Deployment Guide

Citrix EasyCall Conferencing
Citrix NetScaler - Content Filter

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.

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.

Table of Contents

Introduction

Citrix® NetScaler® optimizes the delivery of web applications — increasing security and improving performance and Web server capacity. This approach ensures the best total cost of ownership (TCO), security, availability, and performance for Web applications. The Citrix NetScaler solution is a comprehensive network system that combines high-speed load balancing and content switching with state-of-the-art application acceleration, layer 4-7 traffic management, data compression, dynamic content caching, SSL acceleration, network optimization, and robust application security into a single, tightly integrated solution. Deployed in front of application servers, the system significantly reduces processing overhead on application and database servers, reducing hardware and bandwidth costs.

The EasyCall Gateway is an easy to implement and manage solution that communication-enables enterprise applications. The EasyCall Gateway appliance is deployed as an adjunct to the corporate telephone system and the Citrix Delivery Center. The EasyCall client software is installed, published or streamed to user desktops to communication-enable installed, published, or streamed applications.

Alternatively, the EasyCall Web Services API can be used to communication enable web applications, accelerated by Netscaler.

The EasyCall Agent enables a user to call any phone number displayed in published, streamed, or installed Windows applications without dialing the number. The user simply hovers the mouse pointer over telephone numbers in application windows and then clicks a button to start the call from any telephone (office, mobile, home, and so on).

EasyCall Conferencing, which is a feature of EasyCall, allows EasyCall users to quickly set up ad-hoc conferences by sending participants an EasyCall Conferencing URL. Participants join a conference call simply by clicking a URL instead of having to dial a conference phone number and complex access codes. The calls are hosted on the EasyCall Gateway, providing toll-free access at much lower cost than commercial audio conference services.

To enable external users to join EasyCall Conferences, join requests must be proxied to the EasyCall Gateway from the internet as the EasyCall Gateway is always installed inside the corporate firewall. This is similar to many web applications that require protected external access, and the HTTPS proxy is simple to configure on the Citrix Netscaler to provide the necessary SSL Offloading and Content Filtering.

The Citrix NetScaler System provides continuous service availability through application-level protection by blocking attacks and delivery of applications securely. The Citrix NetScaler Content filtering prevents unwanted requests from reaching the protected server. The system can either drop a suspicious request or send an error page.

In this deployment guide we describe how to configure the Citrix NetScaler as a Content filter for the EasyCall Gateway in the DMZ so that internal users can create conference calls with EasyCall Conferencing, and external users can connect to and participate in the EasyCall Conference calls.

Solution Requirements

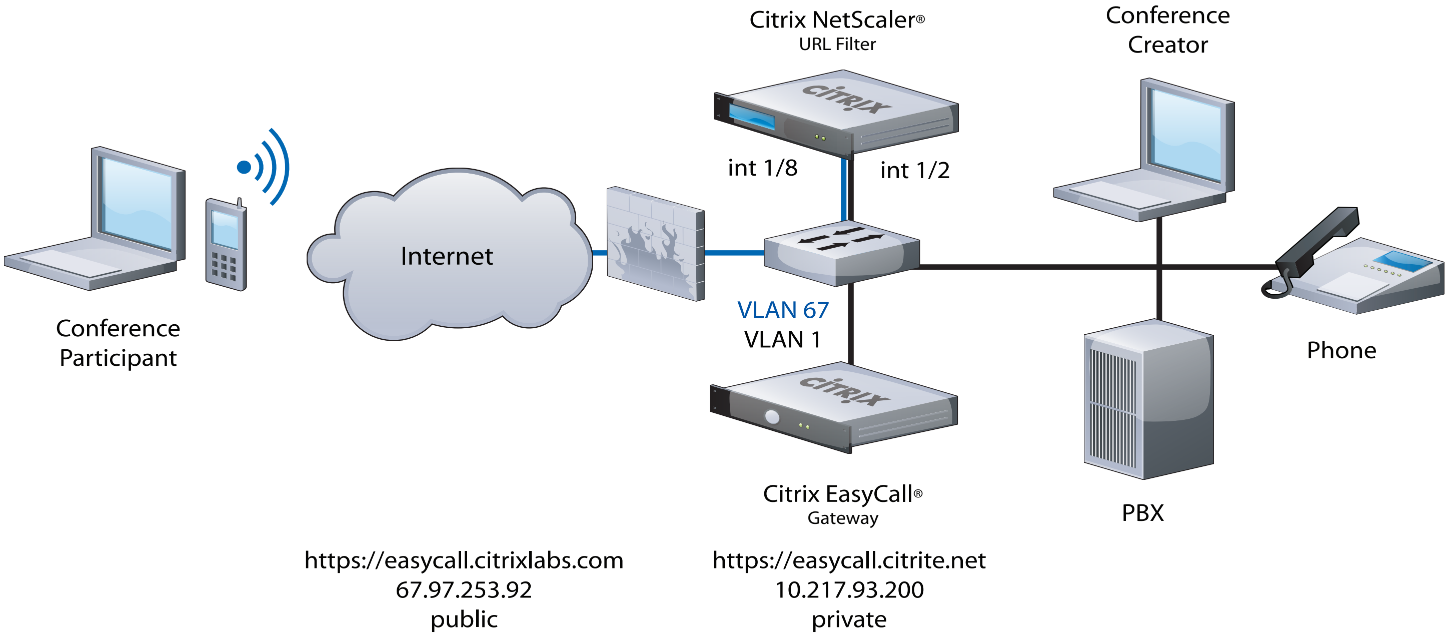
- SSL Offload, HTTPS Proxy
- Content Filter
- EasyCall Conferencing

Prerequisites

- Citrix NetScaler L4/7 Application Switch, running version 9.0+ (Quantity x 2 for HA)
- EasyCall Gateway 2.0+
- EasyCall Client Software 2.0+
- 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.



VLAN Legend	NetScaler	EasyCall Gateway
🟦 VLAN 67 ⬛ VLAN 1	VLAN 1: Interface 1/2, Untagged NSIP: 10.217.105.52 / 24 SNIP: 10.217.105.53 / 24 VLAN 67: Interface 1/8, Untagged VIP: 67.97.253.92 / 24	VLAN 1: 10.217.93.200

