Deployment Guide

VeriSign Certificate Authority
Citrix NetScaler SSL

Deployment Guide

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.

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.

Table of Contents

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

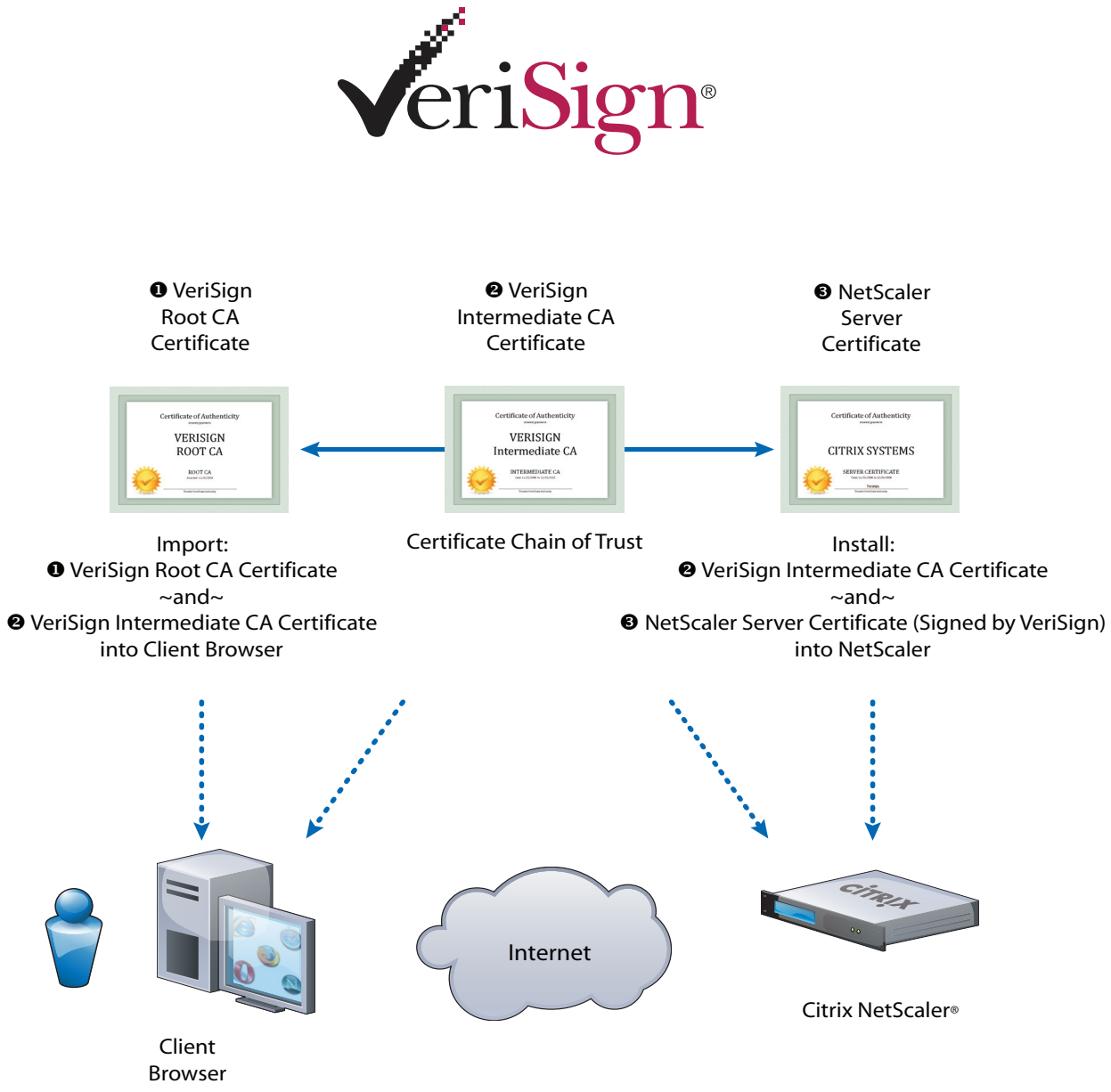
- NetScaler Application Switch - SSL Offload
- Public Trusted Certificate Authority Issued Certificates

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

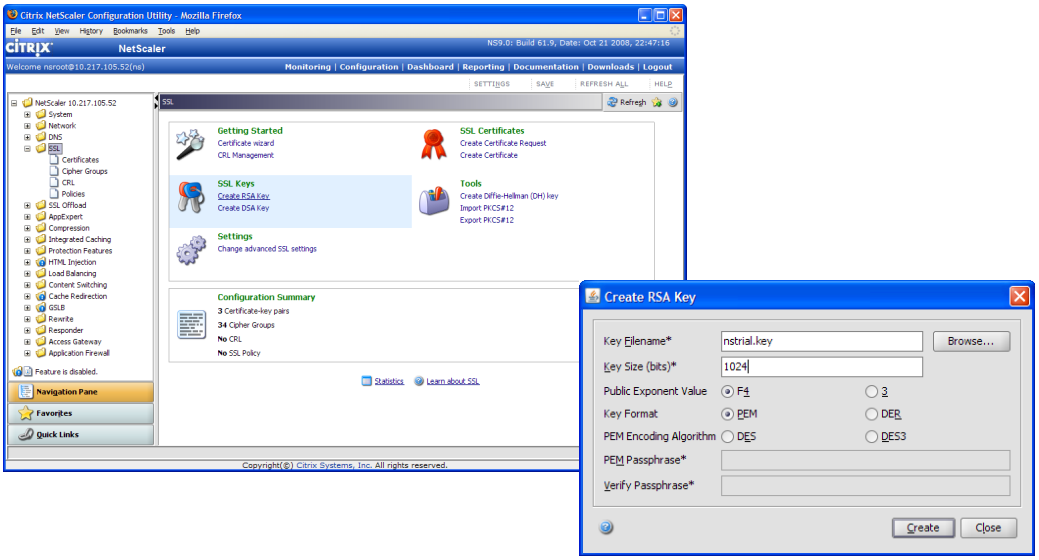
To obtain an SSL certificate from an authorized certificate authority (CA), you must create a Certificate Signing Request (CSR) and submit it to the CA. The following procedures describe how to create a CSR that you can submit to a CA, such as VeriSign, to obtain a valid certificate.

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

Create the private key name and key size.

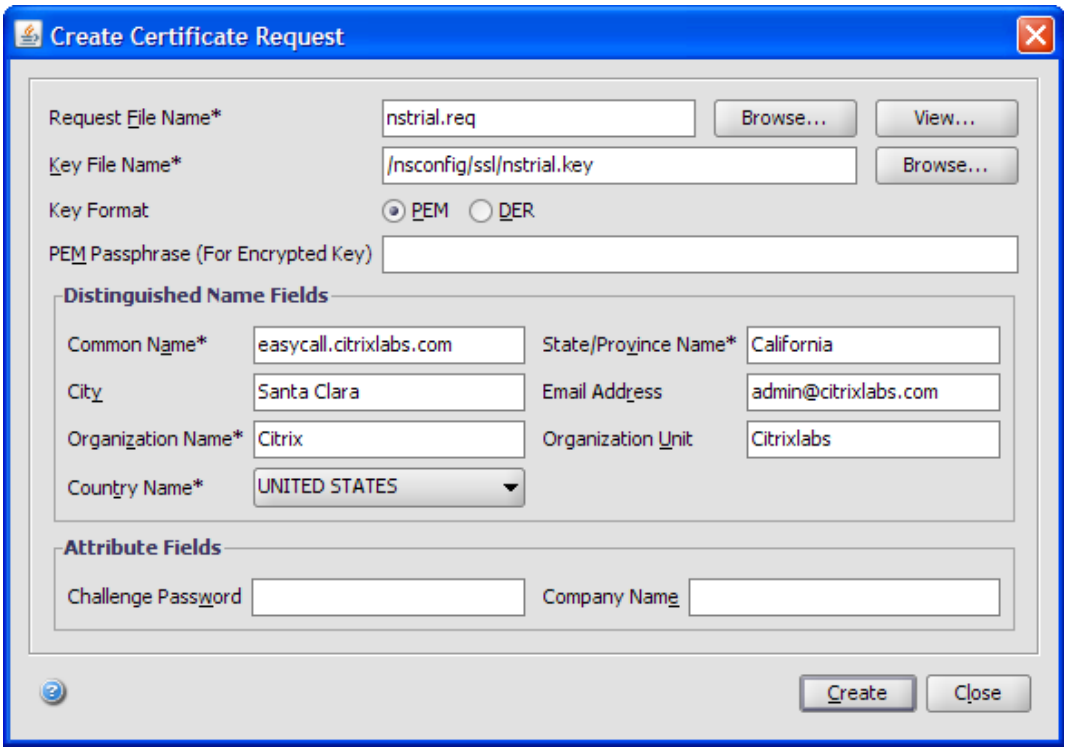
Note: NetScaler v9.0 supports key sizes: 512, 1024, 2048, 4096.

