
Multiple Server Certificates

A **server certificate** helps secure network traffic to and from the IVE using elements such as your company name, a copy of your company's public key, the digital signature of the certificate authority (CA) who issued the certificate, a serial number, and expiration date.

When receiving encrypted data from the IVE, the client's browser first checks whether the IVE's certificate is valid and whether the user trusts the CA that issued the IVE's certificate. If the user has not already indicated that he trusts the IVE's certificate issuer, the Web browser prompts the user to accept or install the IVE's certificate.

When you initialize the IVE, it locally creates a temporary self-signed digital certificate that enables users to immediately begin using your IVE¹. If you do not want to use the IVE's self-signed certificate, however, you may import a digital server certificate file and its corresponding private key to the IVE. For more information, see "Configuring the Certificates > Server Certificate tab" on page 4. If you have an advanced license, you may import multiple server certificates into the IVE.

When using multiple server certificates, each certificate handles validation for a separate domain and may be issued by a different CA. You can use multiple root certificates in conjunction with the following features:

- **Multiple sign-in URLs**

With the multiple sign-in URLs feature, you can provide access to the IVE from multiple hostnames by creating a different sign-in URL for each hostname (domain). Then, you can create separate sign-in pages and authentication requirements for each sign-in URL. With the multiple server certificates feature, you can use different certificates to validate users signing into each of those domains. For example, you can associate one certificate with the `partners.yourcompany.com` domain and another with the `employees.yourcompany.com` domain.

- **Pass-through proxy**

With the pass-through proxy feature, you can intermediate traffic to Web-based applications through an IVE port or virtual hostname. If you choose the latter option, you can use the multiple server certificates feature to validate users who are accessing the various Web applications through different hostnames.

1. The encryption for the self-signed certificate created during initialization is perfectly safe, but users are prompted with a security alert each time they sign in to the IVE because the certificate is not issued by a trusted certificate authority (CA). For production purposes, we recommend that you obtain a digital certificate from a trusted CA.

To enable multiple server certificates, you must:

1. Specify the IP addresses from which users may access the IVE and then create a virtual port for each. A **virtual port** activates an IP alias on a physical port. To create virtual ports for:
 - **Internal users**
Use settings in the **System > Network > Internal Port > Virtual Port** tab to create virtual ports for users such as employees who are signing into the IVE from inside your internal network (page 2).
 - **External users**
Use settings in the **System > Network > External Port > Virtual Port** tab to create virtual ports for users such as customers and partners who are signing into the IVE from outside of your internal network (page 3).
2. Upload your server certificates to the IVE using settings in the **System > Configuration > Certificates > Server Certificates** tab. Upload one server certificate for each domain (hostname) that you want to host on the IVE (page 4).
3. Specify which virtual ports the IVE should associate with the certificates using settings in the **System > Configuration > Certificates > Server Certificates** tab. When a user tries to sign into the IVE using the IP address defined in a virtual port, the IVE uses the certificate associated with the virtual port to initiate the SSL transaction (page 4).

Configuring the Internal Port > Virtual Ports tab

Create virtual ports on the internal interface

Use settings in this tab to create virtual ports for users such as employees who are signing into the IVE from inside your internal network. A **virtual port** activates an IP alias on a physical port and shares all of the network settings (except IP address) with the internal or external port that hosts the virtual port. An **IP alias** is an IP address that is bound to a virtual port. (Note that an IP alias is different from the IVE's primary IP address, which is a required IVE setting that you configure during the IVE initialization process.) You can use virtual ports in conjunction with the multiple server certificates feature to provide users access to the same IVE through different IP aliases (page 4).

For example, you may choose to create two virtual ports on a single appliance, mapping the first virtual port to the IP address 10.10.10.1 (sales.yourcompany.com) and the second virtual port to the IP address 10.10.10.2 (partners.yourcompany.com). Then, you can associate each of

these virtual ports with their own certificate, ensuring that the IVE authenticates different users through different certificates.