Obtaining a Certificate from a Certificate Authority

Creating a Private Key

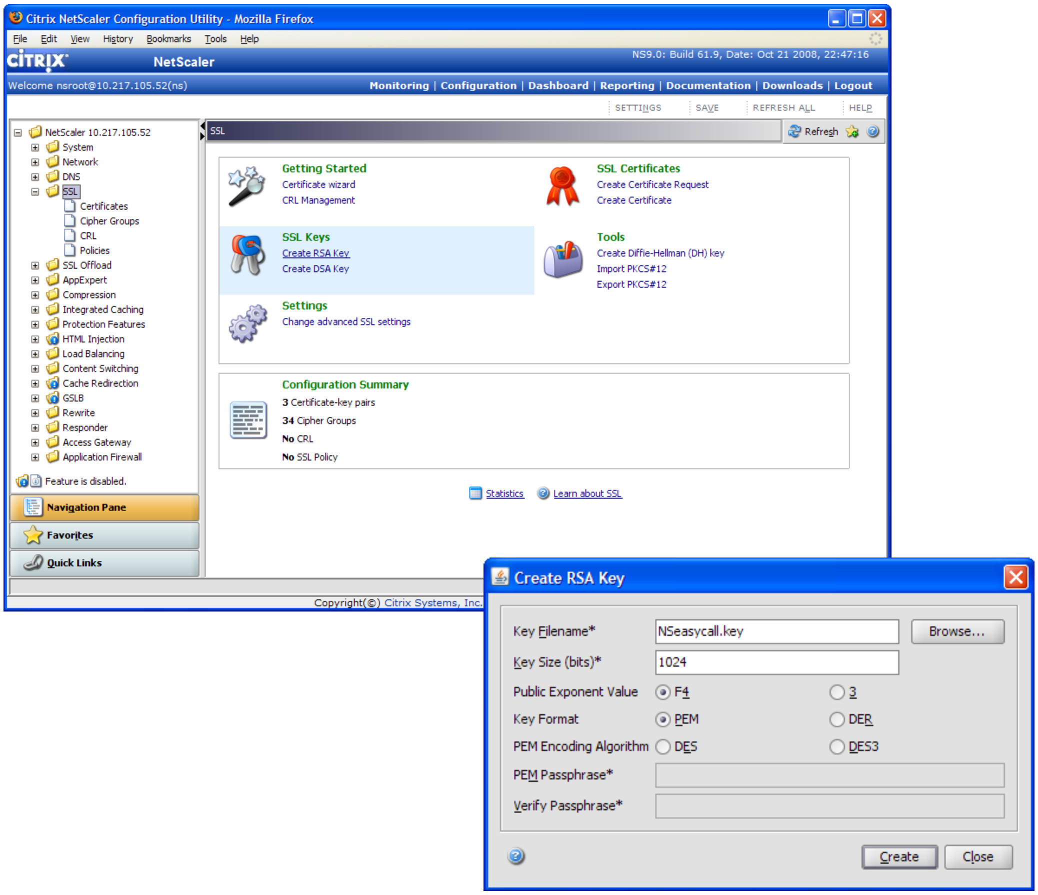
To obtain an SSL certificate from an authorized certificate authority (CA), you must create a Certificate Signing Request (CSR) and submit it to the CA. The following procedures describe how to create a CSR that you can submit to a CA, such as Verisign, to obtain a valid certificate.

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’.

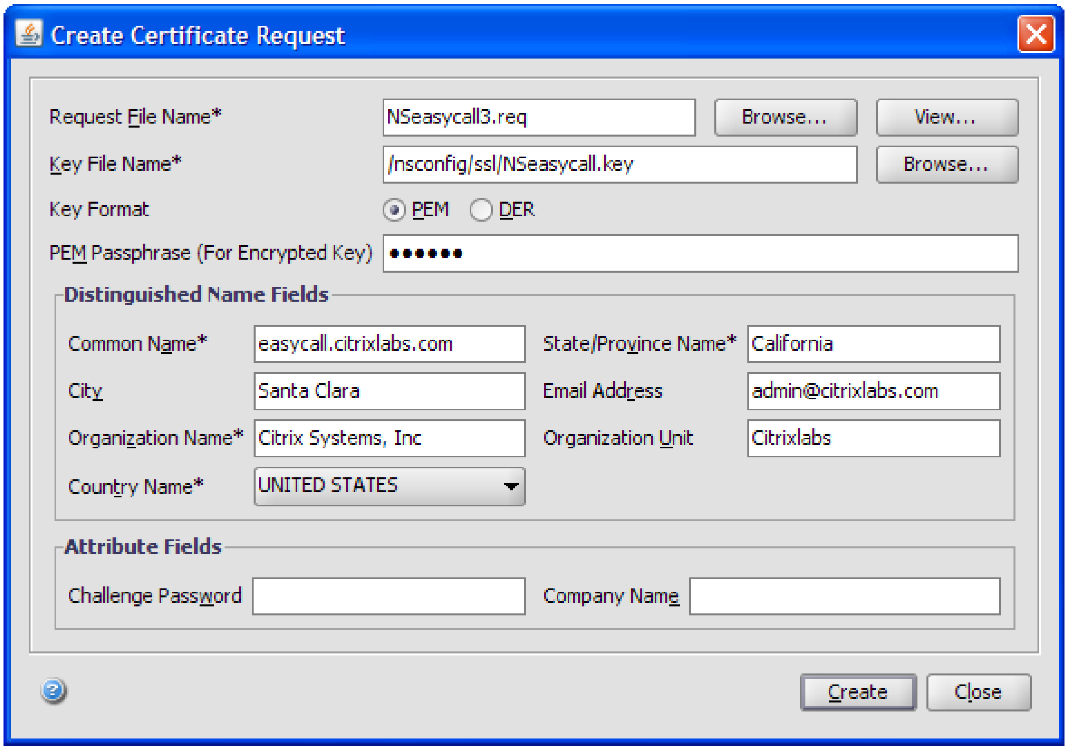


3 Certificate-key pairs
34 Cipher Groups
No CRL
No SSL Policy

Key Filename*	NSeasycall.key	
Key Size (bits)*	1024	
Public Exponent Value	● F4	○ 3
Key Format	● PEM	○ DER
PEM Encoding Algorithm	○ DES	○ DES3
PEM Passphrase*		
Verify Passphrase*		

Create a Certificate Signing Request

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.



Create Certificate Request

Request File Name*	NSeasycall3.req
Key File Name*	/nsconfig/ssl/NSeasycall.key
Key Format	● PEM ○ DER
PEM Passphrase (For Encrypted Key)	••••••

Distinguished Name Fields

Common Name*	easycall.citrixlabs.com	State/Province Name*	California
City	Santa Clara	Email Address	admin@citrixlabs.com
Organization Name*	Citrix Systems, Inc	Organization Unit	Citrixlabs
Country Name*	UNITED STATES		

Attribute Fields

Challenge Password		Company Name	

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.