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.



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.

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

ex:
nstrial.req
nstrial.key

TIP:

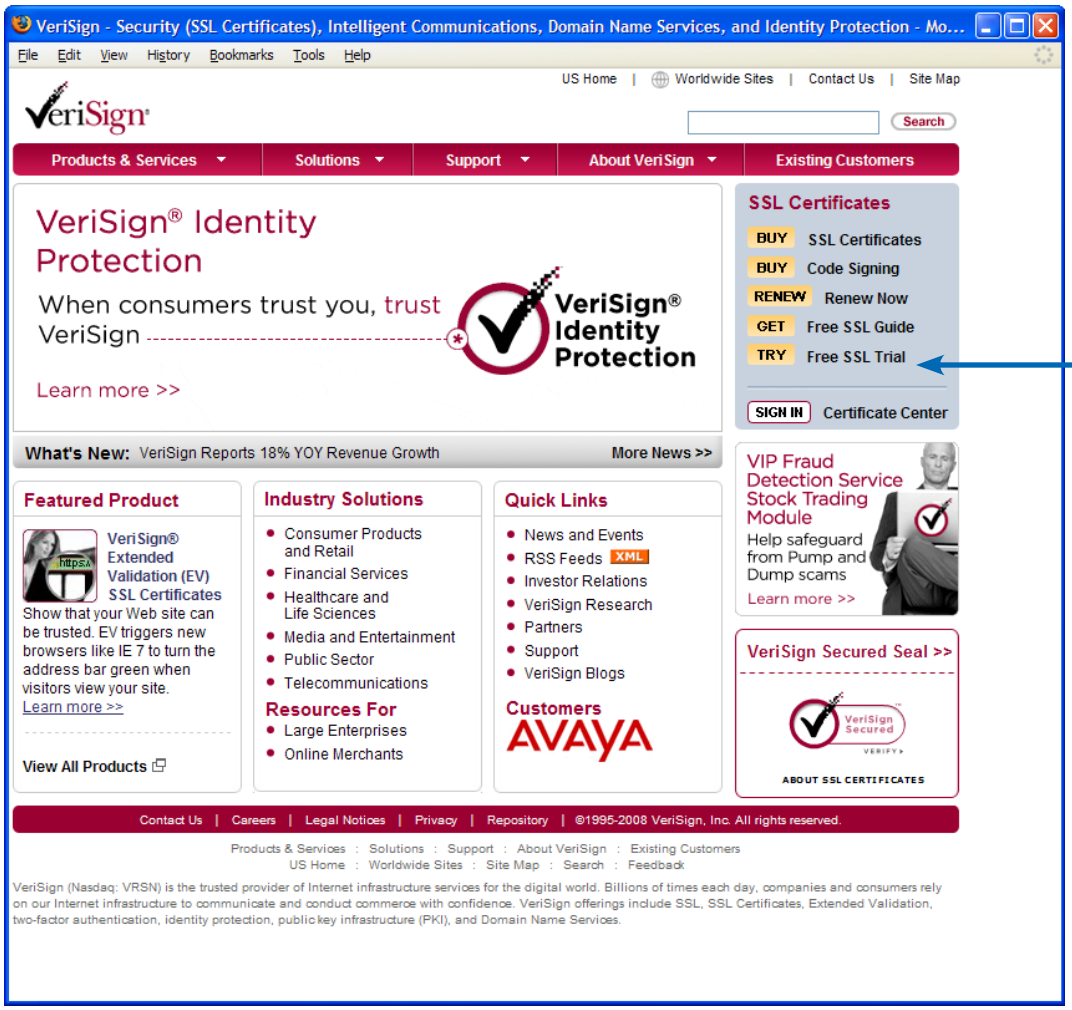
Common Name:
The common name should match the name used by DNS servers during a DNS lookup of your virtual server (for example, vpn.citrixlabs.com). Most browsers use this information for authenticating the virtual server's certificate during the SSL handshake. If the virtual server DNS name does not 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.

Submit CSR to Certificate Authority - VeriSign

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

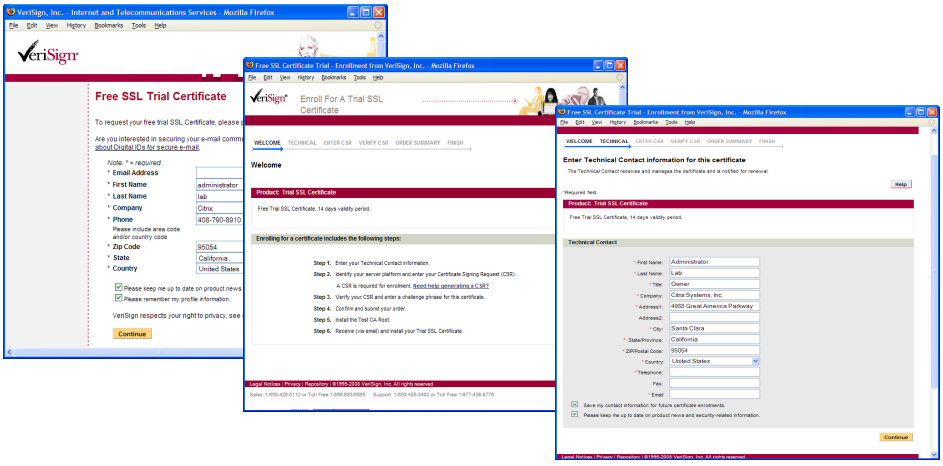
Navigate to the VeriSign website, and select Free SSL Trial.

