



# NETSHIELD Custom Certificates

## Overview

The self-signed certificates that ship with NETSHIELD will allow you to set up your appliance, but give security warnings in modern browsers. These security warnings may also affect your ability to use the NetSHIELD Command Center. To fix these issues, you can create trusted certificates for all your appliances.

**IMPORTANT:** Ensure all your appliances are updated to the latest patch before proceeding.

## Certificate Manager

Certificate Status			
Issuer Name	10.10.5.114/emailAddress=support@nets	Common Name	10.10.5.114/emailAddress=support@nets
	hieldcorp.com		hieldcorp.com
Issuer Organizational Unit	NETSHIELD	Subject Alternative Name	
Issuer Organization	NETSHIELD	Valid From	Sep 7 13:21:34 2018 GMT
Issuer Locality	Nashua	Valid To	Sep 2 13:21:34 2038 GMT
Issuer State/Province	NH		
Issuer Country	US		

### Appliance Certificate

Before generating the appliance certificate, you must import your root certificate into each browser that will access the appliance. If you don't have a root certificate, use the form below to generate one.

To generate the appliance certificate, you must provide a root certificate in PEM format. Upload or paste the private key into the left box, and the certificate into the right box. Press the Generate button when ready. **You may have to refresh or restart your browser to pick up the new certificate.**

Private Key <input type="button" value="Browse..."/> No file selected.	Certificate <input type="button" value="Browse..."/> No file selected.
<div style="border: 1px solid #ccc; height: 100px;"></div>	<div style="border: 1px solid #ccc; height: 100px;"></div>
<input type="button" value="Generate"/>	

### Root Certificate

If your organization does not already have a root certificate, you can generate one here. Note that only one certificate should be generated! You will import this certificate into every browser that is going to access the NETSHIELD user interface.

To generate the root certificate, enter your organization and site information into the blanks below and click the Generate button. To import the certificate into your browser, follow the instructions provided by NETSHIELD support or by your browser software support.

Common Name	<input type="text"/>	Organizational Unit	<input type="text"/>
Organization	<input type="text"/>	Locality	<input type="text"/>
State/Province	<input type="text"/>	Country	<input type="text"/>
<input type="button" value="Generate"/>			



## Create the Root Certificate

If your organization does not already have a root certificate, you can generate one here. Note that only one certificate should be generated! You will import this certificate into every browser that is going to access the NETSHIELD user interface.

To generate the root certificate, enter your organization and site information into the blanks below and click the Generate button.

Root Certificate			
If your organization does not already have a root certificate, you can generate one here. Note that only one certificate should be generated! You will import this certificate into every browser that is going to access the NETSHIELD user interface.			
To generate the root certificate, enter your organization and site information into the blanks below and click the Generate button. To import the certificate into your browser, follow the instructions provided by NETSHIELD support or by your browser software support.			
Common Name	<input type="text" value="Test"/>	Organizational Unit	<input type="text" value="Division"/>
Organization	<input type="text" value="Company"/>	Locality	<input type="text" value="Nashua"/>
State/Province	<input type="text" value="NH"/>	Country	<input type="text" value="US"/>
<input type="button" value="Generate"/>			

This will generate two files – rootCA.pem and rootCA.key. Save and store both of these files in a secure location. To import the certificate into your browser, follow the instructions provided in the last section or by your browser software support.

## Create the Appliance Certificate

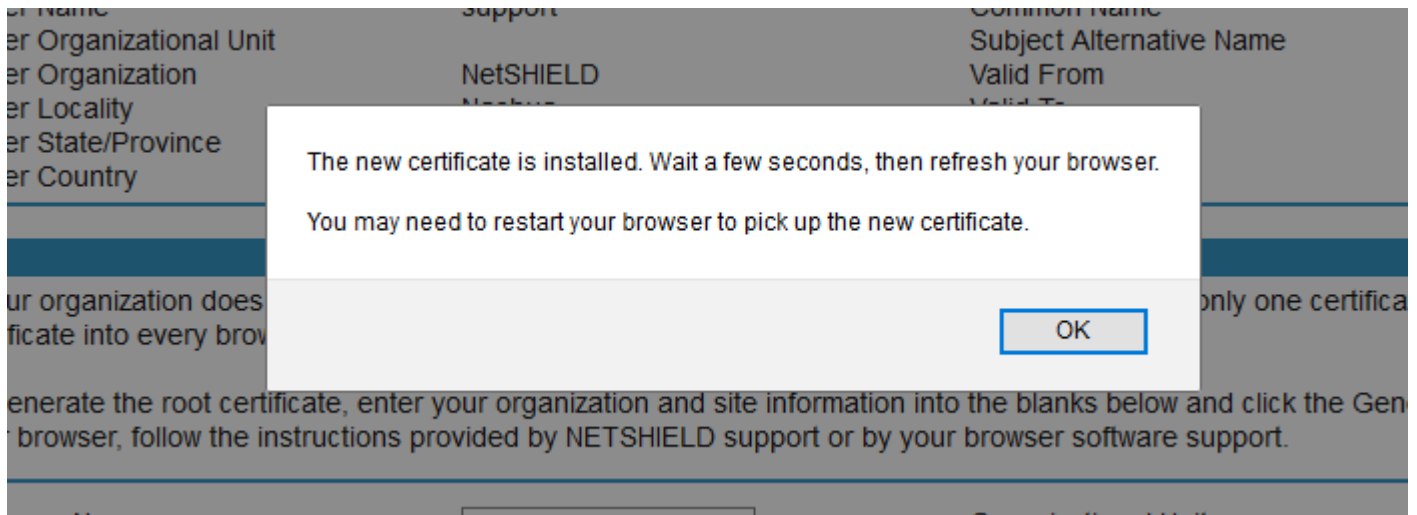
To generate the appliance certificate, you must provide a root certificate in PEM format. Upload or paste the private key (Ex. rootCA.pem) into the left box, and the certificate (Ex. rootCA.key) into the right box.

