



# Deployment Guide

VeriSign Certificate Authority

Citrix NetScaler SSL





Notice:

The information in this publication is subject to change without notice.

THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. CITRIX SYSTEMS, INC. ("CITRIX"), SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR DIRECT, INCIDENTAL, CONSEQUENTIAL OR ANY OTHER DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS PUBLICATION, EVEN IF CITRIX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

This publication contains information protected by copyright. Except for internal distribution, no part of this publication may be photocopied or reproduced in any form without prior written consent from Citrix.

The exclusive warranty for Citrix products, if any, is stated in the product documentation accompanying such products. Citrix does not warrant products other than its own.

Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Copyright © 2008 Citrix Systems, Inc., 851 West Cypress Creek Road, Ft. Lauderdale, Florida 33309-2009 U.S.A. All rights reserved.

# Table of Contents

Introduction .....	4
Solution Requirements.....	5
Prerequisites.....	5
Network Diagram .....	6
Obtaining a Certificate from a Certificate Authority .....	7
Creating a Private Key - NetScaler .....	7
Create a Certificate Signing Request - NetScaler .....	8
Submit CSR to Certificate Authority - VeriSign .....	9
Receive Certificate from Certificate Authority - VeriSign .....	12
Obtain Root CA & Intermediate CA Certificates.....	13
Obtain Root CA and Intermediate Root CA Certificates from Certificate Authority - VeriSign.....	13
Installing Server (NetScaler) Certificates .....	15
Installing Server Certificate From Certificate Authority - NetScaler .....	15
Installing Intermediate CA Certificate - NetScaler .....	16
Linking VeriSign Intermediate CA Certificate to NetScaler Signed Certificate - NetScaler.....	17
Importing Client (Browser) Certificates .....	18
Importing VeriSign Trial Root CA Cert and Trial Int CA Cert into Client browser - Browser.....	18
Verifying Certificate Chain in Client browser - Browser .....	19
Citrix NetScaler SSL Offload Configuration .....	20
SSL Offload Configuration - NetScaler .....	20
Testing the Client to NetScaler Certificate Chain .....	22
Testing the VeriSign SSL Certificate Chain between Client and NetScaler - VeriSign.....	22

# Introduction

Citrix® NetScaler® optimizes the delivery of web applications — increasing security and improving performance and Web server capacity. Processing secure SSL transactions can consume a large portion of a Web server's CPU capacity, degrading performance and increasing end-user response times.

A NetScaler configured with SSL acceleration is placed in front of a Web server, where it intercepts SSL transactions on behalf of the server, processes the SSL transactions, applies the NetScalers load balancing and content switching policies, then relays the transactions to the servers.

To configure SSL, you must first create an SSL virtual server and services on the NetScaler. Then, you must bind a valid SSL certificate and the configured services to the SSL virtual server.

An SSL certificate is an integral element of the SSL encryption and decryption process. The certificate is used during SSL handshaking to determine the cipher that will be used for SSL processing, and also to establish the identity of the SSL server, in this case the NetScaler, as the NetScaler will be acting as the SSL termination point for the clients.

You can create your own SSL certificate on the NetScaler for proof of concept, however, it is recommended that you obtain a valid SSL certificate that has been issued by a trusted certificate authority for production environments. VeriSign is an example of a trusted certificate authority.

The Citrix NetScaler supports chaining of Certificates, and the use of Intermediate CA certificates. As of the time of the writing of this guide, VeriSign released a statement that all VeriSign SSL Certificates issued after December 11, 2008 will be chained to offline Certificate Authority (CA) roots to align with security best practices. Chained certificates are preferred because offline CA storage provides greater protection of the root's key pair from attacks, and Intermediate Root CAs can be maintained for each unique product and updated without disruption to the customer.

VeriSign, along with other Certificate Authorities, provide Trial Root CA and Trial Intermediate Root CA Certificates for use with the Trial Certificates that they issue. As of April 2006, all SSL certificates issued by VeriSign require the installation of an Intermediate CA Certificate. The SSL certificates are signed by an Intermediate CA using a two-tier hierarchy (also known as a Trust Chain) which enhances the security of your SSL Certificate. If the proper Intermediate CA is not installed on the NetScaler, your customers will see browser errors and may choose not to proceed further and close their browser.

The NetScaler Server Certificate (Signed by VeriSign) must be sent to the Client Browser along with the Trusted Certificate Authority Intermediate CA Certificate (Linked) in order for the SSL handshake to proceed successfully. Otherwise, the browser terminates the SSL session ~or~ presents a warning message to the client, after it fails to authenticate the NetScaler Server Certificate.

You must create a chain of certificates that will be sent to the client during the SSL handshake. This chain links the server certificate to its issuer (the intermediate CA). In order for this to work, the intermediate CA certificate file must already be installed in the NetScaler.

In this deployment guide we describe how to obtain a valid SSL certificate (a 14 day Trial certificate) from VeriSign, a public trusted certificate authority (CA) and install it on the NetScaler for use with the SSL functions of the NetScaler.

# Solution Requirements

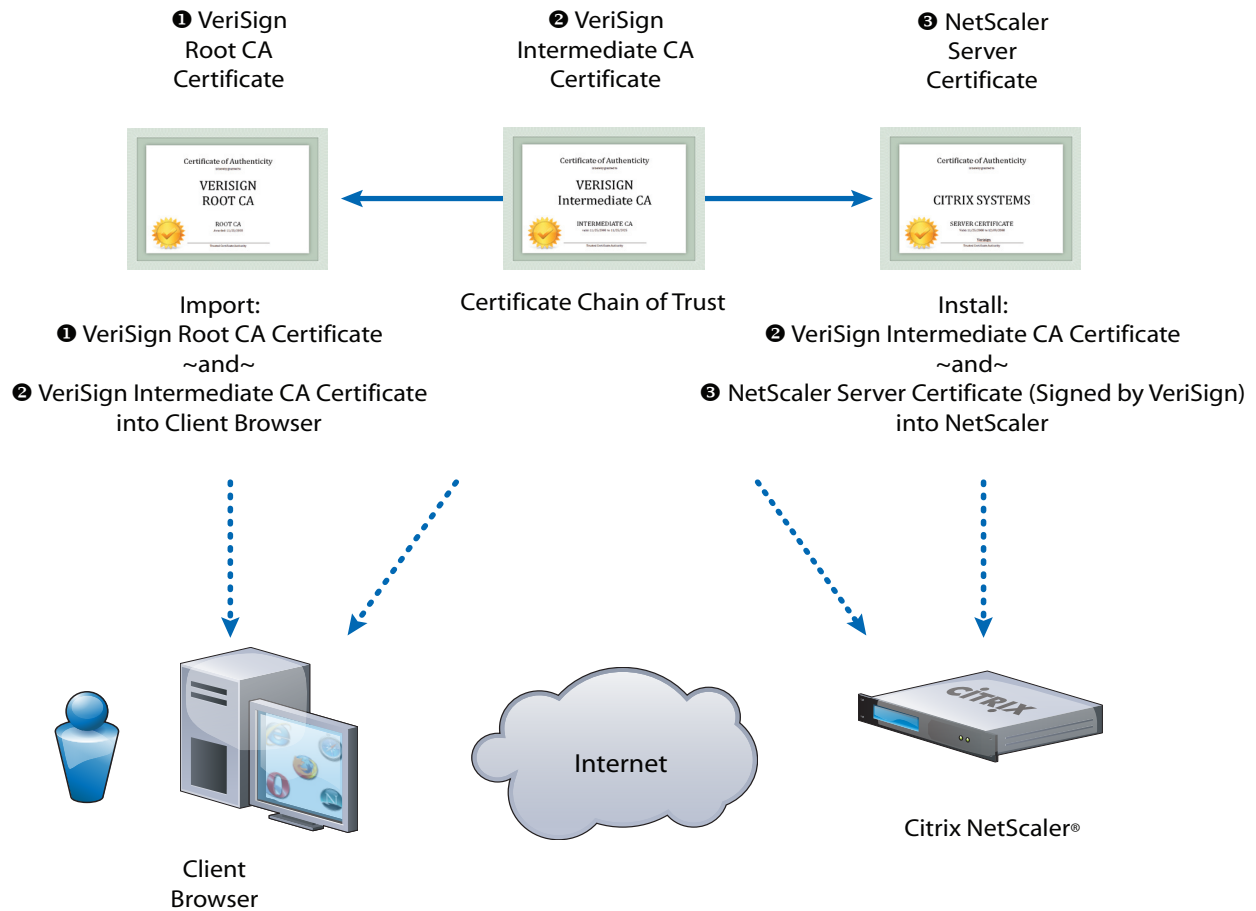
- NetScaler Application Switch - SSL Offload
- Public Trusted Certificate Authority Issued Certificates