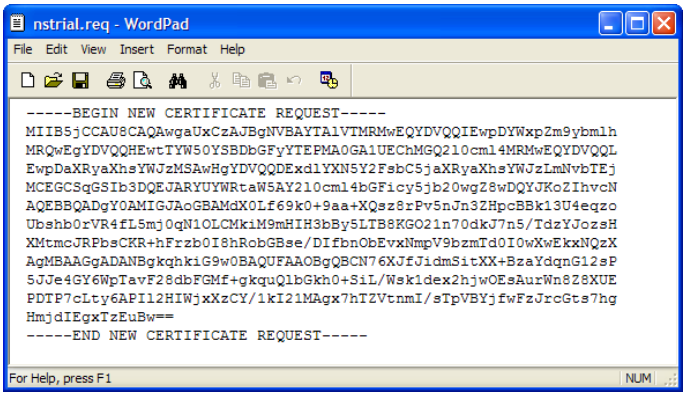


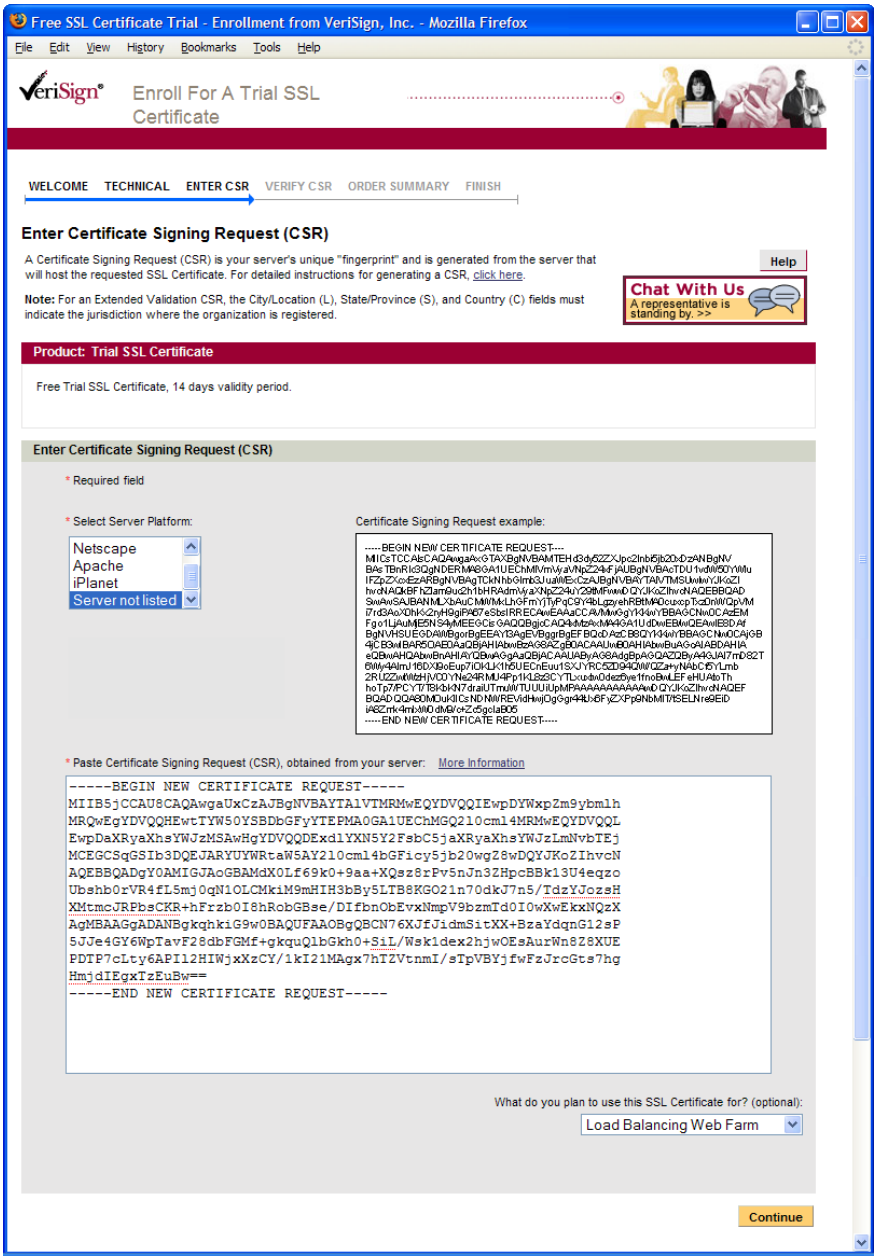
Note:

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.







Open the CSR file on the local computer.

Copy the entire contents of the file including the

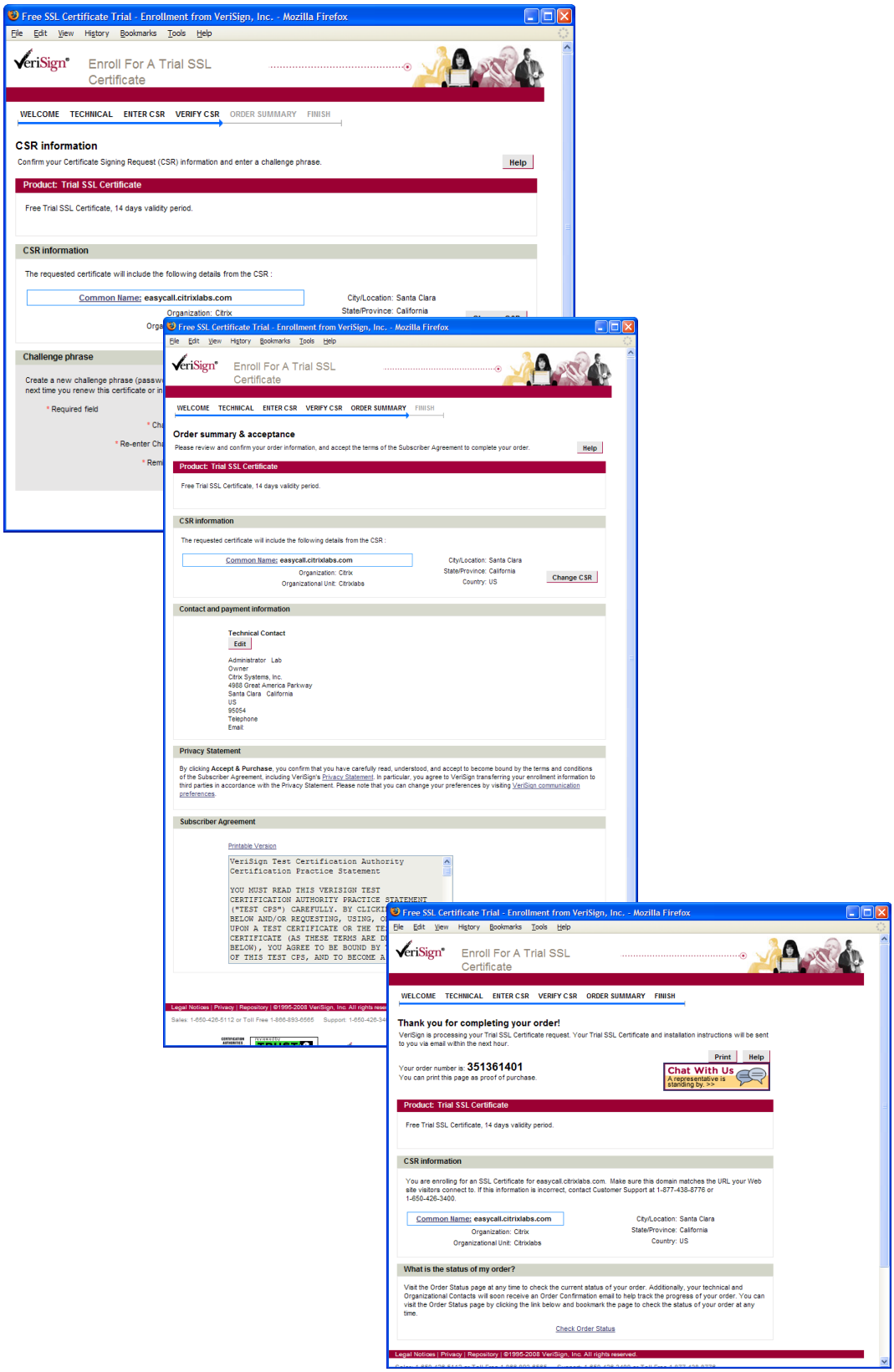
-----BEGIN CERTIFICATE REQUEST-----

... to the ...

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

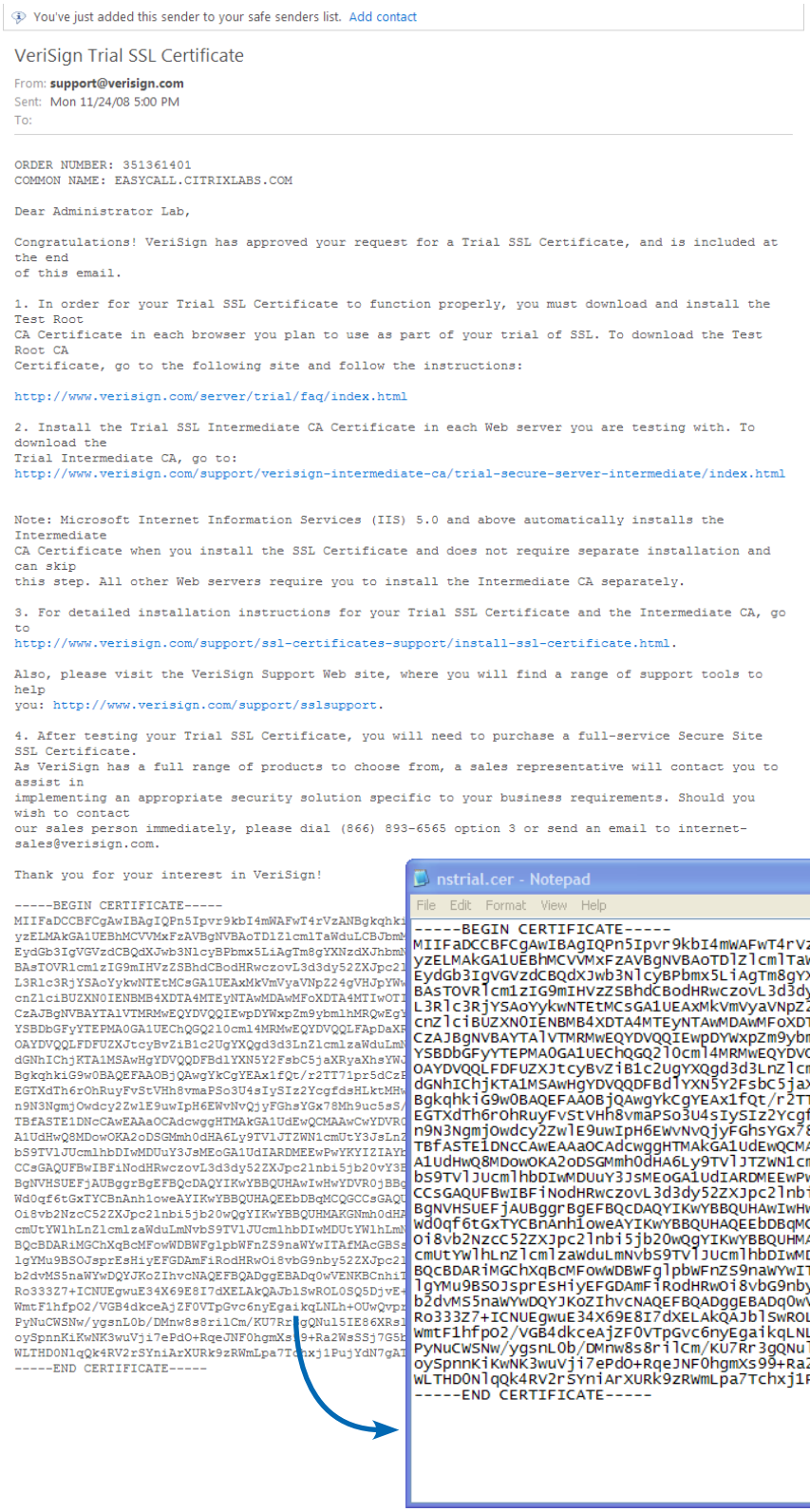
Paste it into the CSR form on the VeriSign Certificate Authority website.