When configuring virtual ports on a clustered IVE, note that all nodes in the cluster share some virtual port information. In an active/active cluster or multi-site cluster, the virtual port names are the same across the cluster, but the IP aliases defined in the virtual ports vary from node to node. In an active/passive cluster, the virtual port names and IP aliases are both shared across the cluster. (Within an active/passive cluster, when the second node takes over a cluster, it inherits the first node's IP alias and activates them on the second node.)

To create a virtual port:

1. In the Web console, choose **System > Network > Internal Port > Virtual Ports**.
2. Click **New Port**.
3. Enter a unique name for the virtual port.
4. Enter a unique IP alias to associate with the virtual port—do not use an IP address that is already associated with another virtual port. Note that if you do not enter an IP address, the IVE does not activate the virtual port.
5. Click **Save Changes**.
6. Use settings in the **System > Configuration > Certificates > Server Certificates** tab to associate the virtual port with a server certificate (page 4).

Configuring the External Port > Virtual Ports tab

Create virtual ports on the external port

Use settings in this tab to create virtual ports for users such as customers and partners who are signing into the IVE from outside of your internal network, as explained in "Configuring the Internal Port > Virtual Ports tab" on page 2.

To create a virtual port:

1. In the Web console, choose **System > Network > External Port > Virtual Ports**.
2. Click **New Port**.
3. Enter a unique name for the virtual port.

4. Enter a unique IP alias to associate with the virtual port—do not use an IP address that is already associated with another virtual port. Note that if you do not enter an IP address, the IVE does not activate the virtual port.
5. Click **Save Changes**.
6. Use settings in the **System > Configuration > Certificates > Server Certificates** tab to associate the virtual port with a server certificate (page 4).

Configuring the Certificates > Server Certificate tab

Use settings in the **System > Configuration > Certificates > Server Certificate** tab associate a certificate with a virtual port.

Associate a certificate with a virtual port

If you choose to associate multiple hostnames with a single IVE, you must specify which certificates the IVE should use to validate users signing in to the different hostnames. Options include:

- **Associate all hostnames with a single wildcard certificate**

With this method, you use a single wildcard certificate to validate all users, regardless of which hostname they use to sign into the IVE. A **wildcard certificate** includes a variable element in the domain name, making it possible for users signing in from multiple hosts to map to the “same” domain. For example, if you create a wildcard certificate for *.yourcompany.com, the IVE uses the same certificate to authenticate users who sign into employees.yourcompany.com as it does to authenticate users who sign into partners.yourcompany.com.

- **Associate each hostname with its own certificate**

With this method, you associate different hostnames with different certificates. Since the IVE does not know the user’s hostname when he signs into the IVE, however, you must create a virtual port for each hostname and then associate your certificates with the virtual ports. A **virtual port** activates an IP alias on a physical port. For example, you may choose to create two virtual ports on a single appliance, mapping the first virtual port to the IP address 10.10.10.1 (sales.yourcompany.com) and the second virtual port to the IP address 10.10.10.2 (partners.yourcompany.com). Then, you can associate each of these virtual ports with their own certificate, ensuring that the IVE authenticates different users through different certificates.

To associate different certificates with different virtual ports:

1. In the Web console, navigate to the **System > Network > Internal Port** tab (page 2) or **External Port** tab (page 3). Then, create your virtual ports using settings in the **Virtual Ports** page.
2. Navigate to **System > Configuration > Certificates > Server Certificates** and import the server certificates that you want to use to validate user certificates (page 4).
3. Click the link that corresponds to a certificate that you want to use to validate user certificates.
4. Under **Present certificate on these ports**, specify the port(s) that the IVE should associate with the certificate—you can choose internal or external ports and primary or virtual ports, but you cannot choose a port that is already associated with another certificate.
5. Click **Save Changes**.
6. Repeat steps 3-6 for each of the certificates that you want to use to authenticate users.