## Prerequisites

- Citrix NetScaler L4/7 Application Switch, running version 9.0+ (Quantity x 2 for HA)
- NetScaler Server SSL Certificate (Signed by VeriSign)
- VeriSign Trial Root CA SSL Certificate
- VeriSign Trial Intermediate CA SSL Certificate
- Client laptop/workstation running Internet Explorer 6.0+, Ethernet port
- 9-pin serial cable -or- USB-to-serial cable

# Network Diagram

The following is the Network that was used to develop this deployment guide.



# Obtaining a Certificate from a Certificate Authority

## Creating a Private Key - NetScaler

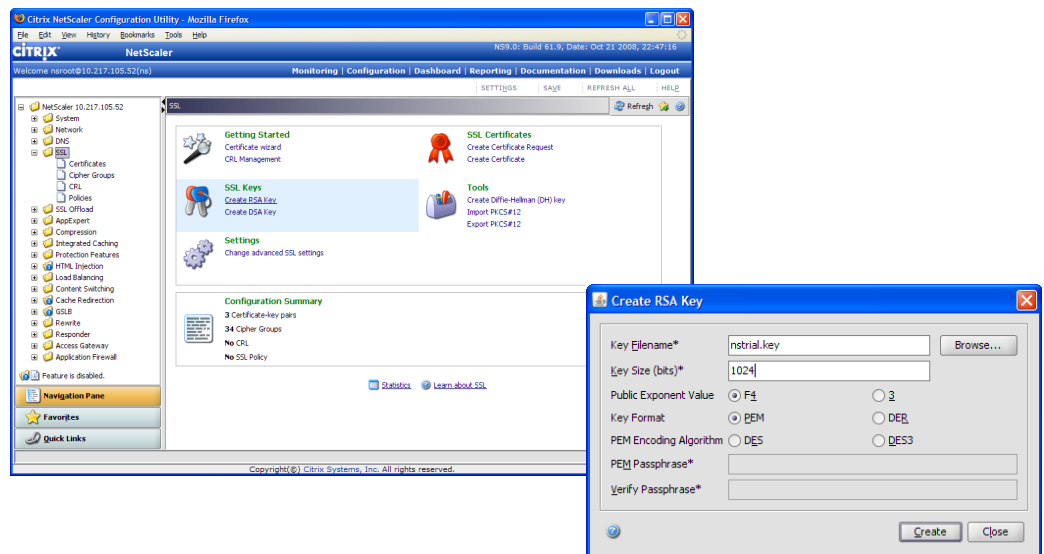
To obtain an SSL certificate from an authorized certificate authority (CA), you must create a Certificate Signing Request (CSR) and submit it to the CA. The following procedures describe how to create a CSR that you can submit to a CA, such as VeriSign, to obtain a valid certificate.

From the NetScaler GUI, select NetScaler → SSL → Create RSA Key.

Create the private key name and key size.

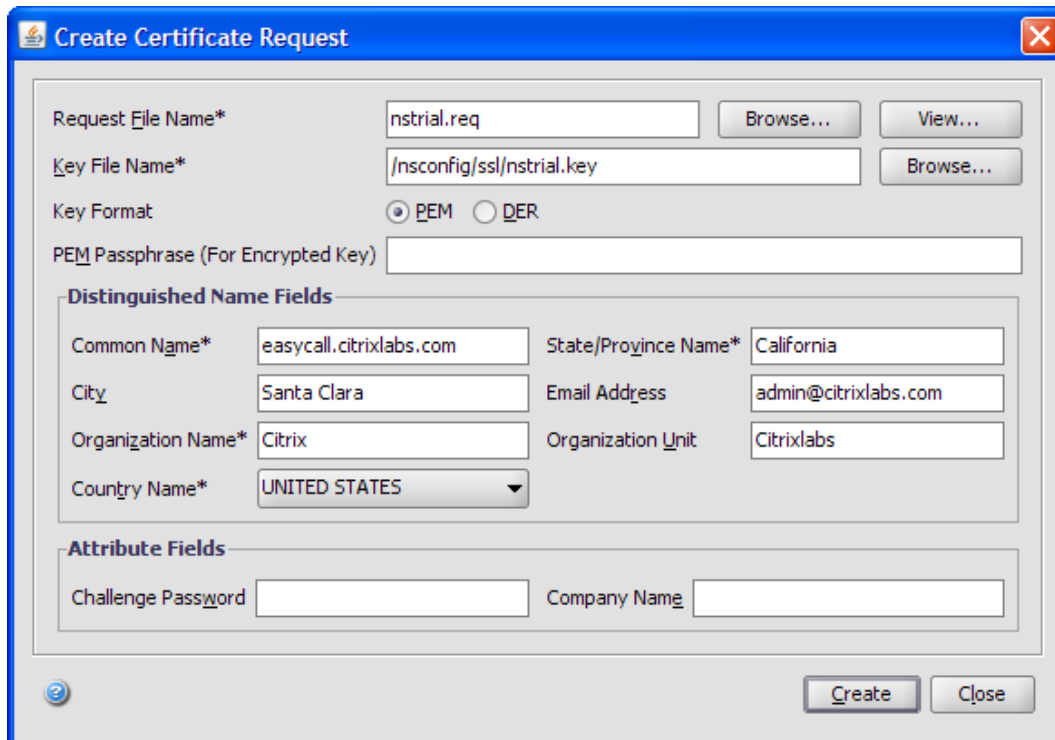
Note: NetScaler v9.0 supports key sizes: 512, 1024, 2048, 4096.

Select 'Create'.



## Create a Certificate Signing Request - NetScaler

The certificate signing request (CSR) is a collection of details, including the domain name, other important company details, and the private key to be used to create the certificate. To avoid generating an invalid certificate, you need to ensure that the details provided are accurate.



The screenshot shows the 'Create Certificate Request' dialog box. It has a blue title bar with a close button. The main area contains several input fields and buttons. At the top, there are 'Request File Name\*' and 'Key File Name\*' fields, each with a 'Browse...' button. Below these is the 'Key Format' section with radio buttons for 'PEM' (selected) and 'DER'. A 'PEM Passphrase (For Encrypted Key)' field is below that. The 'Distinguished Name Fields' section contains: 'Common Name\*' (easycall.citrixlabs.com), 'State/Province Name\*' (California), 'City' (Santa Clara), 'Email Address' (admin@citrixlabs.com), 'Organization Name\*' (Citrix), 'Organization Unit' (Citrixlabs), and 'Country Name\*' (UNITED STATES). The 'Attribute Fields' section has 'Challenge Password' and 'Company Name' fields. At the bottom right are 'Create' and 'Close' buttons.

From the NetScaler GUI, select NetScaler → SSL → Create Certificate Request.

Enter the request filename.

Enter the key filename, created in the previous step.

Enter the DN fields and select 'Create'.