Press the Generate button when ready.

Appliance Certificate	
To generate the appliance certificate, you must provide a root certificate in PEM format. Upload or paste the private key into the left box, and the certificate into the right box. Press the Generate button when ready.	
Private Key <input type="button" value="Browse..."/> rootCA.key	Certificate <input type="button" value="Browse..."/> rootCA.pem
<pre>-----BEGIN RSA PRIVATE KEY----- MIIEowIBAAKCAQEAlqM28IvSbOdVdY5p0f1CDyAn089xZNUMztyvngHtU+NhodIp iFmxYPMqLzIwYCbE1dAjJOebDEmlDUC3PHXGFqqo16x//xFrQpknzM0fmI3yrOk6 OMr2iK8mCEPcF8cLTNq5DBnlG62JmaQHDJyKKCsRcvHHx17yA89P0Qzik+g18SpB 7QptN2nWenWU3RYfDiF/9yX4QBaK1ZSMsTrt84oDDWR/WJyaacSEmstGqrlJQ1W WRjRp9HAD2msaXNzeF+Jmj9x2bmu5k/GIMYengpNsqtgg1v4g7Pm1K8WXXr2nZz9 YoaFh+Xkrzmz3NuwhwiXCLb0YvvpwWMQpdtT8s9QIDAQABAoIBAHE47jNxnNFsM1yv 1TQjgkJyLd1TP2zFgeH+F/SX21VCRADoQRvELSeavZ1LWpIksG/VCIVVm8FpnShP 6yoDb8dbsJqi6nXiNteQ3ExgJQ56KtvyVTOYwiLMWu69arFoh0LRBKvmz7hIdqc -----</pre>	<pre>-----BEGIN CERTIFICATE----- MIIDkTCCAnmgAwIBAgIJAMwrW17ItKkMMA0GCSqGSIb3DQEBCwUAMF8xDTALBgNV BAMBFRL1c3QxEtAPBgNVBAsMCERpdm1zaW9uMRAwDgYDVQKDAgDb21wYW55SMQ8w DQYDVQQHDAZOYXN0dWEwCzAJBgNVBAGMAk5IMQswCQYDVQGEwJVUzAeFw0xODA4 MDgyMDI4MjhaFw0yODA4MDUyMDI4MjhaMF8xDTALBgNVBAMBFRL1c3QxEtAPBgNV BAsMCERpdm1zaW9uMRAwDgYDVQKDAgDb21wYW55SMQ8wDQYDVQQHDAZOYXN0dWEw CzAJBgNVBAGMAk5IMQswCQYDVQGEwJVUzCCAS1wDQYJKoZIhvcNAQEBBQADggEP ADCCAQoCggEBAJajNvCL0mznVXWoadH9Qg8gJ9PpcWIVDM7cx5xh7VPjYaH5KvZz sWDzKi801mEmxNXQIyTnmwxJpQ1Atzx1xhaqqNesf/8Ra0KZJ8zNH5iN8qzpOjjK -----</pre>
<input type="button" value="Generate"/>	



You will receive a message that the certificate is installed.



## Install the Root Certificate

The root certificate (rootCA.pem) must be imported into every browser that will access the appliance. The procedure for doing this differs for every browser (and across operating systems).

### Google Chrome

Click the menu button at the top right, then Settings. Go to Show Advanced Settings, Manage Certificates. On Windows, click the Trusted Root Certification Authorities tab. On Linux, click the Authorities tab. Click the Import... button and select the rootCA.pem file you created in the previous step. Exit the dialog and restart the browser.

### Mozilla Firefox

Click the menu button at the top right, then Preferences. Go to Advanced, then Certificates, then the View Certificates button. On Windows, click the Trusted Root Certification Authorities tab. On Linux, click the Authorities tab. Click the Import... button, and select the rootCA.pem file you created in the previous step. Exit the dialog and restart the browser.



## Other Browsers

Enter the Settings (or Preferences) area in your browser. Find a button marked something like Manage Certificates. It may be accessible via an advanced tab or dialog. Click the button to get the lists of which certificates are currently installed on your browser or workstation. Find a tab or area marked Authorities or Certificate Authorities, click it, and look for a button marked Import or Install. Click it and select the 'rootCA.pem' file you created in the previous step. Get out of the certificates dialog, and restart the browser.

For additional support, please refer to your browser's documentation or support information.