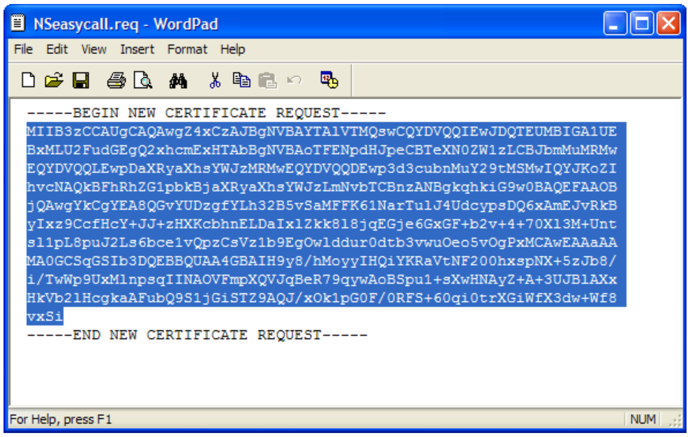
Submit CSR to Certificate Authority

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

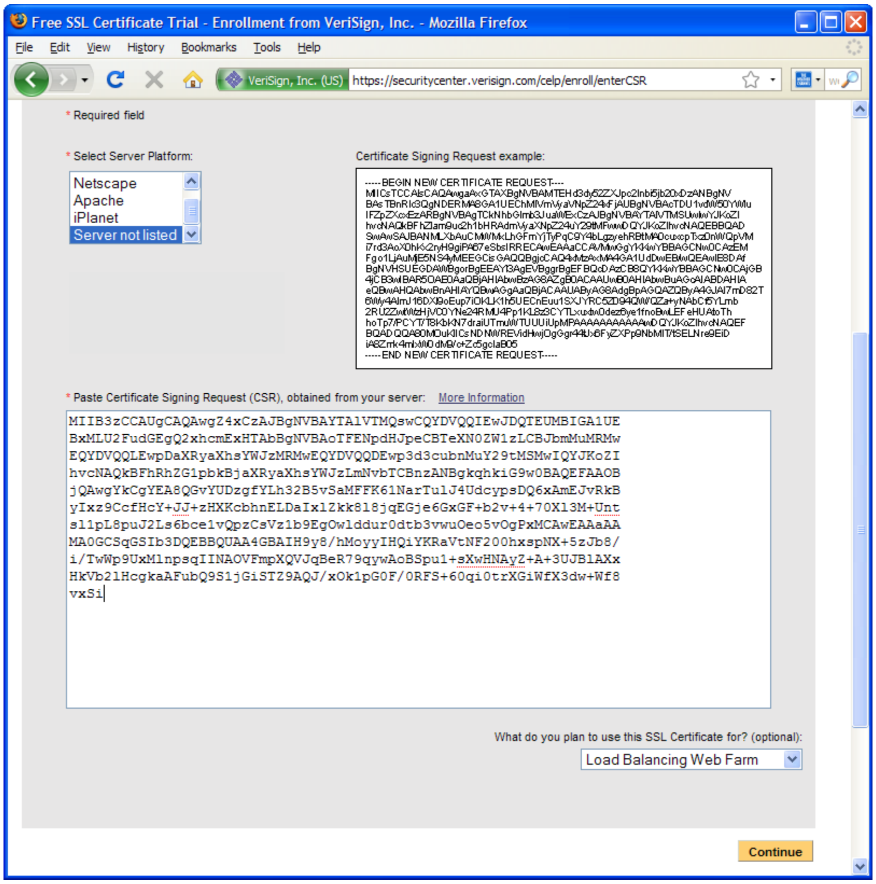
Open the CSR file on the local computer.

Copy the entire contents of the file.

Paste it into the CSR form on the Certificate Authorities website.



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIB3zCCAUgCAQAwgZ4xCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEUMBIGA1UE
BxMLU2FudGEgQ2xhcmExHTAbBgNVBAoTFENpdHJpeCBTeXN0ZW1zLCBJbmMuMRMw
EQYDVQQLEwpDaXRyaXhsYWJzMRMwEQYDVQQDEwp3d3cubnMuY29tMSMwIQYJKoZI
hvcNAQkBFhRhZG1pbkBjaXRyaXhsYWJzLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOB
jQAwgYkCgYEA8QGvYUDzgfYLh32B5vSaMFFK61NarTulJ4UdcypsDQ6xAmEJvRkB
yIxz9CcfHcY+JJ+zHXKcbhnELDaIxlZkk8l8jqEGje6GxGF+b2v+4+70Xl3M+Unt
sl1pL8puJ2Ls6bce1vQpzCsVz1b9EgOwlddur0dtb3vwuOeo5vOgPxMCAwEAAaAA
MA0GCSqGSIb3DQEBBQUAA4GBAIH9y8/hMoyyIHQiYKRaVtNF200hxspNX+5zJb8/
i/TwWp9UxMlnpsqIINAOVFmpXQVJqBeR79qywAoBSpu1+sXwHNAyZ+A+3UJBlAXx
HkVb2lHcgkaAFubQ9S1jGiSTZ9AQJ/xOk1pG0F/0RFS+60qi0trXGiWfX3dw+Wf8
vxSi
-----END NEW CERTIFICATE REQUEST-----
```


Free SSL Certificate Trial - Enrollment from VeriSign, Inc. - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
VeriSign, Inc. (US)

https://securitycenter.verisign.com/celp/enroll/enterCSR

* Required field

* Select Server Platform:

- Netscape
- Apache
- iPlanet
- Server not listed

Certificate Signing Request example:

```
-----BEGIN NEW CERTIFICATE REQUEST----
MIICsTCCAbsCAQAwgaAxGTAXBgNVBAMTEHd3dy52ZXJpc2lnbi5jb20xDzANBgNV
BAsTBnRlc3QgNDERMA8GA1UEChMIVmVyaVNpZ24xFjAUBgNVBAcTDU1vdW50YWlu
IFZpZXcxEzARBgNVBAgTCkNhbGlmb3JuaWExCzAJBgNVBAYTAlVTMSUwIwYJKoZI
hvcNAQkBFhZlam9uc2h1bHRAdmVyaXNpZ24uY29tMFwwDQYJKoZIhvcNAQEBBQAD
SwAwSAJBANMLXbAuCMWMkLhGFmYjTyPqC9Y4bLgzyehRBtMA0cuxcpTxz0nWQpVM
i7rd3AoXDhKx2nyH9giPA67eSbsIRRECAwEAAaCCAVMwGgYKKwYBBAGCNw0CAzEM
Fgo1LjAuMjE5NS4yMEEGCisGAQQBgjcCAQ4xMzAxMA4GA1UdDwEBwQEAwIB8DAf
BgNVHSUEGDAWBgorBgEEAYI3AgEVBggrBgEFBQcDAzCB8QYKKwYBBAGCNw0CAjGB
4jCB3wIBAR5OAB0AaQBjAHIAbwBzAG8AZgB0ACAAUwB0AHIAbwBuAGcAIABDAHIA
eQBwAHQAbwBnAHIAYQBwAGgAaQBjACAAUAByAG8AdgBpAGQAZQByA4GJAI7mD82T
6Wy4AlmJ16DXl9oEup7iOKLK1h5UECnEuu1SXJYRC5ZD94QWQZa+yNAbCf5YLmb
2RU2ZwWzHjVC0YNe24RMU4Pp1KL8z3CYTLxuxdw0dez6ye1fnoBwLEFeHUAtoTh
hoTp7/PCYT/T8KbKN7draiUTmuW/TUUUiUpMPAAAAAAAAAAAwDQYJKoZIhvcNAQEF
BQADQQA80MDuKIICsNDNWREVidHwjOgGgr44tUx6FyZXPp9NbMIT/tSELNre9EiD
iA8Zmk4mlxW0dMB/c+Zc5gclaB05
-----END NEW CERTIFICATE REQUEST----
```

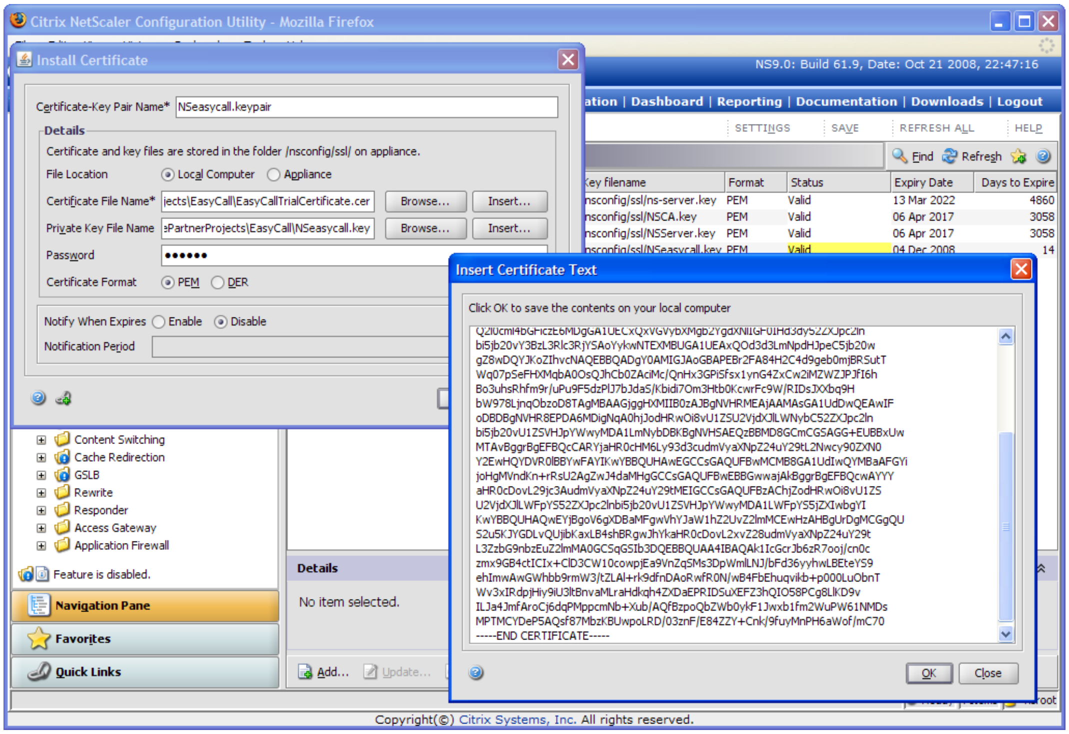
* Paste Certificate Signing Request (CSR), obtained from your server: More Information