## Copy Certificate Signing Request to Local Computer

The certificate signing request (CSR) will be sent to the Certificate Authority to create the Certificate for the NetScaler. The Certificate Signing Request file (INSeasycall3.req in this example) can be copied to the local computer a tool such as WinSCP, <http://winscp.net>.

The CSR file is located in the /nsconfig/ssl directory.

### TIP:

#### Common Name:

The common name should match the name used by DNS servers during a DNS lookup of your virtual server (for example, vpn.citrixlabs.com). Most browsers use this information for authenticating the virtual server's certificate during the SSL handshake. If the virtual server DNS name does not match the common name as given in the server certificate, the browsers will terminate the SSL handshake or prompt the user with a warning message. Do not use wildcard characters such as \* or ? and do not use an IP address as a common name. The common name should be without the protocol specifier http:// or https://.

#### Organization Name:

The organization name (corporation, limited partnership, university, or government agency) must be registered with some authority at the national, state, or city level. Use the legal name under which the organization is registered. Do not abbreviate the organization name and do not use the following characters in the name: < > ~ ! @ # \$ % ^ \* / \ ( ) ?. For example, Citrix Systems, Inc.

Use a program such as WinSCP to copy the Certificate Signing Request and key file to the Local computer.

ex:

nstrial.req  
nstrial.key

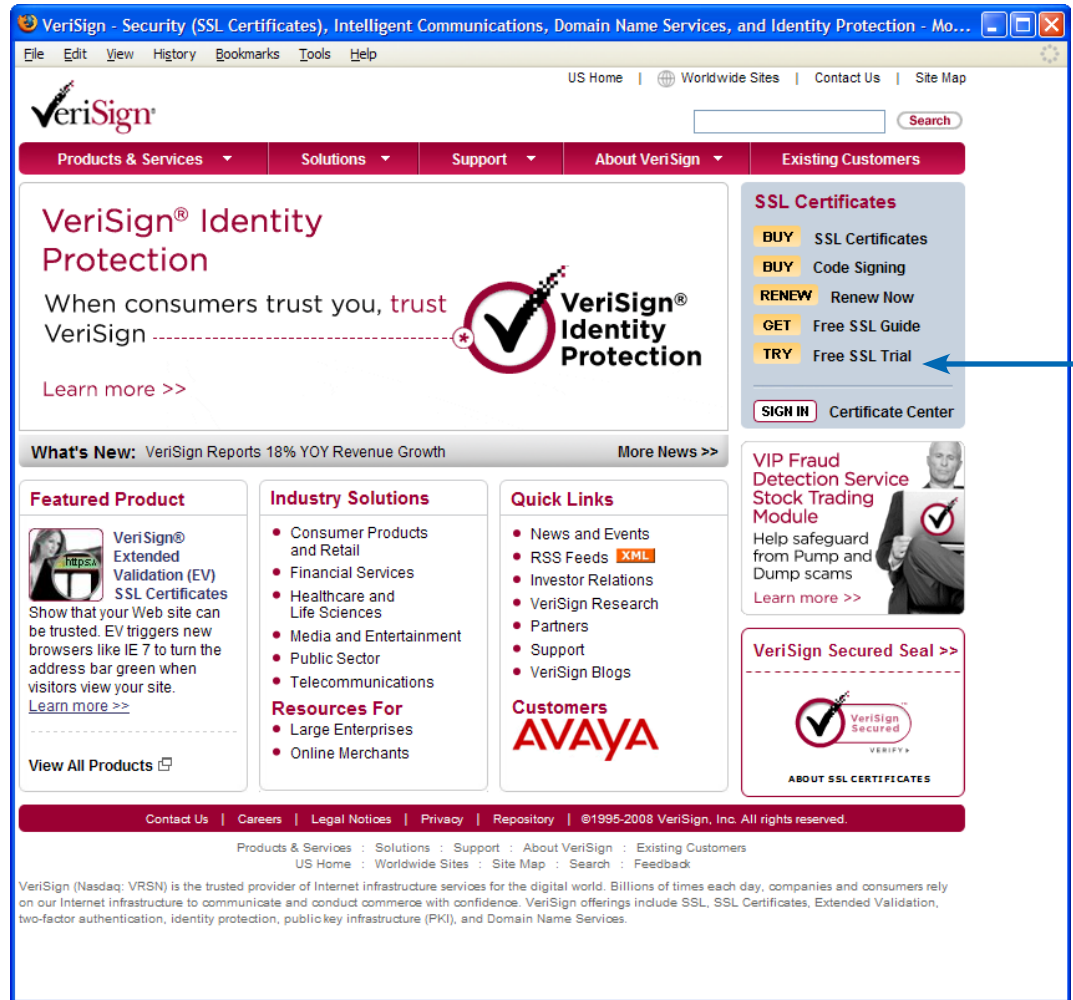
## Submit CSR to Certificate Authority - VeriSign

The Certificate Authority usually accepts Certificate Signing Requests directly on their website through an input form.

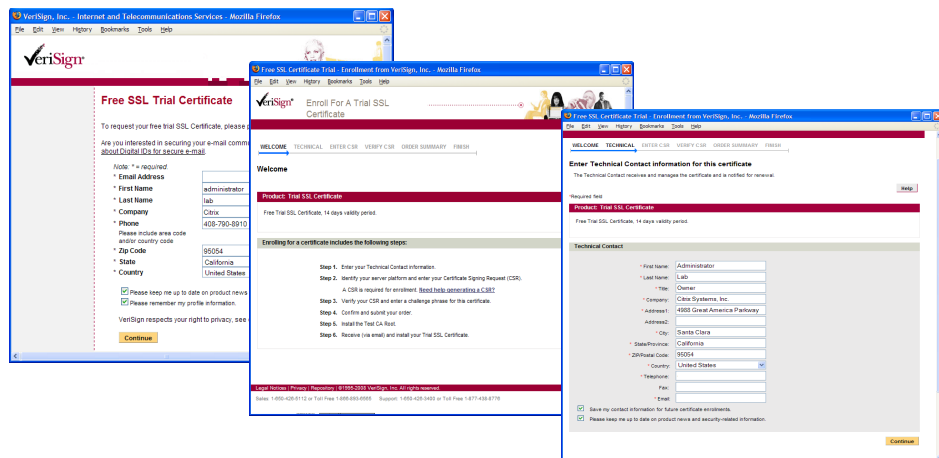
Navigate to the VeriSign website, and select Free SSL Trial.

### Note:

This VeriSign SSL certificate is for Trial purposes only. After the Trial period of 14 days, you will need to purchase a valid certificate from VeriSign at <http://verisign.com>.



Fill in the forms.



```

nstrial.req - WordPad
File Edit View Insert Format Help
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIB5jCCAUSCAQAwgaUxCzAJBgNVBAYTA1VTMRMwEQYDVQQLIEpDZW50Ym91bnRl
MRQwEgYDVQQLH2EwYzMsYSAwHGMwYjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEw
EwPDAeXRYaXhsYWZzMSAwHGMwYjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEw
MCEGCSqGSIb3DQEJARYUWYWRtaW5AY210cm14bGFiYy5jb20wZ28wZDQyJkoZInVcN
AQEBBQADgY0AMIGJAoGBAMdXOLf69k0+9aa+XQsz8rPv5nJn3ZHpCBBk13U4eqzo
Ubsbh0rVR4fL5mj0qN1OLCMkiM9mHIH3bBySLTB8KGO21n70dkJ7n5/TdzYJozsH
XMtmcJRFBsCKR+hFzrb0I8hRobGBse/DI fbnObEvXNmpV9bzmTd0I0wXwEkkNqzX
AgMBAAGgADANBgkqhkiG9w0BAQUFAAOBQBCN76XJfJ1dmS1tXX+BzaYdqnG12sP
5UJe4GY6WpTavF28dbFGMf+gkquQ1bGkh0+S1L/Wsk1dex2hjwOEsAurWn8Z8XUE
PDPF7cLty6APi12HIWjXxZCY/1kI21MAgX7hTZVtnmI/sTpVBYjfwFzJrcGts7hg
Hmj dIEgTzEuBw==
-----END NEW CERTIFICATE REQUEST-----
For Help, press F1
NUM

```



Open the CSR file on the local computer.