Complete the remaining forms.



Receive Certificate from Certificate Authority - VeriSign

The Certificate Authority will send the certificate via email, along with instructions on how to install it.



You've just added this sender to your safe senders list. Add contact

VeriSign Trial SSL Certificate

From: **support@verisign.com**
Sent: Mon 11/24/08 5:00 PM
To:

ORDER NUMBER: 351361401
COMMON NAME: EASYCALL.CITRIXLABS.COM

Dear Administrator Lab,

Congratulations! VeriSign has approved your request for a Trial SSL Certificate, and is included at the end
of this email.

1. In order for your Trial SSL Certificate to function properly, you must download and install the Test Root
CA Certificate in each browser you plan to use as part of your trial of SSL. To download the Test Root CA
Certificate, go to the following site and follow the instructions:

http://www.verisign.com/server/trial/faq/index.html

2. Install the Trial SSL Intermediate CA Certificate in each Web server you are testing with. To download the
Trial Intermediate CA, go to:
http://www.verisign.com/support/verisign-intermediate-ca/trial-secure-server-intermediate/index.html

Note: Microsoft Internet Information Services (IIS) 5.0 and above automatically installs the Intermediate
CA Certificate when you install the SSL Certificate and does not require separate installation and can skip
this step. All other Web servers require you to install the Intermediate CA separately.

3. For detailed installation instructions for your Trial SSL Certificate and the Intermediate CA, go to
http://www.verisign.com/support/ssl-certificates-support/install-ssl-certificate.html.

Also, please visit the VeriSign Support Web site, where you will find a range of support tools to help
you: http://www.verisign.com/support/sslsupport.

4. After testing your Trial SSL Certificate, you will need to purchase a full-service Secure Site SSL Certificate.
As VeriSign has a full range of products to choose from, a sales representative will contact you to assist in
implementing an appropriate security solution specific to your business requirements. Should you wish to contact
our sales person immediately, please dial (866) 893-6565 option 3 or send an email to internet-sales@verisign.com.

Thank you for your interest in VeriSign!

-----BEGIN CERTIFICATE-----
MIIFaDCCBFCgAwIBAgIQPn5Ipvr9kbI4mWAFwT4rVzANBgkqhki
yzELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmM
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmN
BAsTOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2l
L3Rlc3RjYSAoYykwNTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWw
cnZlciBUZXN0IENBMB4XDTA4MTEyNTAwMDAwMFoXDTA4MTIwOTI
CzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRQwEg
YSBDbGFyYTEPMA0GA1UEChQGQ210cml4MRMwEQYDVQQLFApDaX
OAYDVQQLFDFUZXJtcyBvZiB1c2UgYXQgd3d3LnZlcmlzaWduLmN
dGNhICAjKTA1MSAwHgYDVQQDFBdlYXN5Y2FsbC5jaXRyaXhsYWJ
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAx1fQt/r2TT71pr5dCzP
EGTXdTh6rOhRuyFvStvVHh8vmaPSo3U4sIySIz2YcgfdsHLktMH
n9N3NgmjOwdcy2ZwlE9uwIpH6EWvNvQjyFGhsYGx78Mh9uc5sS/
TBfASTE1DNcCAwEAAaOCAdcwggHTMAkGA1UdEwQCMAAwCwYDVR0
A1UdHwQ8MDowOKA2oDSGMmh0dHA6Ly9TVlJTZWN1cmUtY3JsLn
bS9TVlJUcmlhbDIwMDUuY3JsMEoGA1UdIARDMEEwPwYKYIZIAY
CCsGAQUFBwIBFiNodHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3
BgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwHwYDVR0jBB
Wd0qf6tGxTYCBnAnh1oweAYIKwYBBQUHAQEEbDBqMCQGCCsGAQ
Oi8vb2NzcC52ZXJpc2lnbi5jb20wQgYIKwYBBQUHMAKGNmh0dH
cmUtYWlhLnZlcmlzaWduLmNvbS9TVlJUcmlhbDIwMDUtYWlhLm
BQcBDARiMGChXqBcMFowWDBWFglpbWFnZS9naWYwITAfMAcGBS
lgYMu9BSOJsprEsHiyEFGDAmFiRodHRwOi8vbG9nby52ZXJpc2
b2dvMS5naWYwDQYJKoZIhvcNAQEFBQADggEBADq0wVENKBCnhi
Ro333Z7+ICNUEgwuE34X69E8I7dXELAkQAJblSwROL0SQ5DjvE
WmtF1hfpO2/VGB4dkceAjZF0VTpGvc6nyEgaikqLNLh+OUwQvp
PyNuCWSNw/ygsnL0b/DMnw8s8rilCm/KU7Rr3gQNul5IE86XRs
oySpnnKiKwNK3wuVji7ePdO+RqeJNF0hgmXs99+Ra2WsS5j7G5
WLTHD0NlqQk4RV2rSYniArXURk9zRWmLpa7Tchxj1PujYdN7gA
-----END CERTIFICATE-----

Copy the entire contents of the Certificate, including the

-----BEGIN CERTIFICATE-----

... to the ...

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

Open Notepad.

Turn on Wordwrap.

Paste it and save it to a filename with a .cer extension.