```
MIIB3zCCAUgCAQAwgZ4xCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEUMBIGA1UE
BxMLU2FudGEgQ2xhcmExHTAbBgNVBAoTFENpdHJpeCBTeXN0ZW1zLCBJbmMuMRMw
EQYDVQQLEwpDaXRyaXhsYWJzMRMwEQYDVQQDEwp3d3cubnMuY29tMSMwIQYJKoZI
hvcNAQkBFhRhZG1pbkBjaXRyaXhsYWJzLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOB
jQAwgYkCgYEA8QGvYUDzgfYLh32B5vSaMFFK61NarTulJ4UdcypsDQ6xAmEJvRkB
yIxz9CcfHcY+JJ+zHXKcbhnELDaIxlZkk8l8jqEGje6GxGF+b2v+4+70Xl3M+Unt
sl1pL8puJ2Ls6bce1vQpzCsVz1b9EgOwlddur0dtb3vwuOeo5vOgPxMCAwEAAaAA
MA0GCSqGSIb3DQEBBQUAA4GBAIH9y8/hMoyyIHQiYKRaVtNF200hxspNX+5zJb8/
i/TwWp9UxMlnpsqIINAOVFmpXQVJqBeR79qywAoBSpu1+sXwHNAyZ+A+3UJBlAXx
HkVb2lHcgkaAFubQ9S1jGiSTZ9AQJ/xOk1pG0F/0RFS+60qi0trXGiWfX3dw+Wf8
vxSi
```

What do you plan to use this SSL Certificate for? (optional): Load Balancing Web Farm

Installing NetScaler Certificate From Certificate Authority

When you receive the Certificate, signed by the Certificate Authority, there will be some text that starts with “BEGIN CERTIFICATE” and ends with “END CERTIFICATE”. Highlight this text, including the BEGIN and END lines and copy to the clipboard. We will use this to create a Certificate on the NetScaler.



Install Certificate

Certificate-Key Pair Name* NSeasycall.keypair

Details

Certificate and key files are stored in the folder /nsconfig/ssl/ on appliance.

File Location ● Local Computer ○ Appliance

Certificate File Name* jects\EasyCall\EasyCallTrialCertificate.cer Browse... Insert...

Private Key File Name :PartnerProjects\EasyCall\NSeasycall.key Browse... Insert...

Password ●●●●●●

Certificate Format ● PEM ○ DER

Notify When Expires ○ Enable ● Disable

Notification Period

Key filename	Format	Status	Expiry Date	Days to Expire
nsconfig/ssl/ns-server.key	PEM	Valid	13 Mar 2022	4860
nsconfig/ssl/NSCA.key	PEM	Valid	06 Apr 2017	3058
nsconfig/ssl/NSServer.key	PEM	Valid	06 Apr 2017	3058
nsconfig/ssl/NSeasycall.key	PEM	Valid	04 Dec 2008	14

Feature is disabled.

Details

No item selected.

Insert Certificate Text

Click OK to save the contents on your local computer