Copy the entire contents of the file including the

-----BEGIN CERTIFICATE REQUEST-----

... to the ...

-----END CERTIFICATE REQUEST-----.

Paste it into the CSR form on the VeriSign Certificate Authority website.

Free SSL Certificate Trial - Enrollment from VeriSign, Inc. - Mozilla Firefox

Enroll For A Trial SSL Certificate

WELCOME TECHNICAL ENTER CSR VERIFY CSR ORDER SUMMARY FINISH

### Enter Certificate Signing Request (CSR)

A Certificate Signing Request (CSR) is your server's unique "fingerprint" and is generated from the server that will host the requested SSL Certificate. For detailed instructions for generating a CSR, [click here](#).

Note: For an Extended Validation Certificate, the City/Location (L), State/Province (S), and Country (C) fields must indicate the jurisdiction where the organization is registered.

Product: Trial SSL Certificate

Free Trial SSL Certificate, 14 days validity period.

#### Enter Certificate Signing Request (CSR)

\* Required field

\* Select Server Platform:

Netscape  
Apache  
iPlanet  
Server not listed

Certificate Signing Request example:

```

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIB5jCCAUSCAQAwgaUxCzAJBgNVBAYTA1VTMRMwEQYDVQQLIEpDZW50Ym91bnRl
MRQwEgYDVQQLH2EwYzMsYSAwHGMwYjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEw
EwPDAeXRYaXhsYWZzMSAwHGMwYjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEw
MCEGCSqGSIb3DQEJARYUWYWRtaW5AY210cm14bGFiYy5jb20wZ28wZDQyJkoZInVcN
AQEBBQADgY0AMIGJAoGBAMdXOLf69k0+9aa+XQsz8rPv5nJn3ZHpCBBk13U4eqzo
Ubsbh0rVR4fL5mj0qN1OLCMkiM9mHIH3bBySLTB8KGO21n70dkJ7n5/TdzYJozsH
XMtmcJRFBsCKR+hFzrb0I8hRobGBse/DI fbnObEvXNmpV9bzmTd0I0wXwEkkNqzX
AgMBAAGgADANBgkqhkiG9w0BAQUFAAOBQBCN76XJfJ1dmS1tXX+BzaYdqnG12sP
5UJe4GY6WpTavF28dbFGMf+gkquQ1bGkh0+S1L/Wsk1dex2hjwOEsAurWn8Z8XUE
PDPF7cLty6APi12HIWjXxZCY/1kI21MAgX7hTZVtnmI/sTpVBYjfwFzJrcGts7hg
Hmj dIEgTzEuBw==
-----END NEW CERTIFICATE REQUEST-----

```

\* Paste Certificate Signing Request (CSR), obtained from your server: [More Information](#)

```

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIB5jCCAUSCAQAwgaUxCzAJBgNVBAYTA1VTMRMwEQYDVQQLIEpDZW50Ym91bnRl
MRQwEgYDVQQLH2EwYzMsYSAwHGMwYjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEw
EwPDAeXRYaXhsYWZzMSAwHGMwYjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEw
MCEGCSqGSIb3DQEJARYUWYWRtaW5AY210cm14bGFiYy5jb20wZ28wZDQyJkoZInVcN
AQEBBQADgY0AMIGJAoGBAMdXOLf69k0+9aa+XQsz8rPv5nJn3ZHpCBBk13U4eqzo
Ubsbh0rVR4fL5mj0qN1OLCMkiM9mHIH3bBySLTB8KGO21n70dkJ7n5/TdzYJozsH
XMtmcJRFBsCKR+hFzrb0I8hRobGBse/DI fbnObEvXNmpV9bzmTd0I0wXwEkkNqzX
AgMBAAGgADANBgkqhkiG9w0BAQUFAAOBQBCN76XJfJ1dmS1tXX+BzaYdqnG12sP
5UJe4GY6WpTavF28dbFGMf+gkquQ1bGkh0+S1L/Wsk1dex2hjwOEsAurWn8Z8XUE
PDPF7cLty6APi12HIWjXxZCY/1kI21MAgX7hTZVtnmI/sTpVBYjfwFzJrcGts7hg
Hmj dIEgTzEuBw==
-----END NEW CERTIFICATE REQUEST-----

```

What do you plan to use this SSL Certificate for? (optional):

Complete the remaining forms.

The image displays three overlapping screenshots of the VeriSign enrollment process for a trial SSL certificate. The browser window is titled "Free SSL Certificate Trial - Enrollment from VeriSign, Inc. - Mozilla Firefox".

**Top Screenshot (ENTER CSR):** Shows the "ENTER CSR" step. The "Product" is "Trial SSL Certificate" with a 14-day validity period. The CSR information includes: Common Name: `easycall.citrixlabs.com`, City/Location: Santa Clara, State/Province: California, Organization: Citrix.

**Middle Screenshot (VERIFY CSR):** Shows the "VERIFY CSR" step. The "Order summary & acceptance" section includes the product details and CSR information. A "Change CSR" button is visible.

**Bottom Screenshot (ORDER SUMMARY):** Shows the "ORDER SUMMARY" step. It includes contact and payment information for the technical contact (Administrator: Lab, Owner: Citrix Systems, Inc., 4950 Great America Parkway, Santa Clara, California, US, 95054). It also includes a Privacy Statement and a Subscriber Agreement section with a "Printable Version" link.

**Final Confirmation Page:** The bottom-most screenshot shows a "Thank you for completing your order!" message. It states: "VeriSign is processing your Trial SSL Certificate request. Your Trial SSL Certificate and installation instructions will be sent to you via email within the next hour." The order number is 351361401. A "Chat With Us" button is also present.



# Obtain Root CA & Intermediate CA Certificates

## Note:

These VeriSign SSL Root CA and Intermediate CA certificates are for Trial purposes only.

