



Adding Certificates and Modifying ESX Server Web Proxy Settings

In adding certificates for ESX Server and thinking about encryption and user security, be aware of the following:

- ESX Server doesn't handle pass phrases, also known as encrypted keys. If you set up a pass phrase, ESX Server processes will be unable to start correctly, so avoid setting up certificates using pass phrases.
 - You can configure the Web proxy so that it searches for certificates in a location other than the default location. This capability proves useful for companies that prefer to centralize their certificates on a single machine so the certificates can be used by multiple hosts.
- Caution** If you store certificates in a location other than the ESX Server host, you will be unable to use the certificates if the host loses network connectivity with the machine storing the certificates.
- To support encryption for user names, passwords, and packets, SSL is enabled by default for VI Web Access and Web SDK connections. If you want to configure these connections so that they don't encrypt transmissions, disable SSL for your VI Web Access connection or Web SDK connection by switching the connection from HTTP to HTTPS as described in [To change security settings for a Web proxy service](#). Consider disabling SSL only if you have created a fully trusted environment for these clients, meaning that firewalls are in place and transmissions to and from the host are fully isolated. Disabling SSL can improve performance for VI Web Access because you avoid the overhead required to perform encryption.
 - To protect against misuse of ESX Server services such as the internal Web server that hosts VI Web Access, most internal ESX Server services are accessible only through port 443, the port used for HTTPS transmission. Port 443 acts as a reverse proxy for ESX Server. You can see a list of services on ESX Server through an HTTP welcome page, but you can't directly access these services without proper authorization. You can change this configuration so that individual services are directly accessible through HTTP connections. VMware recommends that you not make this change unless you are using ESX Server in a fully trusted environment.
 - When you upgrade VirtualCenter and VI Web Access, the certificate remains in place. If you remove VirtualCenter and VI Web Access, the certificate directory is not removed from the service console.

To configure the Web proxy to search for certificates in nondefault locations

- 1 Log on to the service console as the root user.
- 2 Change directories to /etc/vmware/hostd/.
- 3 Use nano or another text editor to open the config.xml file and find the following XML segment:

```
<ssl>
  <!-- The server private key file -->
  <privateKey>/etc/vmware/ssl/rui.key</privateKey>
  <!-- The server side certificate file -->
  <certificate>/etc/vmware/ssl/rui.crt</certificate>
</ssl>
```

- 4 Replace /etc/vmware/ssl/rui.key with the absolute path to the private key file that you received from your trusted certificate authority.

This path can be on the ESX Server host or on a centralized machine on which you store certificates and keys for your company.

Note Leave the <privateKey> and </privateKey> XML tags in place.

- 5 Replace /etc/vmware/ssl/rui.crt with the absolute path to the certificate file that you received from your trusted certificate authority.

Caution Do not delete the original rui.key and rui.crt files. These files are used by the ESX Server host.

- 6 Save your changes and close the file.
- 7 Enter the following command to restart the vmware-hostd process:

```
service mgmt-vmware restart
```

To change security settings for a Web proxy service

- 1 Log on to the service console as the root user.
- 2 Change directories to /etc/vmware/hostd/.
- 3 Use nano or another text editor to open the config.xml file and find the following XML segment:

```
<proxysvc>
  <path>/usr/lib/vmware/hostd/libproxysvc.so</path>
  <http>
    <port>80</port>
    <proxyDatabase>
      <server id="0">
        <namespace> / </namespace>
        <host> localhost </host>
        <port> 9080 </port>
      </server>
      <redirect id="0"> /ui </redirect>
      <redirect id="1"> /mob </redirect>
      <redirect id="2"> /sdk </redirect>
    </proxyDatabase>
  </http>
  <https>
    <port>443</port>
    <proxyDatabase>
      <server id="0">
        <namespace> / </namespace>
        <host> localhost </host>
        <port> 9080 </port>
      </server>
      <server id="1">
        <namespace> /sdk </namespace>
        <host> localhost </host>
        <port> 8085 </port>
      </server>
      <server id="2">
        <namespace> /ui </namespace>
        <host> localhost </host>
        <port> 8080 </port>
      </server>
      <server id="3">
        <namespace>/mob</namespace>
        <host>localhost</host>
        <port>8087</port>
      </server>
    </proxyDatabase>
  </https>
</proxysvc>
```

- 4 For every HTTPS service that you want to access using HTTP, move the following segment up to the HTTP area:

```
<server id="id_number">
  <namespace> service_domain </namespace>
  <host> localhost </host>
  <port> port_number </port>
</server>
```

Where:

- *id_number* is an ID number for the server ID XML tag. ID numbers must be unique within the HTTP area.
- *service_domain* is the name of the service you are moving, for example /sdk or /mob.
- *port_number* is the port number assigned to the service. You can assign a different port number to the service.

- 5 In the HTTP section, remove the redirect statement for the service you are moving.
- 6 Save your changes and close the file.
- 7 Enter the following command to restart the vmware-hostd process:

```
service mgmt-vmware restart
```

To move an HTTP service to the HTTPS section, use the same procedure but add a redirect statement to the HTTP section after you move the service. Place the new redirect statement after the other redirect statements and use a unique number as the ID number for the redirect tag.

Example: Setting up VI Web Access to communicate through an insecure port

VI Web Access normally communicates with an ESX Server host through a secure port (HTTPS, 443). If you are in a fully trusted environment, you might decide that you can use an insecure port (for example, HTTP, 80). To do so, change the proxy services area of the `/etc/vmware/hostd/config.xml` file as described in the procedure. The result is as follows, with changed and moved areas shown in bold. Note that the server segment for `/ui` (the VI Web Access service) is moved to the HTTP section and the redirect statement for `/ui` has been removed.

```
<proxysvc>
  <path>/usr/lib/vmware/hostd/libproxysvc.so</path>
  <http>
    <port>80</port>
    <proxyDatabase>
      <server id="0">
        <namespace> / </namespace>
        <host> localhost </host>
        <port> 9080 </port>
      </server>
      <server id="1">
        <namespace> /ui </namespace>
        <host> localhost </host>
        <port> 8080 </port>
      </server>
      <redirect id="0"> /mob </redirect>
      <redirect id="1"> /sdk </redirect>
    </proxyDatabase>
  </http>
  <https>
    <port>443</port>
    <proxyDatabase>
      <server id="0">
        <namespace> / </namespace>
        <host> localhost </host>
        <port> 9080 </port>
      </server>
      <server id="1">
        <namespace> /sdk </namespace>
        <host> localhost </host>
        <port> 8085 </port>
      </server>
      <server id="2">
        <namespace> /mob</namespace>
        <host>localhost</host>
        <port>8087</port>
      </server>
    </proxyDatabase>
  </https>
</proxysvc>
```