ex:
nstrial.cer

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

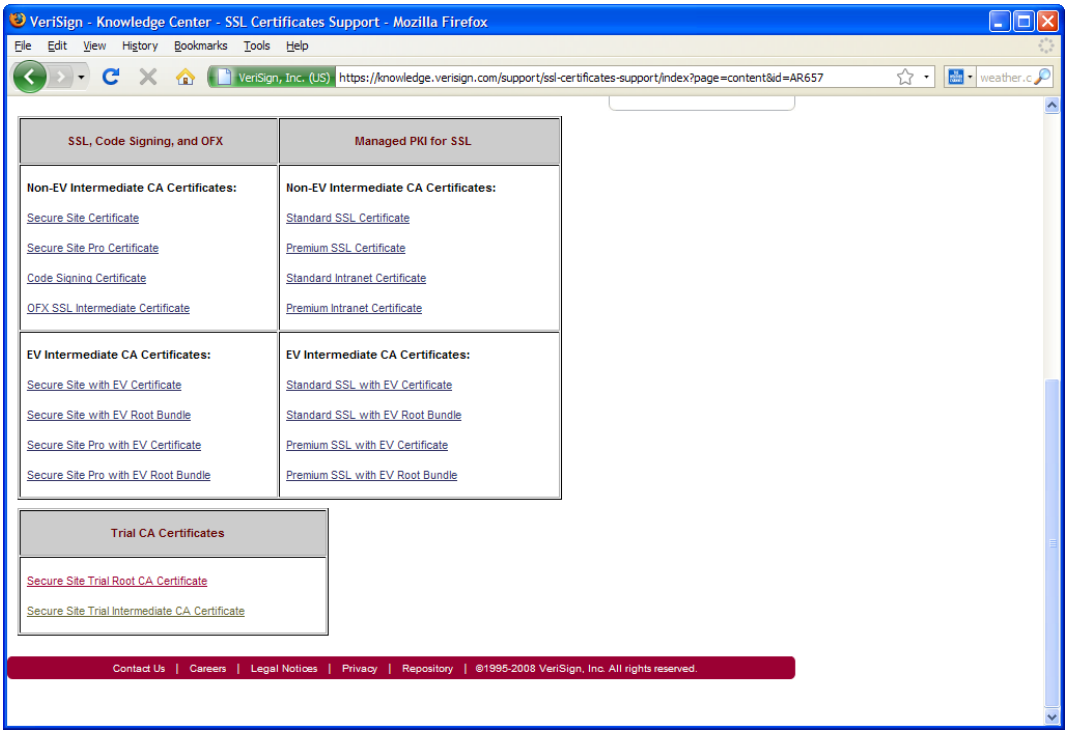
The Citrix NetScaler supports chaining of Certificates, and the use of Intermediate CA certificates. As of the time of the writing of this guide, VeriSign released a statement that all VeriSign SSL Certificates issued after December 11, 2008 will be chained to offline Certificate Authority (CA) roots 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.

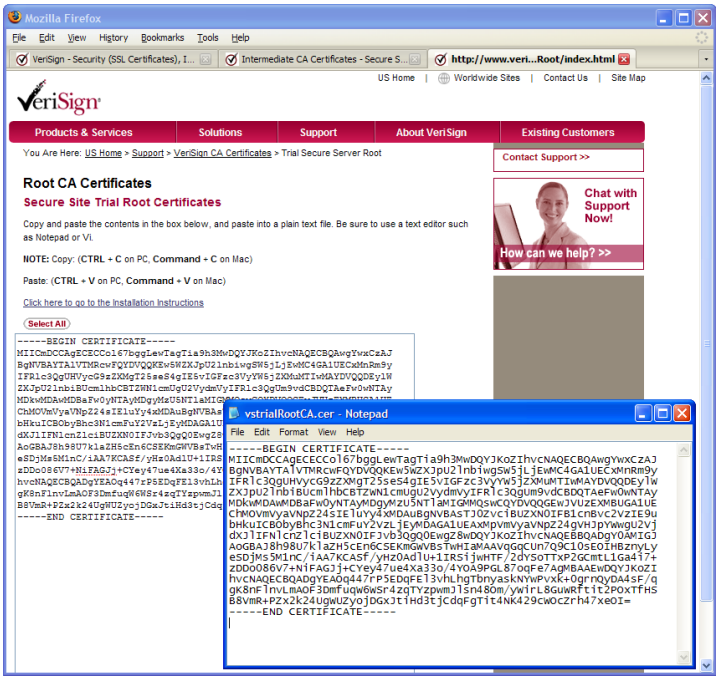
VeriSign, along with other Certificate Authorities, provide Trial Root CA and Trial Intermediate Root CA Certificates for use with the Trial Certificates that they issue. We will download the Trial Root CA and Trial Intermediate Root CA Certificates and save them for later use.

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

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

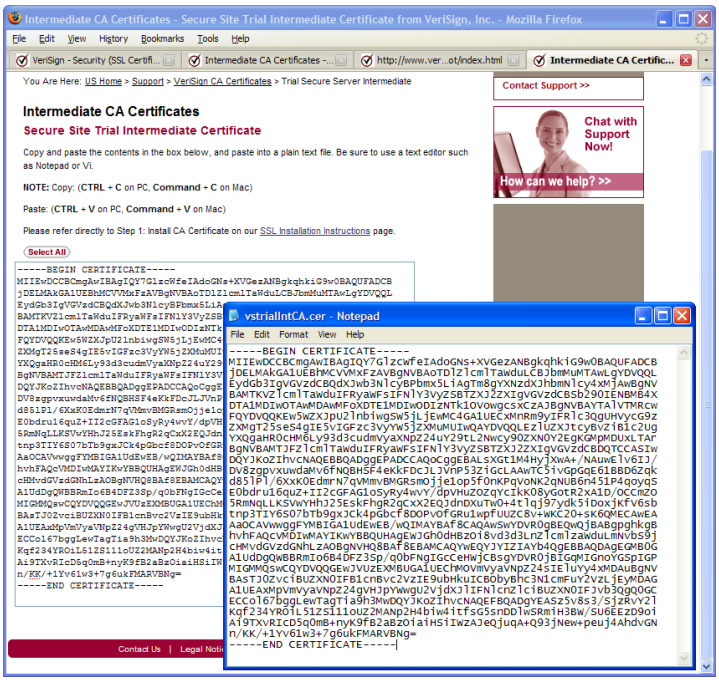
Navigate to the VeriSign website, Where the Trial CA Certificates are located.





Open, copy, paste and save the Trial Root CA Certificate to the local computer.

ex:vstrialRootCA.cer



Open, copy, paste and save the Trial Intermediate CA Certificate to the local computer.

ex: vstrialIntCA.cer

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

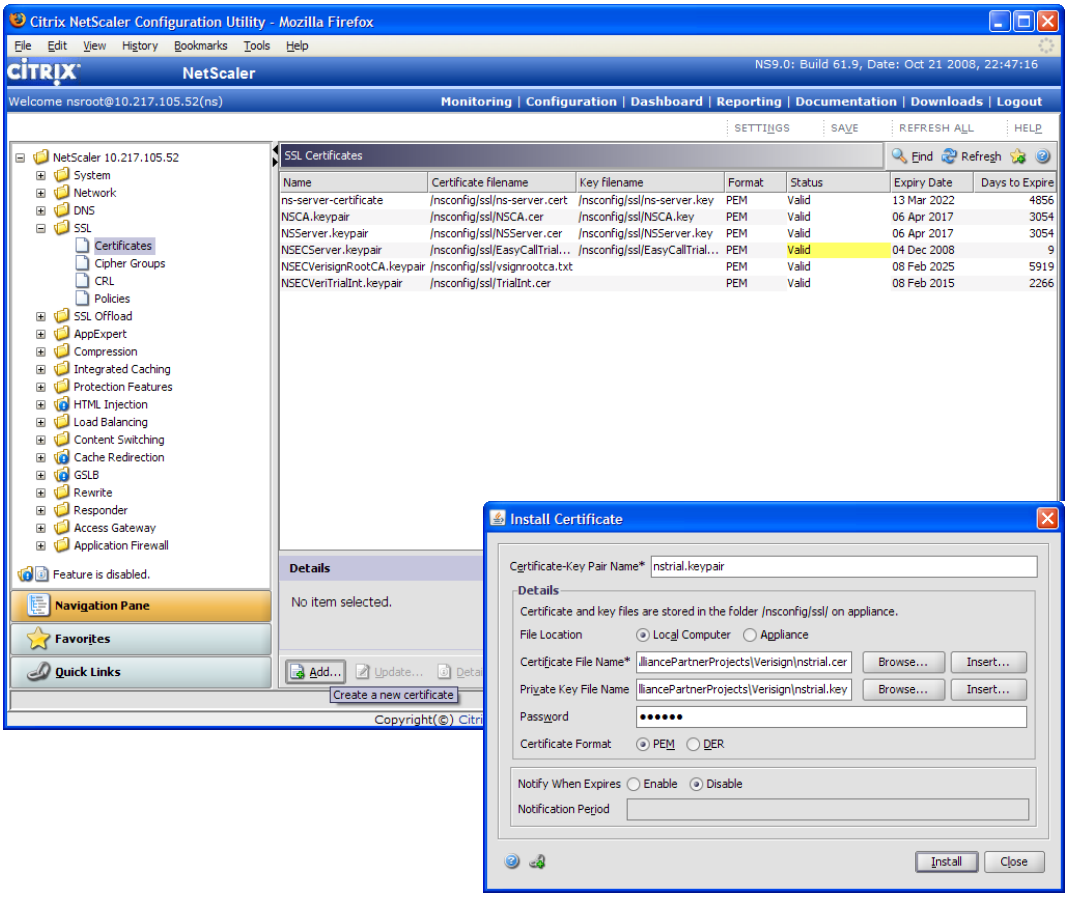
Certificate File Name:
- <Browse>
- Select filename NetScaler Trial Certificate was saved to in previous step. ex: nstrial.cer.