## Obtain Root CA and Intermediate Root CA Certificates from Certificate Authority - VeriSign

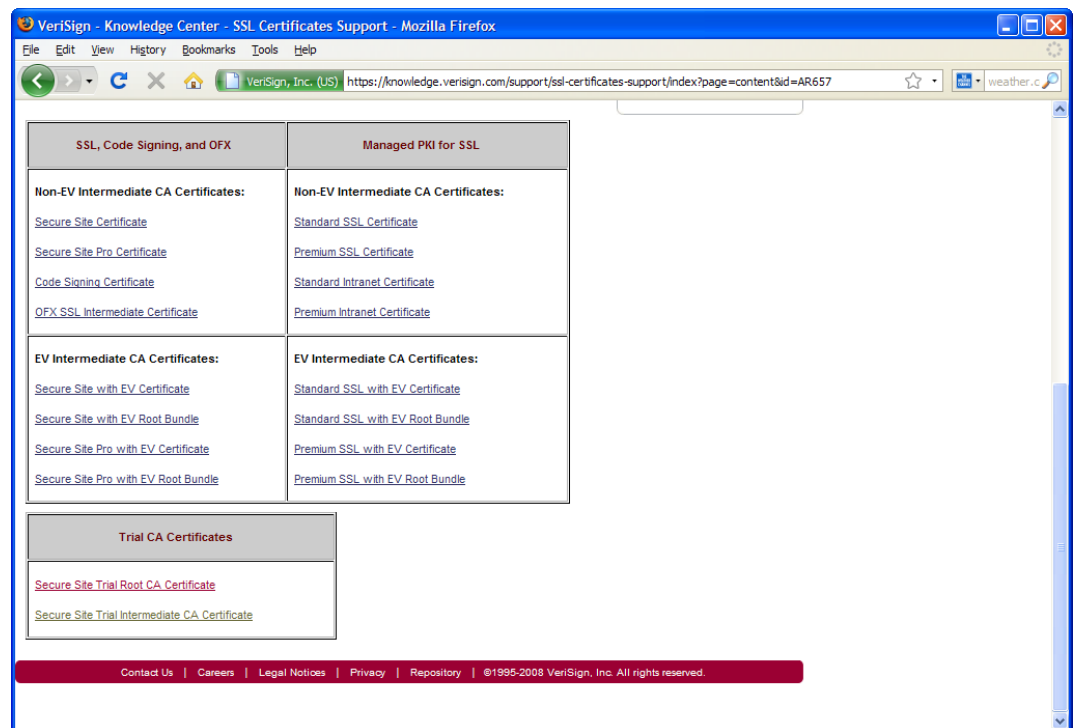
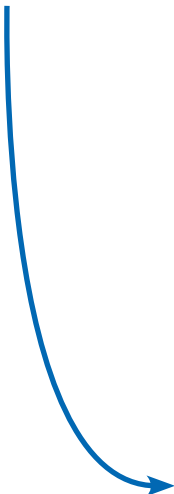
The Citrix NetScaler supports chaining of Certificates, and the use of Intermediate CA certificates. As of the time of the writing of this guide, VeriSign released a statement that all VeriSign SSL Certificates issued after December 11, 2008 will be chained to offline Certificate Authority (CA) roots to align with security best practices. Chained certificates are preferred because offline CA storage provides greater protection of the root's key pair from attacks, and Intermediate Root CAs can be maintained for each unique product and updated without disruption to the customer.

VeriSign, along with other Certificate Authorities, provide Trial Root CA and Trial Intermediate Root CA Certificates for use with the Trial Certificates that they issue. We will download the Trial Root CA and Trial Intermediate Root CA Certificates and save them for later use.

The Trial CA Certificates on the VeriSign website are located at:

<https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AR657>

Navigate to the VeriSign website, Where the Trial CA Certificates are located.





# Installing Server (NetScaler) Certificates

## Installing Server Certificate From Certificate Authority - NetScaler

After receiving and saving the Certificate, signed by the Certificate Authority, you need to add it to the NetScaler.

From the NetScaler GUI, select NetScaler → SSL → Certificates.

Select 'Add'.

Name:

- Type in a name for the Cert

File Location:

- Local Computer

Certificate File Name:

- <Browse>
- Select filename NetScaler Trial Certificate was saved to in previous step. ex: nstrial.cer.

Private Key File Name:

- <Browse>
- Select the key that was copy from the NetScaler to the Local Computer earlier. (Used to create the Certificate Signing Request). ex: nstrial.key.

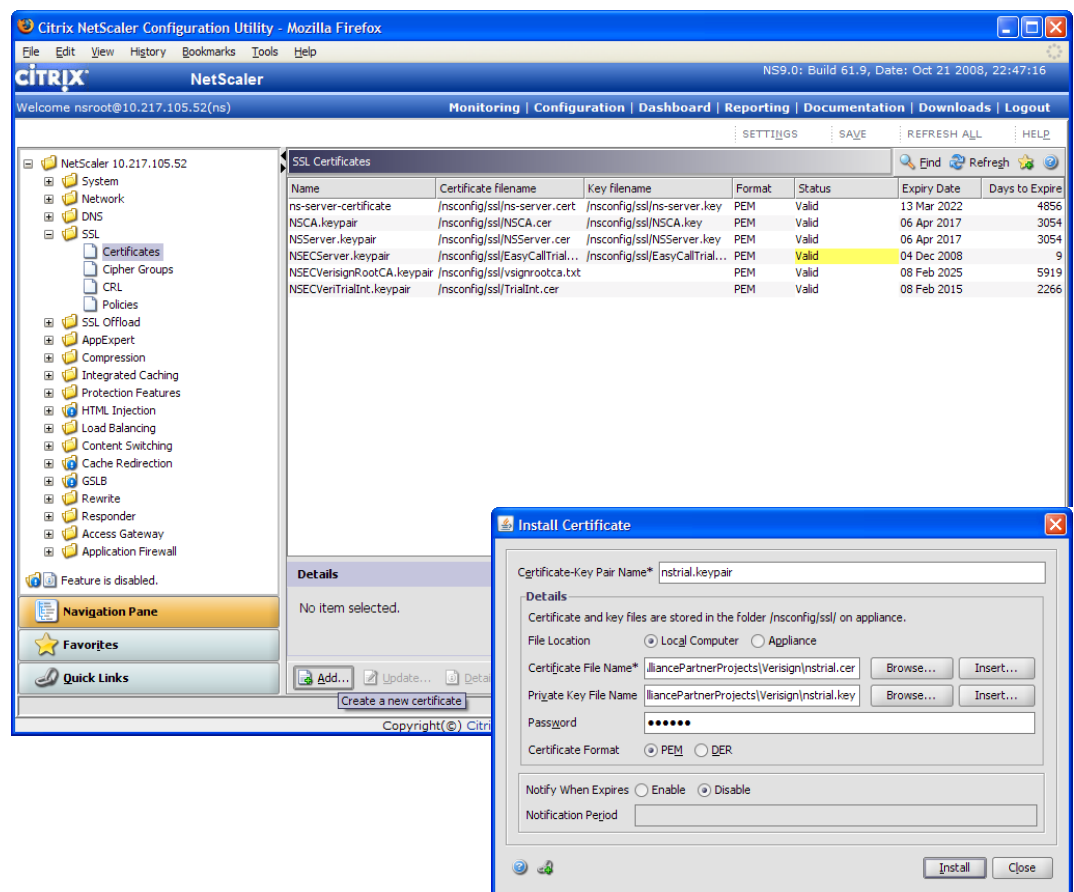
Password:

- Type in a password to encrypt the certificate.

Certificate Format:

- PEM

Click 'Install'.



## Installing Intermediate CA Certificate - NetScaler

In order for the Certificate chain to authenticate properly in the client's browser, the VeriSign Intermediate CA Certificate must be installed in the NetScaler and linked to the VeriSign Signed NetScaler Certificate, so that it can be sent with it when the client connects.

The screenshot shows the Citrix NetScaler Configuration Utility interface. The main window displays the 'SSL Certificates' table with the following data:

Name	Certificate filename	Key filename	Format	Status	Expiry Date	Days to Expire
ns-server-certificate	/nsconfig/ssl/ns-server.cert	/nsconfig/ssl/ns-server.key	PEM	Valid	13 Mar 2022	4856
NSCA.keypair	/nsconfig/ssl/NSCA.cer	/nsconfig/ssl/NSCA.key	PEM	Valid	06 Apr 2017	3054
NSServer.keypair	/nsconfig/ssl/NSServer.cer	/nsconfig/ssl/NSServer.key	PEM	Valid	06 Apr 2017	3054
NSECServer.keypair	/nsconfig/ssl/EasyCallTrial...	/nsconfig/ssl/EasyCallTrial...	PEM	Valid	04 Dec 2008	9
NSECVerisignRootCA.keypair	/nsconfig/ssl/vsignrootca.txt		PEM	Valid	08 Feb 2025	5919
NSECVeriTrialInt.keypair	/nsconfig/ssl/TrialInt.cer		PEM	Valid	08 Feb 2015	2266
nstrial.keypair	/nsconfig/ssl/nstrial.cer	/nsconfig/ssl/nstrial.key	PEM	Valid	09 Dec 2008	14

The 'Install Certificate' dialog box is open, showing the following details:

- Certificate-Key Pair Name\*: vstrialIntermedCA.keypair
- File Location:  Local Computer  Appliance
- Certificate File Name\*: ;PartnerProjects\Verisign\vstrialIntCA.cer
- Private Key File Name: (empty)
- Certificate Format:  PEM  DER
- Notify When Expires:  Enable  Disable
- Notification Period: (empty)

From the NetScaler GUI, select NetScaler → SSL → Certificates.