```
Q2l0cml4bGFiczE6MDgGA1UECxQxVGVybXMgb2YgdXNlIGF0IHd3dy52ZXJpc2ln
bi5jb20vY3BzL3Rlc3RjYSAoYykwNTEXMBUGA1UEAxQOd3d3LmNpdHJpeC5jb20w
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAPEBr2FA84H2C4d9geb0mjBRSutT
Wq07pSeFHXMqbA0OsQJhCb0ZAciMc/QnHx3GPiSfsx1ynG4ZxCw2iMZWZJPJfI6h
Bo3uhsRhfm9r/uPu9F5dzPlJ7bJdaS/Kbidi7Om3Htb0KcwrFc9W/RIDsJXXbq9H
bW978LjnqObzoD8TAgMBAAGjggHXMIIB0zAJBgNVHRMEAjAAMAsGA1UdDwQEAwIF
oDBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vU1ZSU2VjdXJlLWNybC52ZXJpc2ln
bi5jb20vU1ZSVHJpYWwyMDA1LmNybDBKBgNVHSAEQzBBMD8GCmCGSAGG+EUBBxUw
MTAvBggrBgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0
Y2EwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMB8GA1UdIwQYMBaAFGYi
joHgMVndKn+rRsU2AgZwJ4daMHgGCCsGAQUFBwEBBGwwajAkBggrBgEFBQcwAYYY
aHR0cDovL29jc3AudmVyaXNpZ24uY29tMEIGCCsGAQUFBzAChjZodHRwOi8vU1ZS
U2VjdXJlLWFpYS52ZXJpc2lnbi5jb20vU1ZSVHJpYWwyMDA1LWFpYS5jZXIwbgYI
KwYBBQUHAQwEYjBgoV6gXDBaMFgwVhYJaW1hZ2UvZ2lmMCEwHzAHBgUrDgMCGgQU
S2u5KJYGDLvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNpZ24uY29t
L3ZzbG9nbzEuZ2lmMA0GCSqGSIb3DQEBBQUAA4IBAQAk1IcGcrJb6zR7ooj/cn0c
zmx9GB4ctICIx+ClD3CW10cowpjEa9VnZqSMs3DpWmlLNJ/bFd36yyhwLBEteYS9
ehImwAwGWhbb9rmW3/tZLAl+rk9dfnDAoRwfR0N/wB4FbEhuqvikb+p000LuObnT
Wv3xIRdpjHiy9iU3ltBnvaMLraHdkqh4ZXDaEPRIDSuXEFZ3hQIO58PCg8LlKD9v
ILJa4JmfAroCj6dqPMppcmNb+Xub/AQfBzpoQbZWb0ykF1Jwxb1fm2WuPW61NMDs
MPTMCYDeP5AQsf87MbzKBUwpoLRD/03znF/E84ZZY+Cnk/9fuyMnPH6aWof/mC70
-----END CERTIFICATE-----
```

OK Close

Copyright(©) Citrix Systems, Inc. All rights reserved.

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:

- <Insert>
- Paste Certificate from file or clipboard.

Private Key File Name:

- Copy the private key from the NetScaler to the Local Computer. (Used to create the Certificate Signing Request)
- <Browse> and select the private key.

Password:

- Type in a password to encrypt the certificate.

Certificate Format:

- PEM

Click ‘Install’.

Installing Intermediate CA Certificate

Some Certificate Authorities require that you install an Intermediate CA Certificate to be sent with the Signed Certificate.

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:

- <Insert>
- Paste Intermediate CA Certificate.

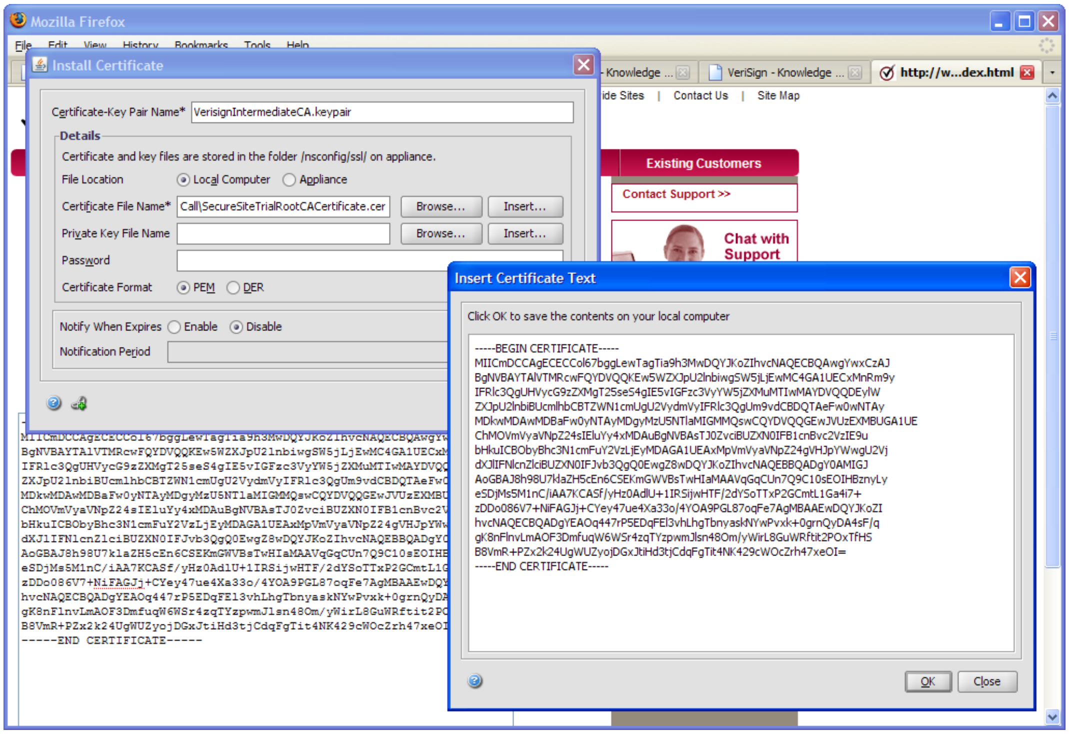
Private Key File Name:

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

Certificate Format:

- PEM

Click ‘Install’.



Install Certificate

Certificate-Key Pair Name* VerisignIntermediateCA.keypair

Details

Certificate and key files are stored in the folder /nsconfig/ssl/ on appliance.

File Location ● Local Computer ○ Appliance

Certificate File Name* Call\SecureSiteTrialRootCACertificate.cer

Private Key File Name

Password

Certificate Format ● PEM ○ DER

Notify When Expires ○ Enable ● Disable

Notification Period

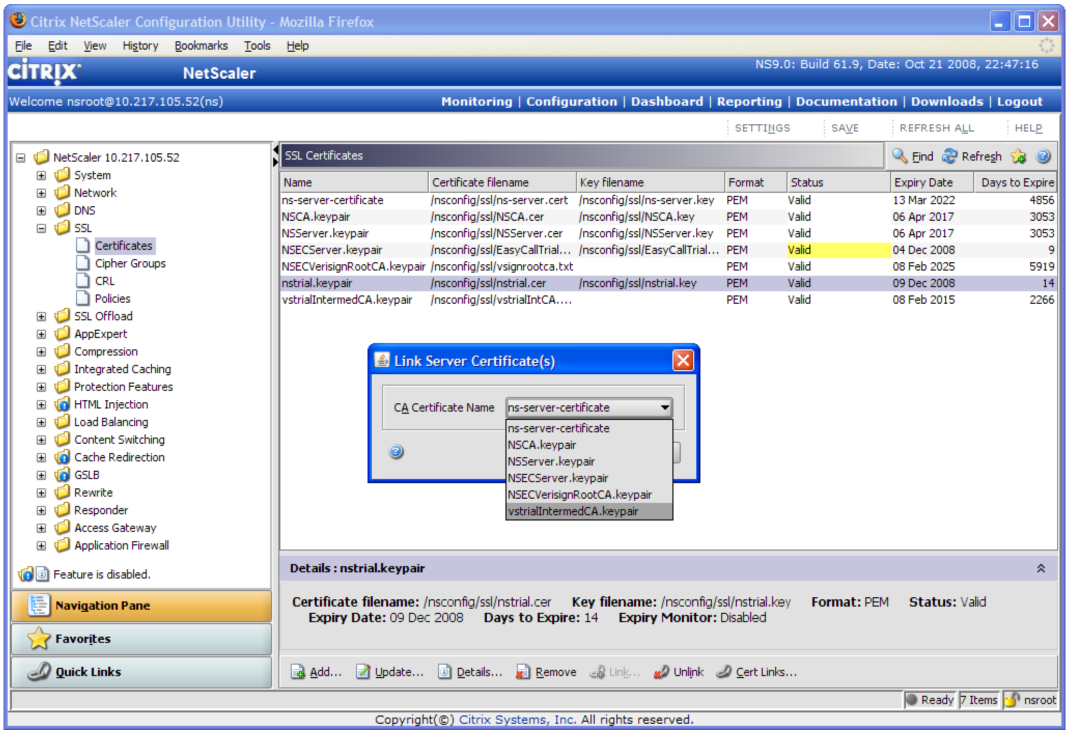
Insert Certificate Text

Click OK to save the contents on your local computer