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.

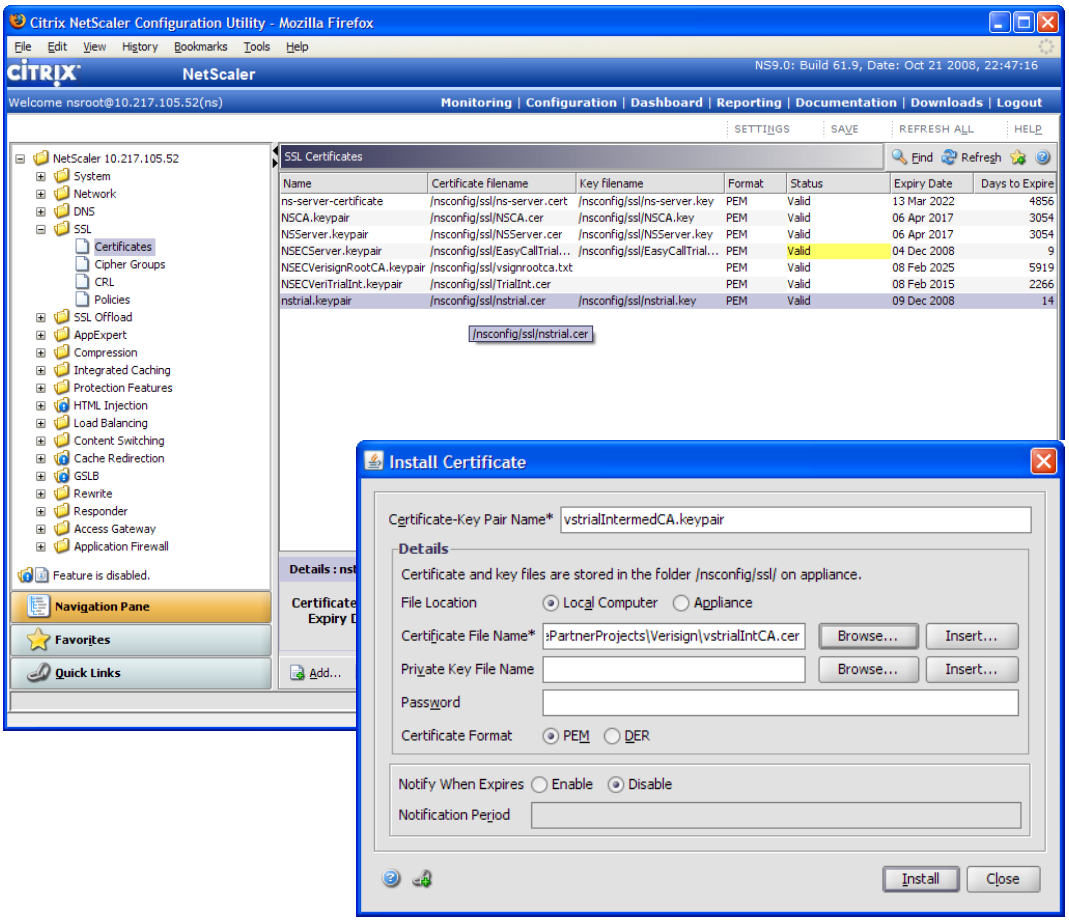
Certificate Format:
- PEM

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.



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.

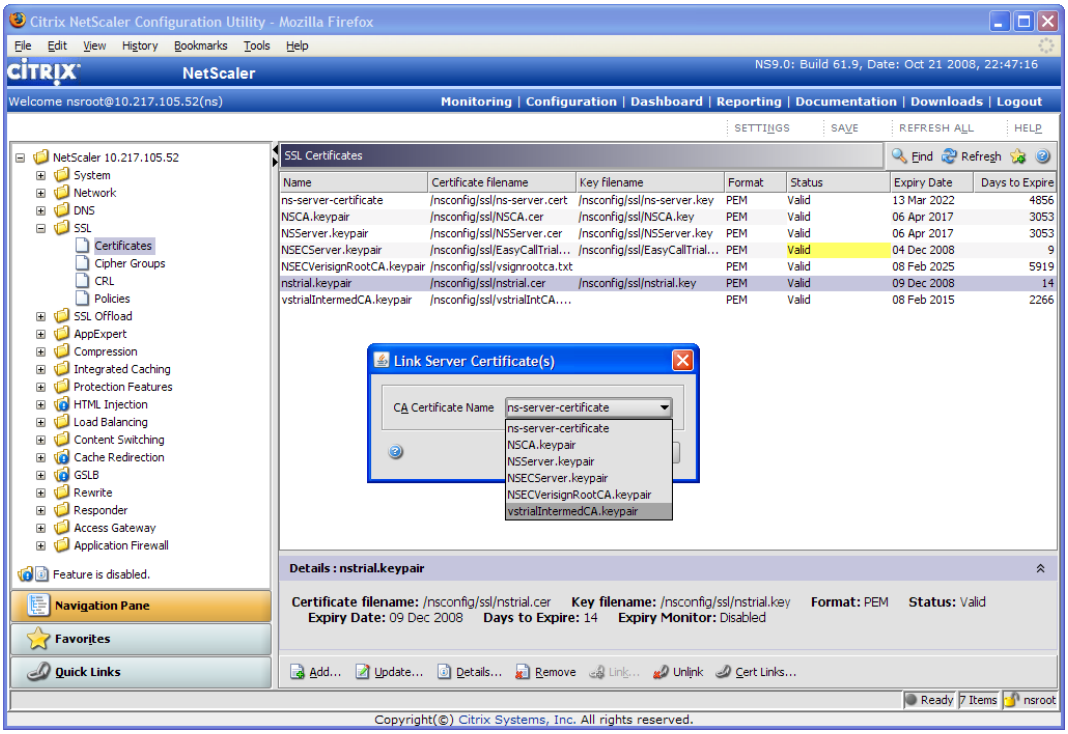
From the NetScaler GUI, select NetScaler ➥ SSL ➥ Certificates.

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

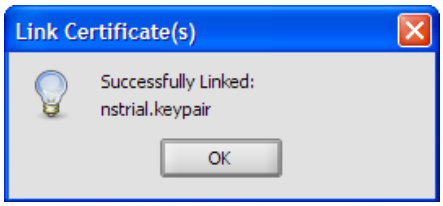
Select “Link”.

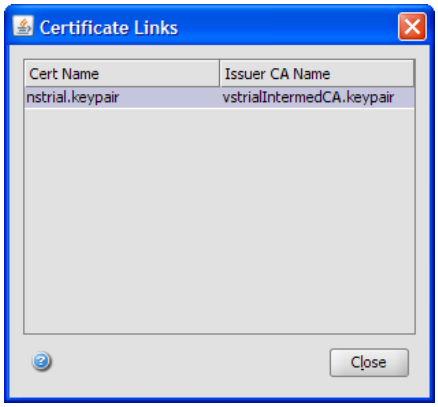
Select the VeriSign Intermediate CA Certificate that was previously installed from the drop down menu.

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.