Select 'Add'.

Name:

- Type in a name for the Cert

File Location:

- Local Computer

Certificate File Name:

- <Browse>
- Select the VeriSign Trial Intermediate CA Certificate that was save in a previous step. ex: vstrialIntCA.cer

Private Key File Name:

- <A key is not needed for an Intermediate CA Certificate>

Certificate Format:

- PEM

Click 'Install'.

## Linking VeriSign Intermediate CA Certificate to NetScaler Signed Certificate - NetScaler

Linking the VeriSign Intermediate CA Certificate to the NetScaler Signed Certificate is easy.

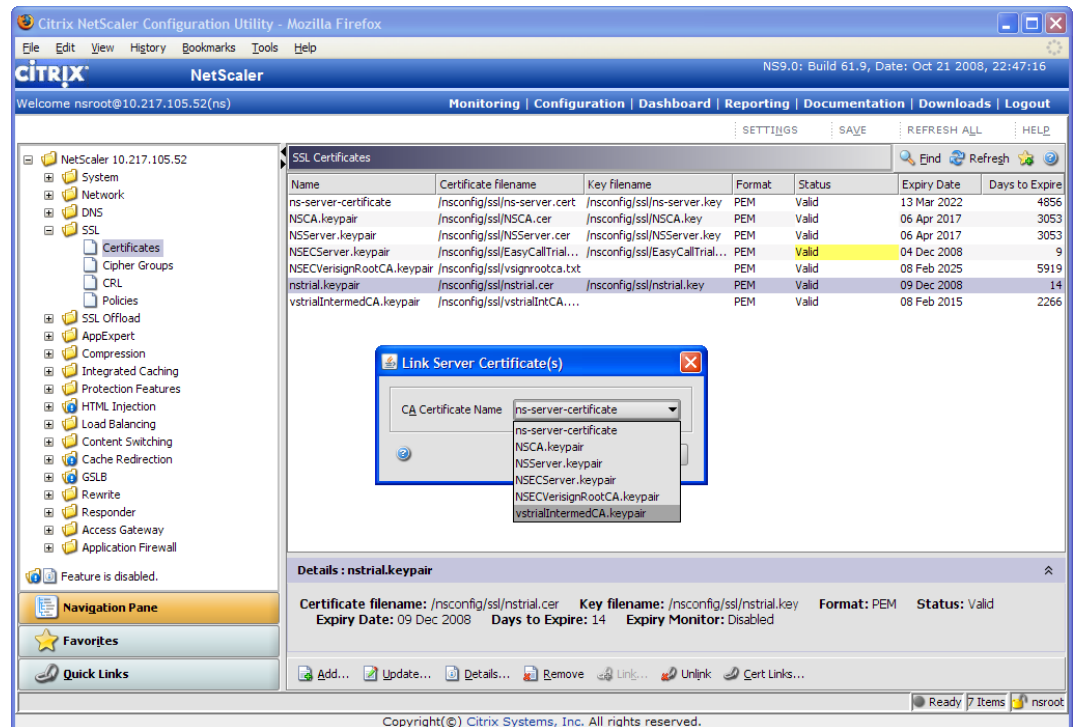
From the NetScaler GUI, select NetScaler → SSL → Certificates.

Highlight or select the NetScaler Signed Trial Certificate that was previously installed.

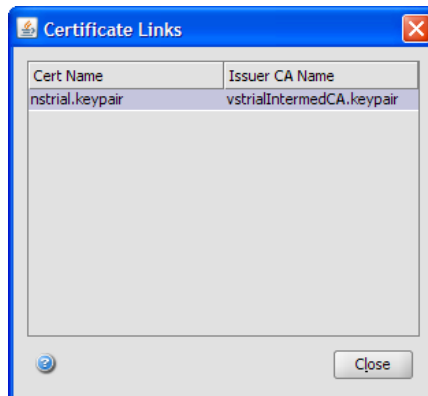
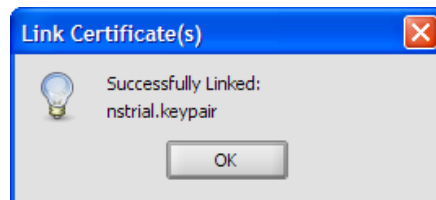
Select "Link".

Select the VeriSign Intermediate CA Certificate that was previously installed from the drop down menu.

Select 'Ok'



The Link can be checked by selecting "Cert Links".



We are finished with the NetScaler.

The nstrial.keypair is ready to be bound to an SSL VServer within the NetScaler.

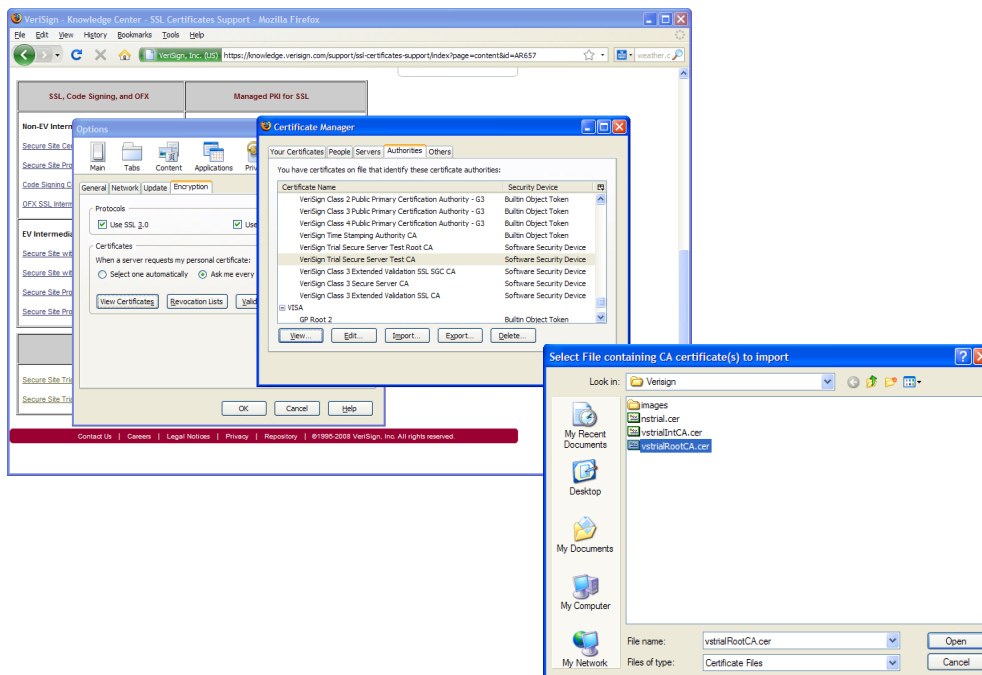
# Importing Client (Browser) Certificates

## Importing VeriSign Trial Root CA Cert and Trial Int CA Cert into Client browser - Browser

For SSL communication to work seamlessly, the Certificate chain received by the client (browser) from the server or SSL endpoint (NetScaler) must validate and authenticate. This chain links the server certificate to its issuer (the Intermediate CA).

In order for this to work, the Intermediate CA certificate must already be installed in the NetScaler and linked to the Server Certificate (Signed by VeriSign), which we performed in the previous step.

In addition, the VeriSign Root CA Certificate and the VeriSign Intermediate CA Certificate must be installed in the clients browser, which we perform in the following steps.



For example, using the Firefox Mozilla browser:

Select Tools → Options → Advanced → Encryption → View Certificates → Import.

Import the VeriSign Trial Root CA Certificate.

Import the VeriSign Trial Intermediate CA Certificate.