```
-----BEGIN CERTIFICATE-----
MIICmDCCAgECECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQECBQAwgYwxCzAJ
BgNVBAYTAlVTMRcwFQYDVQQKEw5WZXJpU2lnbiwgSW5jLjEwMC4GA1UECxMnRm9y
IFRlc3QgUHVycG9zZXMgT25seS4gIE5vIGFzc3VyYW5jZXMuMTIwMAYDVQQDEylW
ZXJpU2lnbiBUcmlhbCBTZWN1cmUgU2VydmVyIFRlc3QgUm9vdCBDQTAeFw0wNTAy
MDkwMDAwMDBaFw0yNTAyMDgyMzU5NTlaMIGMMQswCQYDVQQGEwJVUzEXMBUGA1UE
ChMOVmVyaVNpZ24sIEluYy4xMDAuBgNVBAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9u
bHkuICBObyBhc3N1cmFuY2VzLjEyMDAGA1UEAxMpVmVyaVNpZ24gVHJpYWwgU2Vj
dXJlIFNlcnZlciBUZXN0IFJvb3QgQ0EwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAJ8h98U7klaZH5cEn6CSEKmGWVBsTwHIaMAAVqGqCUn7Q9C10sEOIHBznyLy
eSDjMs5M1nC/iAA7KCASf/yHz0AdlU+1IRSijwHTF/2dYSoTTxP2GCmtL1Ga4i7+
zDDo086V7+NiFAGJj+CYey47ue4Xa33o/4YOA9PGL87oqFe7AgMBAAEwDQYJKoZI
hvcNAQECBQADgYEAOq447rP5EDqFEl3vhLhgTbnyaskNYwPvxk+0grnQyDA4sF/q
gK8nFlnvLmAOF3DmfuqW6WSr4zqTYzpwmJlsn48Om/yWirL8GuWRftit2POxTfHS
B8VmR+PZx2k24UgWUZyojDGxJtiHd3tjCdqFgTit4NK429cWOcZrh47xeOI=
-----END CERTIFICATE-----
```

Linking Intermediate CA Certificate to NetScaler Signed Certificate

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


Citrix NetScaler Configuration Utility - Mozilla Firefox
File Edit View History Bookmarks Tools Help
CITRIX NetScaler
NS9.0: Build 61.9, Date: Oct 21 2008, 22:47:16
Welcome nsroot@10.217.105.52(ns)
Monitoring | Configuration | Dashboard | Reporting | Documentation | Downloads | Logout
SETTINGS SAVE REFRESH ALL HELP
NetScaler 10.217.105.52
System
Network
DNS
SSL
Certificates
Cipher Groups
CRL
Policies
SSL Offload
AppExpert
Compression
Integrated Caching
Protection Features
HTML Injection
Load Balancing
Content Switching
Cache Redirection
GSLB
Rewrite
Responder
Access Gateway
Application Firewall
Feature is disabled.
Navigation Pane
Favorites
Quick Links
SSL Certificates
Find Refresh
Link Server Certificate(s)
Add... Update... Details... Remove Link... Unlink Cert Links...
Ready 7 Items nsroot
Copyright(©) Citrix Systems, Inc. All rights reserved.

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	3053
NSServer.keypair	/nsconfig/ssl/NSServer.cer	/nsconfig/ssl/NSServer.key	PEM	Valid	06 Apr 2017	3053
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
nstrial.keypair	/nsconfig/ssl/nstrial.cer	/nsconfig/ssl/nstrial.key	PEM	Valid	09 Dec 2008	14
vstrialIntermedCA.keypair	/nsconfig/ssl/vstrialIntCA....		PEM	Valid	08 Feb 2015	2266

CA Certificate Name: ns-server-certificate

- ns-server-certificate
- NSCA.keypair
- NSServer.keypair
- NSECServer.keypair
- NSECVerisignRootCA.keypair
- vstrialIntermedCA.keypair

Details : nstrial.keypair

Certificate filename: /nsconfig/ssl/nstrial.cer **Key filename:** /nsconfig/ssl/nstrial.key **Format:** PEM **Status:** Valid
