certificate into a browser's (or other clients') certificate store.

d. Self Signed

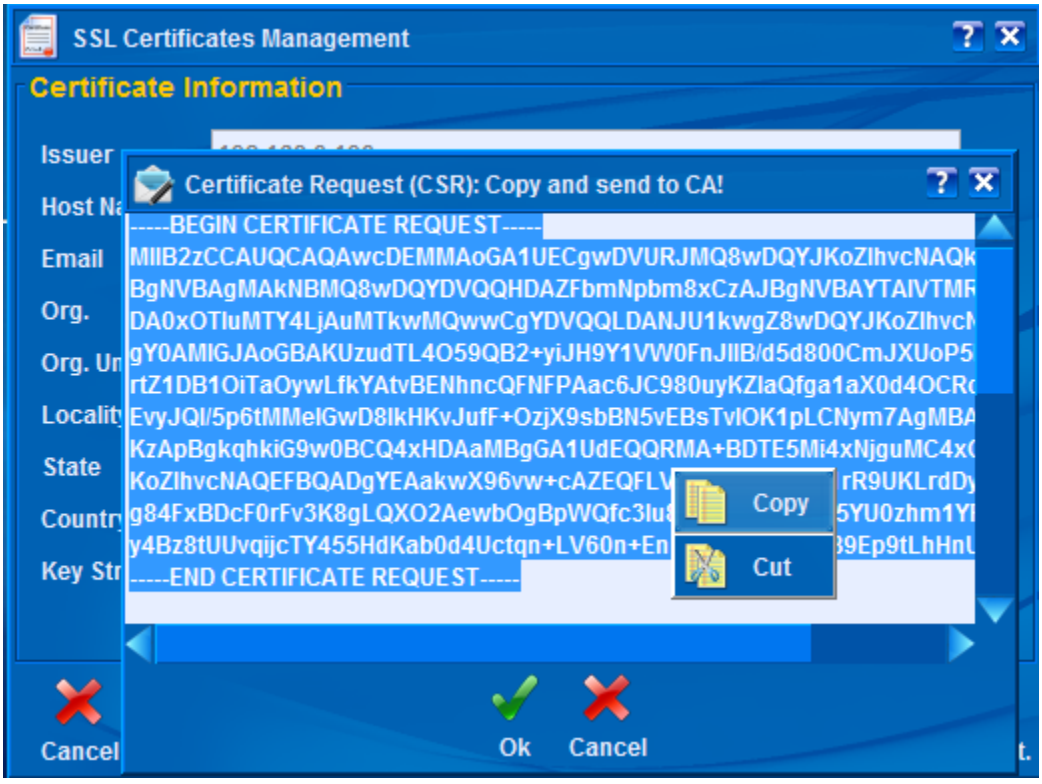
If you wish to create a self signed certificate, make sure to enter and/or update (in case you are working on an existing certificate) all the necessary information in the fields and ***then*** click on the **Self Signed** button.

Once done, ISY will be rebooted for the changes to take effect.

e. Cert. Request

If you wish to have your certificate signed by a CA, you need to create a CSR. To create a CSR, make sure to enter and/or update (in case you are working on an existing certificate) all the necessary information in the fields and ***then*** click on the **Cert. Request** button.

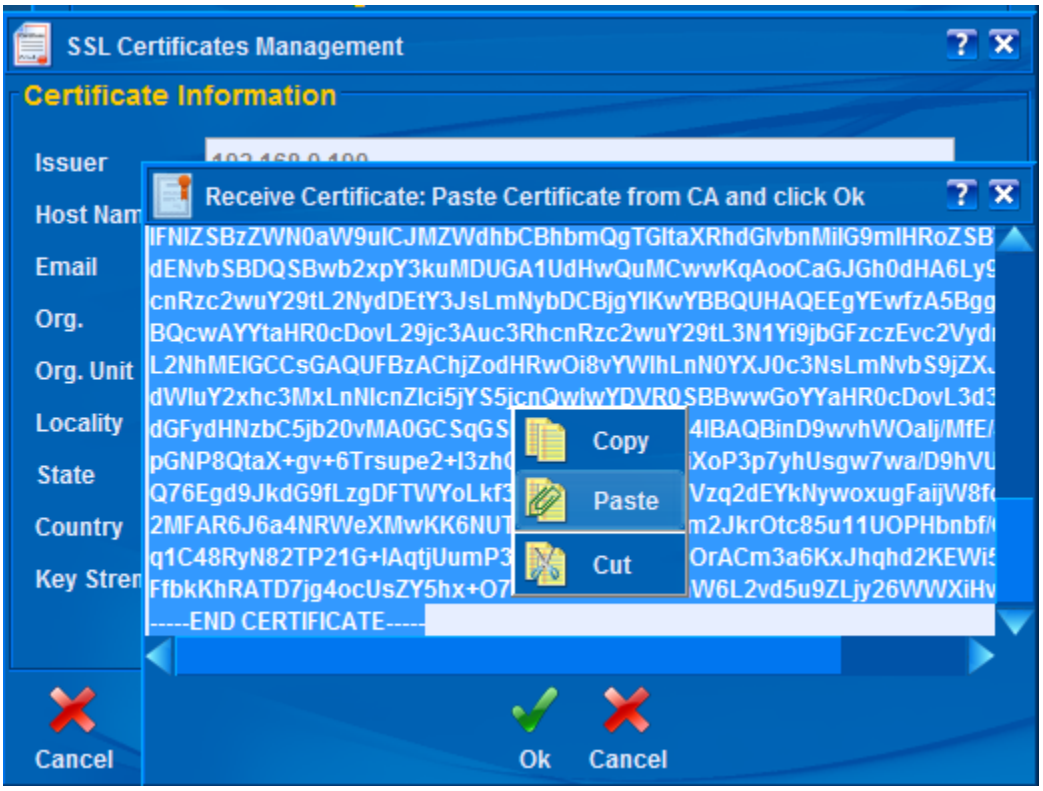
You will be presented with a dialog containing the Certificate Request (see below). Simply right mouse click to copy the contents and then send it to the Certificate Authority.



Make sure to click the ***Save*** button on SSL Certificate Management dialog once done. You may also want to keep a copy of your CSR in case you need to recreate it. This is because ISY creates a new Private Key for every CSR request and thus you will have to start the whole process from scratch in case the original CSR is lost/misplaced.

f. Receive Cert.

If you have already made a Cert Request (#d) and have now been given an actual certificate based on your Cert Request (CSR), then click on the **Receive Cert** button to import the Certificate into ISY. You will be presented with a dialog to paste the certificate into (see below).



Once imported successfully, ISY will reboot for the changes to take effect.