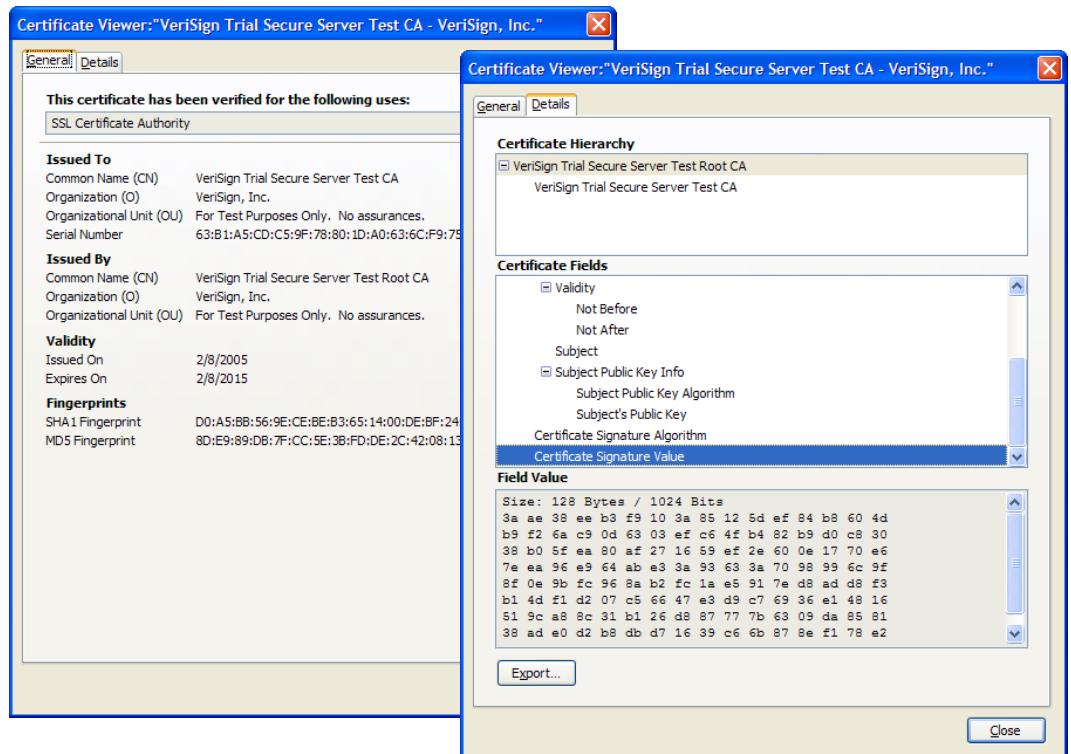
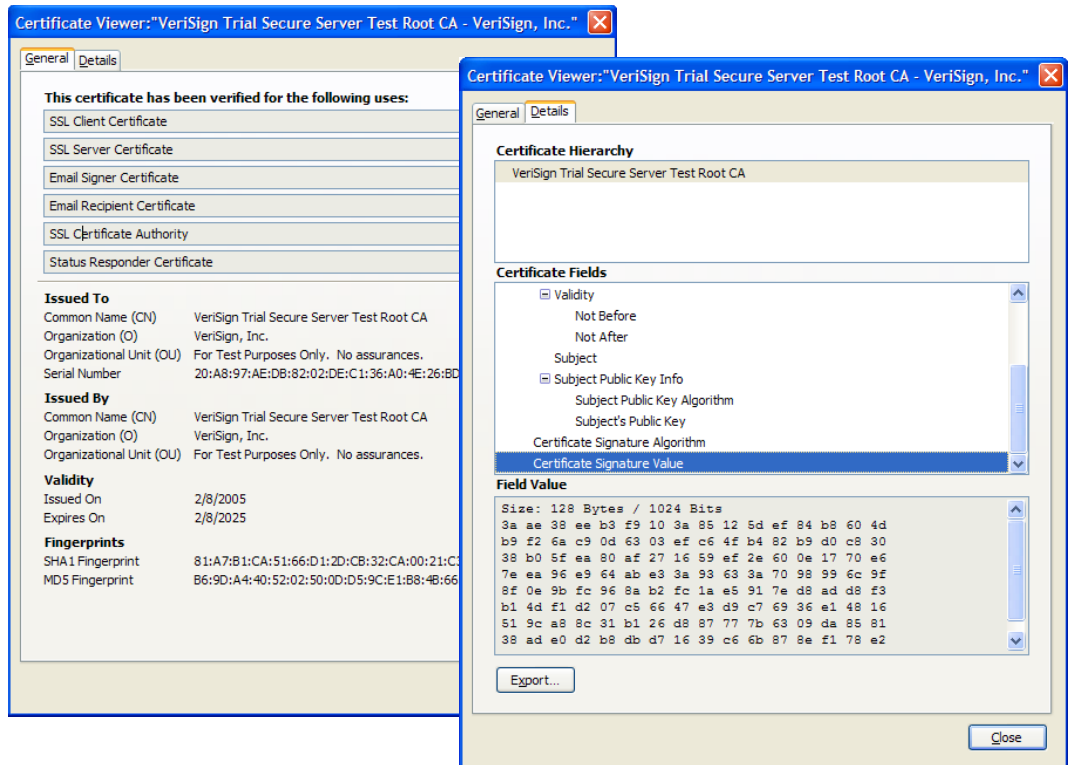
## Verifying Certificate Chain in Client browser - Browser

The VeriSign Root CA Certificate and the VeriSign Intermediate CA Certificate must be installed in the clients browser correctly. Always confirm the Certificates were imported correctly.

For example, using the Firefox Mozilla browser:

- Select Tools → Options →
- Advanced → Encryption →
- View Certificates → View.

The VeriSign Trial Root CA Certificate should be chained to the VeriSign Trial Intermediate CA Certificate.



# Citrix NetScaler SSL Offload Configuration

## SSL Offload Configuration - NetScaler

The Citrix NetScaler Application Switch will be configured for HTTPS on a public IP Address and then send the traffic to a backend server on the private network.

The screenshot shows the 'Create Virtual Server (SSL Offload)' dialog box in the Citrix NetScaler GUI. The configuration is as follows:

- Name\*: EasyCallSSLVIP
- IP Address\*: 67 . 97 . 253 . 92
- Protocol\*: SSL
- Port\*: 443
- Network VServer Range: 1
- Directly Addressable:
- State:

The dialog box also features a breadcrumb trail: Services \ Service Groups \ Policies \ Method and Persistence \ Advanced \ SSL Settings \. Below this, there are 'Activate All' and 'Deactivate All' buttons, and a 'Find' button. A table with the following columns is present:

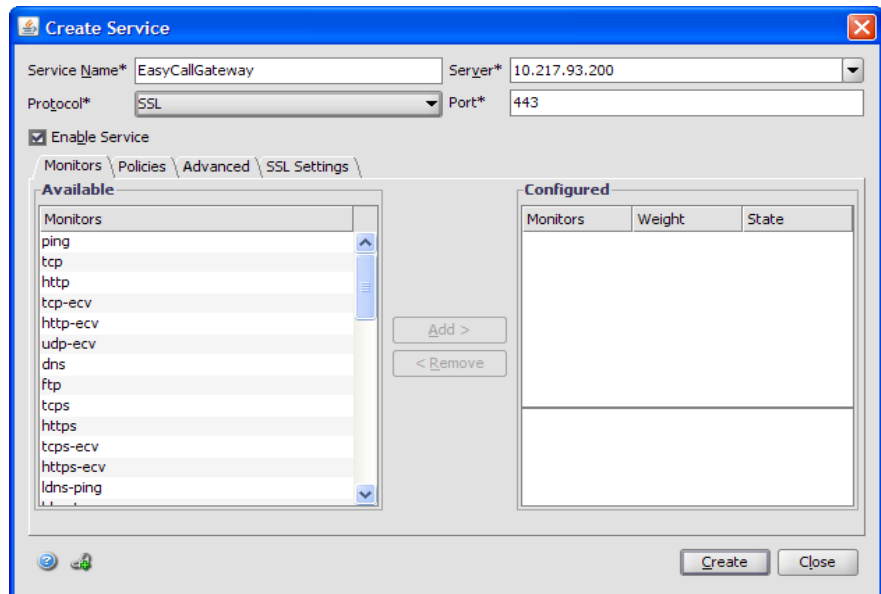
Active	Service Name	IP Address	Port	Protocol	State	Weight	Dynamic Weight
--------	--------------	------------	------	----------	-------	--------	----------------

At the bottom of the dialog box, there are 'Add...', 'Open...', and 'Remove' buttons, and 'Create' and 'Close' buttons.