Expiry Date: 09 Dec 2008 **Days to Expire:** 14 **Expiry Monitor:** Disabled

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

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

Select “Link”.

Select the 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 EasyCall Conferencing AppExpert Template

Import and Public Endpoint Configuration

The EasyCall Conferencing AppExpert Template can be imported into the Citrix NetScaler Application Switch, and is pre-configured for Caching, Compression and Content Filtering. The EasyCall Conferencing AppExpert Template can be found on the Citrix Community Website:

http://community.citrix.com/display/ns/AppExpertTemplates

To Import the EasyCall Conferencing AppExpert Template, click on Application, select Import.

When importing a template, you will need to Add or Select the Public Endpoints.

In this example, we will add a new Public endpoint.

Name: EasyCallSSLVIP_pub

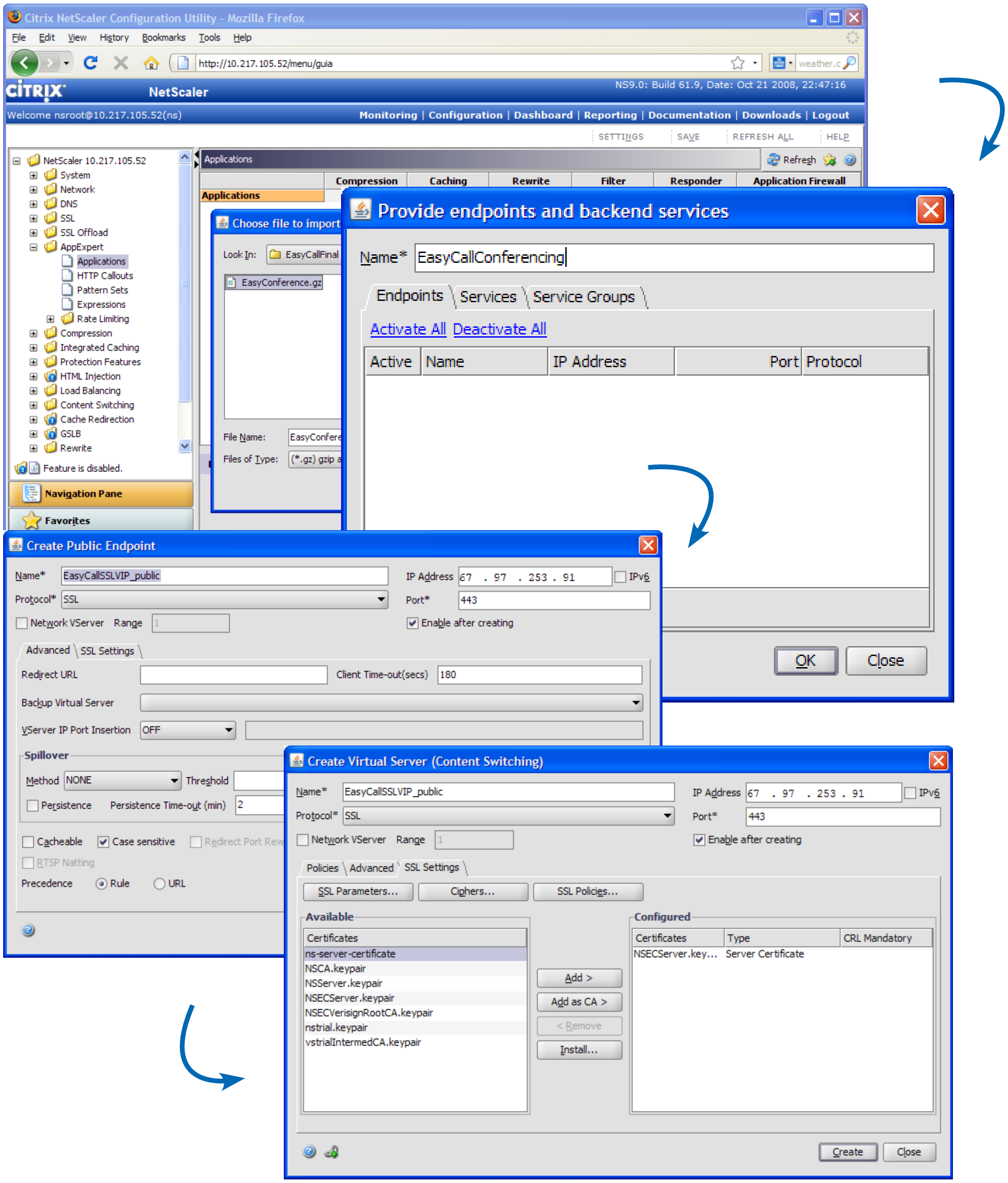
IP Address: 67.97.253.91

Protocol: SSL

Port: 443

'Add' the NetScaler Certificate that was signed by the Certificate Authority (or signed by the NetScaler).

Select 'Ok'.



Citrix NetScaler Configuration Utility - Mozilla Firefox

http://10.217.105.52/menu/guia

NS9.0: Build 61.9, Date: Oct 21 2008, 22:47:16

Welcome nsroot@10.217.105.52(ns)

Choose file to import

Look In: EasyCallFinal

EasyConference.gz

File Name: EasyConfere

Files of Type: (*.gz) gzip a

Provide endpoints and backend services

Name* EasyCallConferencing

Create Public Endpoint

Name* EasyCallSSLVIP_public

IP Address 67 . 97 . 253 . 91 □ IPv6

Protocol* SSL

Port* 443

□ Network VServer Range 1

☑ Enable after creating

Redirect URL

Client Time-out(secs) 180

Backup Virtual Server

VServer IP Port Insertion OFF

Spillover

Method NONE Threshold

□ Persistence Persistence Time-out (min) 2

□ Cacheable ☑ Case sensitive □ Redirect Port Rew

□ RTSP Natting

Precedence ● Rule ○ URL

Create Virtual Server (Content Switching)

Name* EasyCallSSLVIP_public

IP Address 67 . 97 . 253 . 91 □ IPv6

Protocol* SSL

Port* 443

□ Network VServer Range 1

☑ Enable after creating

Available

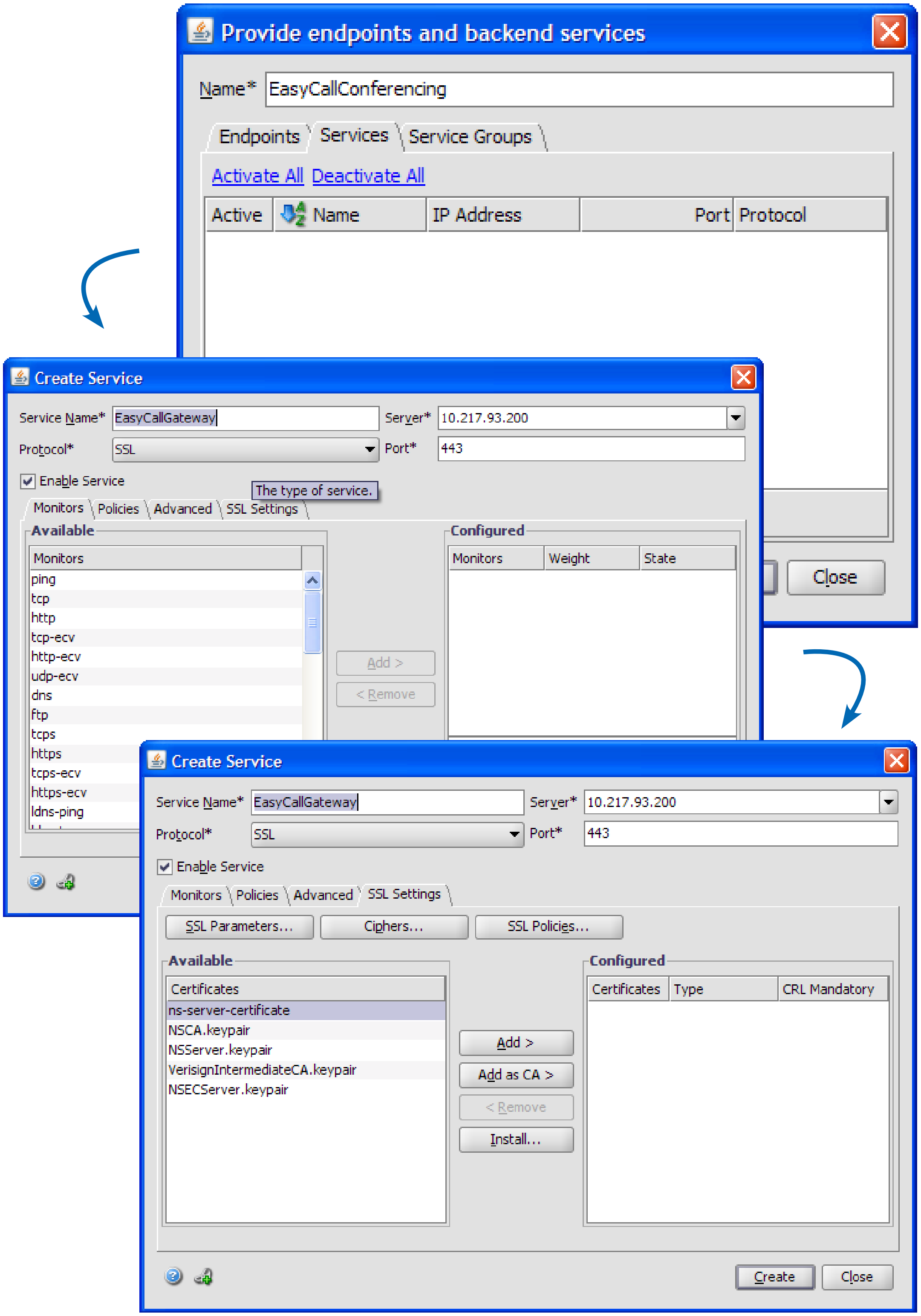
Certificates
ns-server-certificate
NSCA.keypair
NSServer.keypair
NSECServer.keypair
NSECVerisignRootCA.keypair
nstrial.keypair
vstrialIntermedCA.keypair

Configured

Certificates	Type	CRL Mandatory
NSECServer.key...	Server Certificate	

EasyCall Gateway Configuration

Enter the IP Address of the EasyCall Gateway on the internal private network.



Provide endpoints and backend services

Name* EasyCallConferencing

Active	Name	IP Address	Port	Protocol

Create Service

Service Name* EasyCallGateway

Server* 10.217.93.200

Protocol* SSL