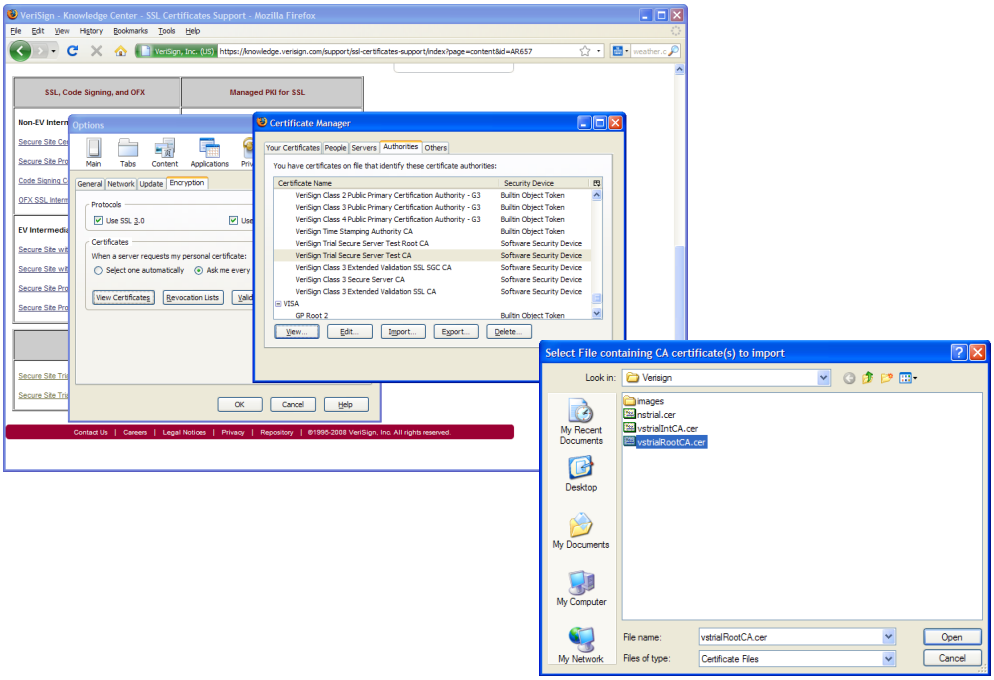
Importing Client (Browser) Certificates

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.

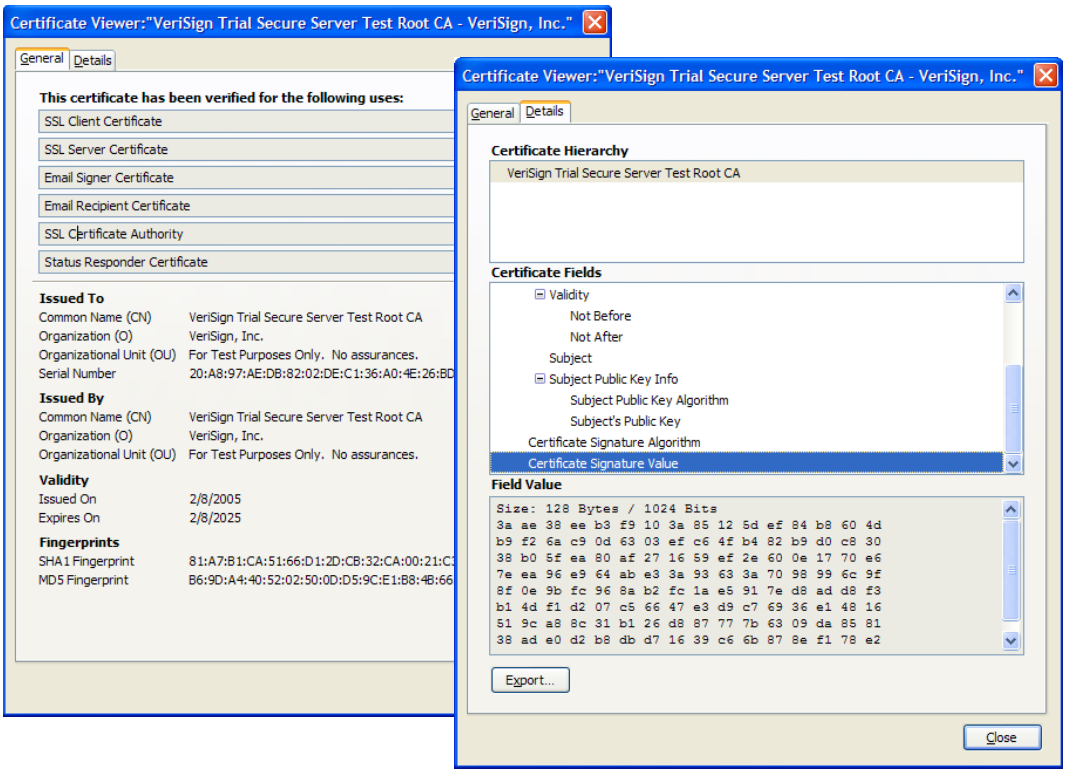
Verifying Certificate Chain in Client browser - Browser

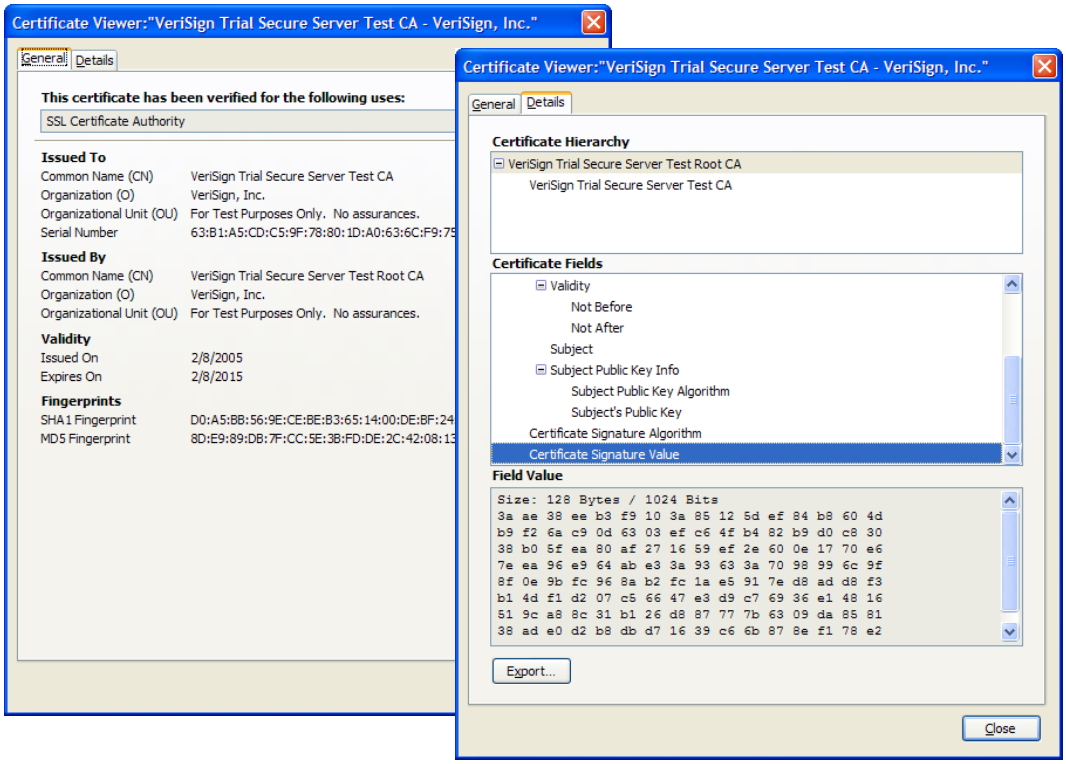
The VeriSign Root CA Certificate and the VeriSign Intermediate CA Certificate must be installed in the clients browser correctly. Always confirm the Certificates were imported correctly.

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.