From the NetScaler GUI, select NetScaler → SSL Offload → Virtual Servers → Add.

Add the SSL Offload name, Public IP Address, Change the Protocol to SSL and use port 443.

Select the Services tab. Enter the Backend Service name, private IP Address, set the protocol to SSL and use port 443.

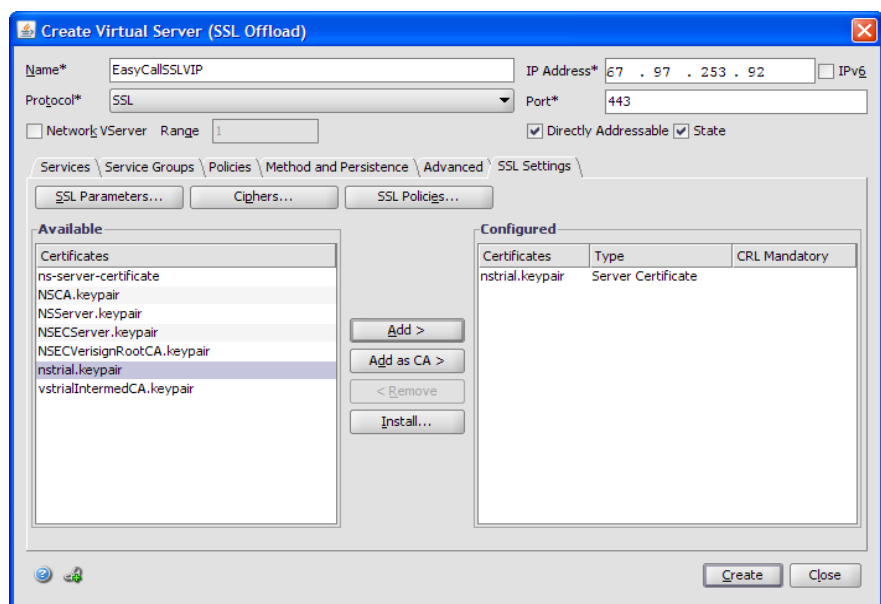


Select the SSL Settings tab.

Add the nstrial.keypair as a Server certificate.

Click on 'Create', 'Close'.

The NetScaler SSL Connection is ready for use.



# Testing the Client to NetScaler Certificate Chain

## Testing the VeriSign SSL Certificate Chain between Client and NetScaler - VeriSign

To verify that the Certificate chain is working correctly between the client browser and the Citrix NetScaler, you can connect to VeriSign's website and verify the Certificate chain by accessing the following link:

<https://knowledge.verisign.com/support/ssl-certificates-support/index?page=certchecker>

VeriSign - Knowledge Center - SSL Certificates Support - Mozilla Firefox

File Edit View History Bookmarks Tools Help

VeriSign, Inc. (US) <https://knowledge.verisign.com/support/ssl-certificates-support/index?page=certchecker>

US Home | Worldwide Sites | Contact Us | Site Map

**VeriSign**

Products & Services Solutions Support About VeriSign Existing Customers

### VeriSign SSL Certificate Installation Checker

Once you have installed your VeriSign SSL Certificate, you can verify that the installation was successful by using the SSL Certificate Installation Checker on this page. Please follow these steps to test your installation:

1. Enter your Domain Name into the Fully Qualified Domain Name field (e.g. type secure.verisign.com).
2. Enter the SSL port number for your Web server. (The default SSL port number for most servers is 443.)
3. Click **Test this Web Server**.

Enter your Web Server's domain name:

Enter your port (443 is default for SSL):

**Test this Web Server**

**Status: Successful**

**easycall.citrixlabs.com is successfully secured by an SSL certificate.**  
The following certificates are correctly installed:

-----Certificate 1-----  
--Issued To--  
Organization: Citrix Systems., Inc  
Organizational Unit: Terms of use at www.verisign.com/cps/testca (c)05  
Organizational Unit 2: Citrixlabs  
Common Name: easycall.citrixlabs.com  
Locale: Santa Clara, California  
Country: US

--Issued By--  
Organization: VeriSign., Inc.  
Organizational Unit: Terms of use at https://www.verisign.com/cps/testca (c)05  
Organizational Unit 2: For Test Purposes Only. No assurances.  
Common Name: VeriSign Trial Secure Server Test CA  
Country: US

Valid from Wed Nov 19 16:00:00 PST 2008 to Thu Dec 04 15:59:59 PST 2008  
Serial Number (hex): 41c7080afa3b54e29127b2d05275538a

-----Certificate 2-----  
--Issued To--

VeriSign, Inc makes no warranties of any kind (whether express, implied, or statutory) with respect to the services described or information contained herein.

Contact Us | Careers | Legal Notices | Privacy | Repository | ©1995-2008 VeriSign, Inc. All rights reserved.

# Citrix Worldwide

## Worldwide headquarters

Citrix Systems, Inc.  
851 West Cypress Creek Road  
Fort Lauderdale, FL 33309  
USA  
T +1 800 393 1888  
T +1 954 267 3000

## Regional headquarters

### Americas

Citrix Silicon Valley  
4988 Great America Parkway  
Santa Clara, CA 95054  
USA  
T +1 408 790 8000

### Europe

Citrix Systems International GmbH  
Rheinweg 9  
8200 Schaffhausen  
Switzerland  
T +41 52 635 7700

### Asia Pacific

Citrix Systems Hong Kong Ltd.  
Suite 3201, 32nd Floor  
One International Finance Centre  
1 Harbour View Street  
Central  
Hong Kong  
T +852 2100 5000

### Citrix Online division

5385 Hollister Avenue  
Santa Barbara, CA 93111  
USA  
T +1 805 690 6400

[www.citrix.com](http://www.citrix.com)

## About Citrix

Citrix Systems, Inc. (Nasdaq:CTXS) is the global leader and the most trusted name in application delivery infrastructure. More than 200,000 organizations worldwide rely on Citrix to deliver any application to users anywhere with the best performance, highest security and lowest cost. Citrix customers include 100% of the Fortune 100 companies and 98% of the Fortune Global 500, as well as hundreds of thousands of small businesses and prosumers. Citrix has approximately 6,200 channel and alliance partners in more than 100 countries. Annual revenue in 2006 was \$1.1 billion.

Citrix®, NetScaler®, GoToMyPC®, GoToMeeting®, GoToAssist®, Citrix Presentation Server™, Citrix Password Manager™, Citrix Access Gateway™, Citrix Access Essentials™, Citrix Access Suite™, Citrix SmoothRoaming™ and Citrix Subscription Advantage™ are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the U.S. Patent and Trademark Office and in other countries. UNIX® is a registered trademark of The Open Group in the U.S. and other countries. Microsoft®, Windows® and Windows Server® are registered trademarks of Microsoft Corporation in the U.S. and/or other countries. VeriSign, the VeriSign logo, the Checkmark Circle logo, VeriSign Secured, and the VeriSign Secured logo are registered or unregistered trademarks of VeriSign, Inc. All other trademarks and registered trademarks are property of their respective owners.