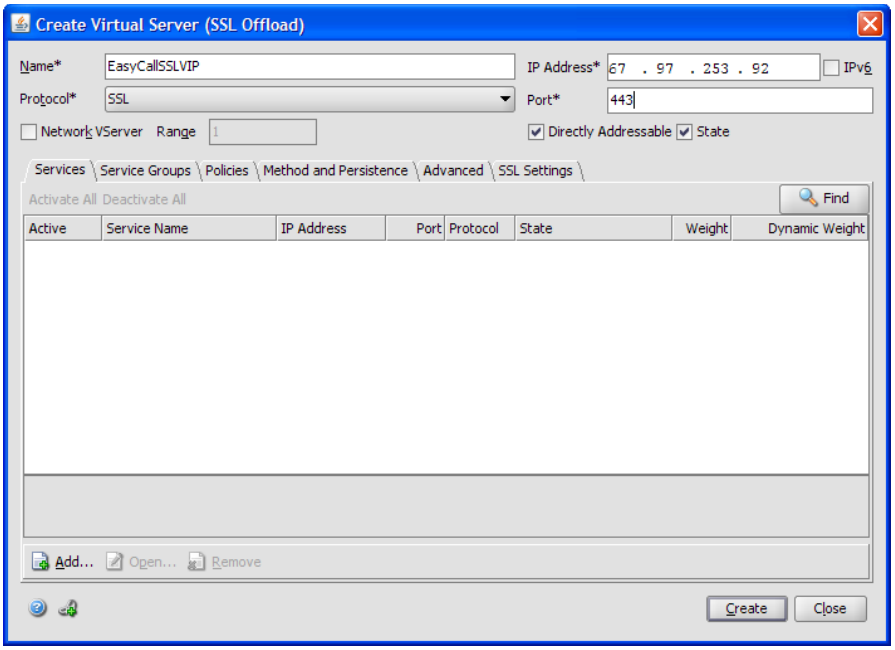




Citrix NetScaler SSL Offload Configuration

SSL Offload Configuration - NetScaler

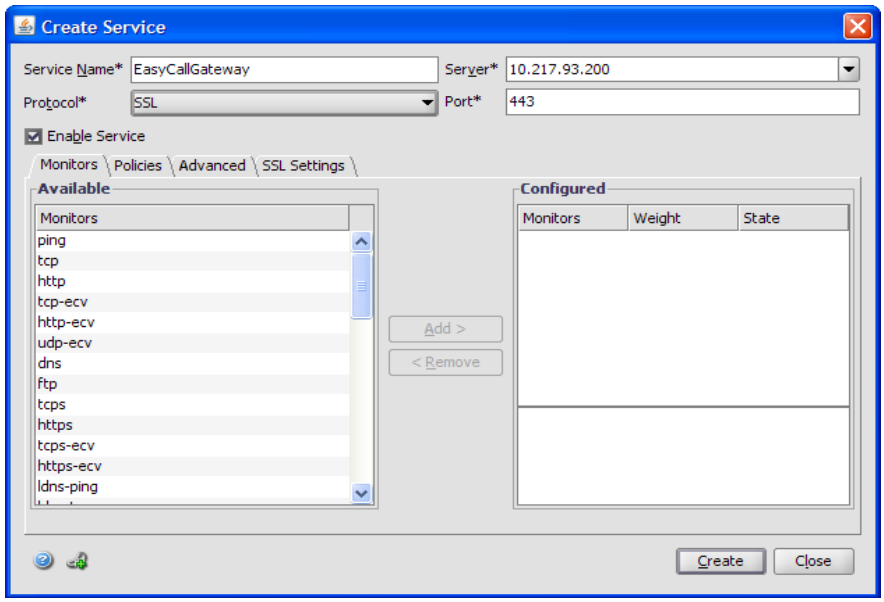
The Citrix NetScaler Application Switch will be configured for HTTPS on a public IP Address and then send the traffic to a backend server on the private network.



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.

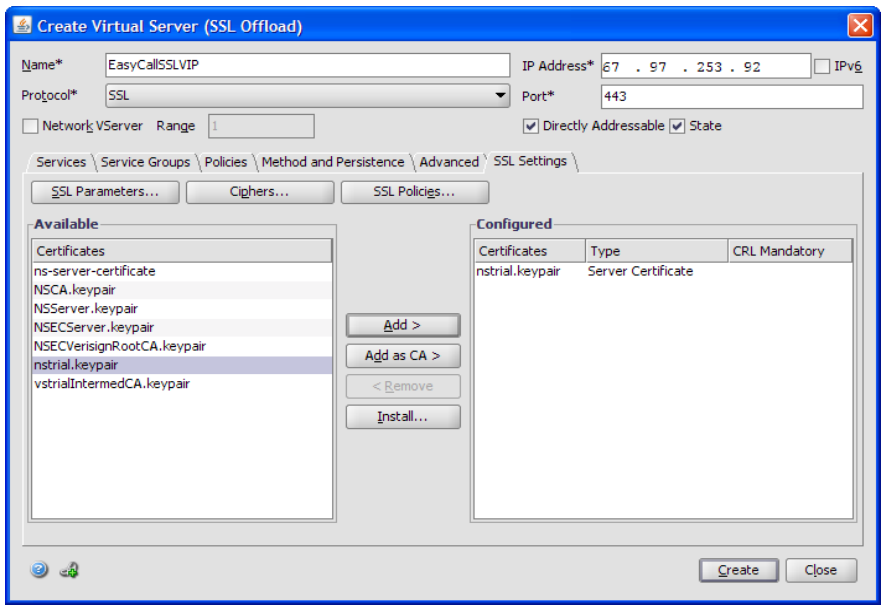


Select the SSL Settings tab.

Add the nstrial.keypair as a Server certificate.

Click on ‘Create’, ‘Close’.

The NetScaler SSL Connection is ready for use.

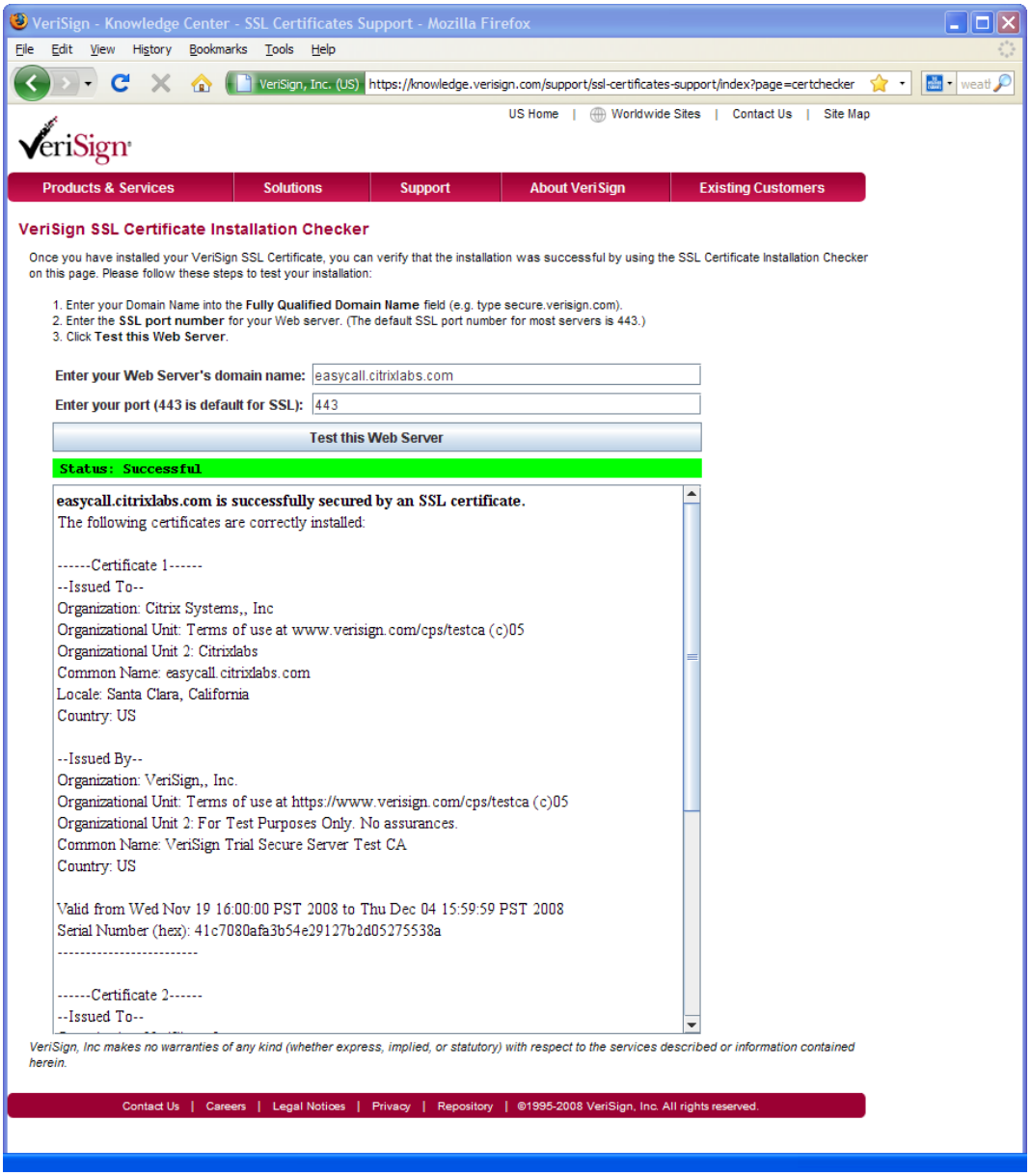


Testing the Client to NetScaler Certificate Chain

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



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

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.