Port* 443

☑ Enable Service

The type of service.

Available

Monitors
ping
tcp
http
tcp-ecv
http-ecv
udp-ecv
dns
ftp
tcps
https
tcps-ecv
https-ecv
ldns-ping

Configured

Monitors	Weight	State

Create Service

Service Name* EasyCallGateway

Server* 10.217.93.200

Protocol* SSL

Port* 443

☑ Enable Service

Available

Certificates
ns-server-certificate
NSCA.keypair
NSServer.keypair
VerisignIntermediateCA.keypair
NSECServer.keypair

Configured

Certificates	Type	CRL Mandatory

Select the Services Tab, Add or Select existing for Backend EasyCall Conferencing Gateway.

Service Name: EasyCallGateway

Server: <internal EasyCall Gateway IP Address>

Protocol: SSL

Port: 443

Note: Do not configure any monitors.

Do not configure any SSL Certificates.

Select ‘Create’

Select ‘Ok’ to finish importing the Template.

Content Filter Configuration

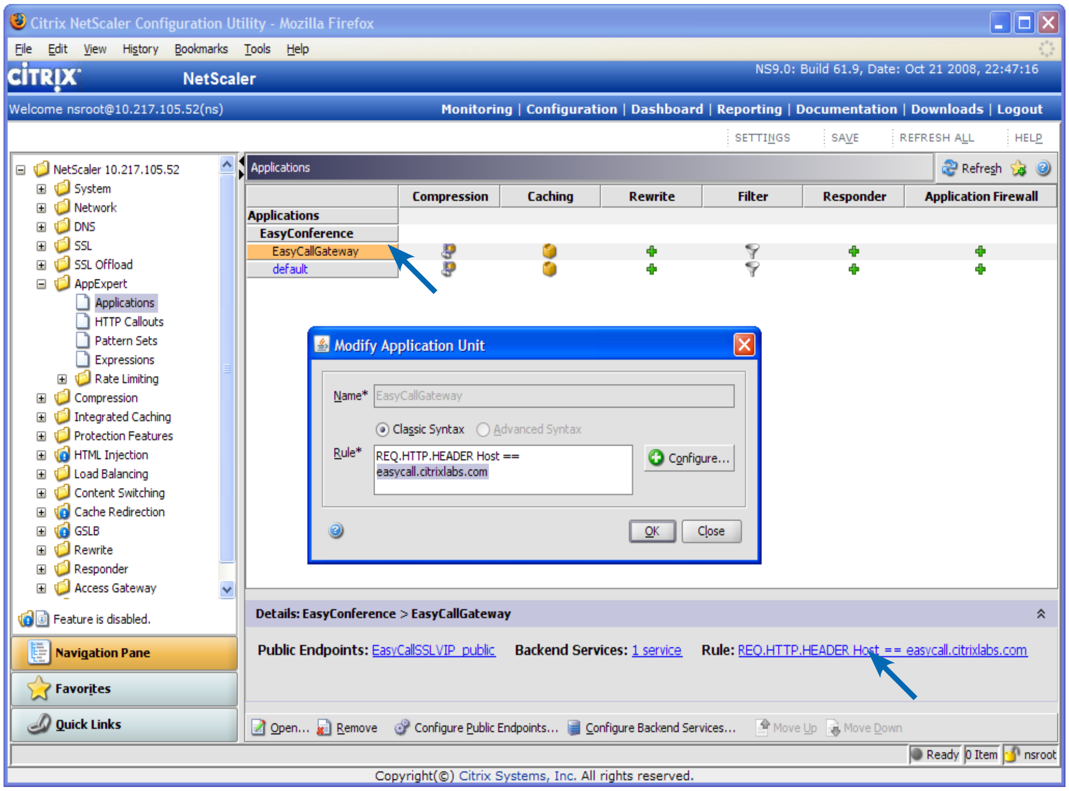
In order for the content filter to work specific to the NetScaler implementation at your site, change the hostname in the Application Unit.

Change the hostname field in the Content Filter rule.

Select the EasyCallGateway Application Unit.

Click on the Rule for the EasyCallGateway Application Unit.

Change the Hostname to match the hostname of the public VIP of the NetScaler.



Name* EasyCallGateway

● Classic Syntax ○ Advanced Syntax

Rule* REQ.HTTP.HEADER Host == easycall.citrixlabs.com

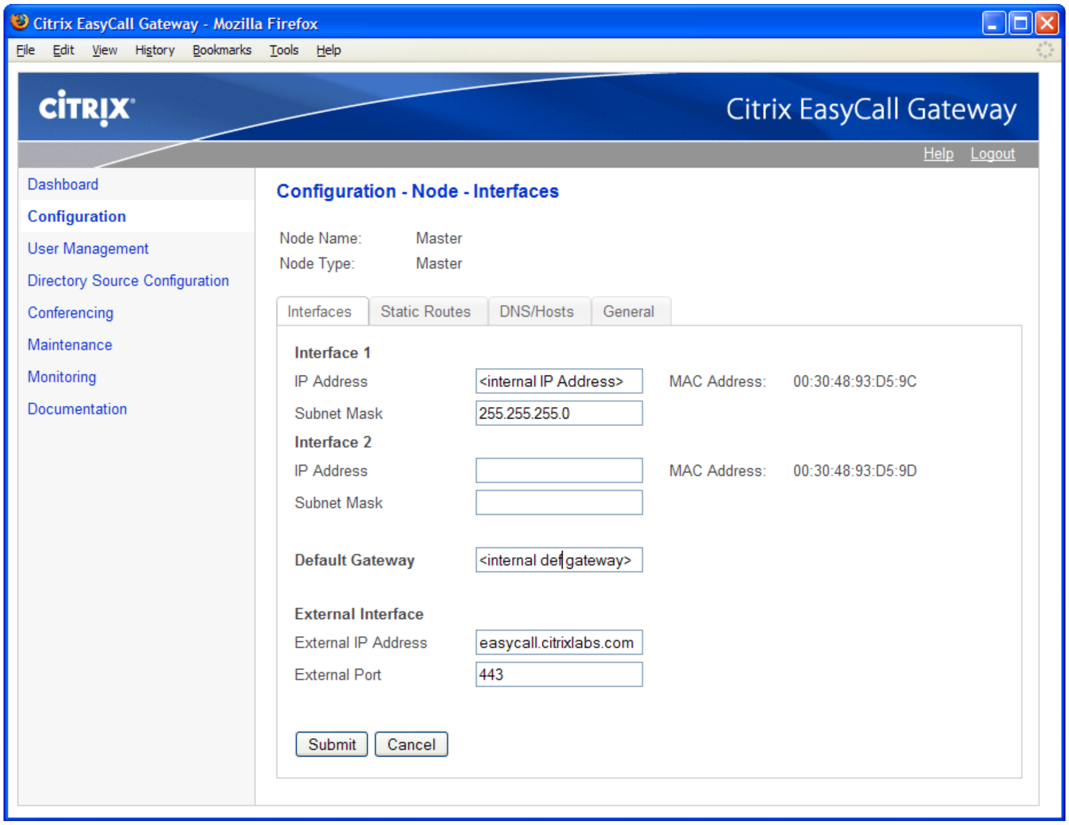
Details: EasyConference > EasyCallGateway

Public Endpoints: EasyCallSSLVIP_public Backend Services: 1 service Rule: REQ.HTTP.HEADER Host == easycall.citrixlabs.com

⚠ Make sure you take this opportunity to “Save” the configuration.

Citrix EasyCall Conferencing Gateway

EasyCall Gateway Configuration



Configuration - Node - Interfaces

Node Name: Master
Node Type: Master

Interface 1
IP Address: <internal IP Address>   MAC Address: 00:30:48:93:D5:9C
Subnet Mask: 255.255.255.0

Interface 2
IP Address: MAC Address: 00:30:48:93:D5:9D
Subnet Mask:

Default Gateway: <internal def gateway>

External Interface
External IP Address: easycall.citrixlabs.com
External Port: 443

Log into the EasyCall Gateway.

Navigate to Dashboard ➥ Configuration ➥ Interfaces.

External Interface: Enter the external (public network) hostname that will resolve in DNS to the Citrix NetScaler SSL Offload VIP. (This is the hostname that external and internal clients will use to connect when they receive EasyCall Conferencing invitations through e-mail).

If left empty, the invitation will contain the internal hostname, and EasyCall Conferencing participants will not be able to connect to that URL, as the Citrix NetScaler will filter the request, and block any HTTPS request destined for the internal network.

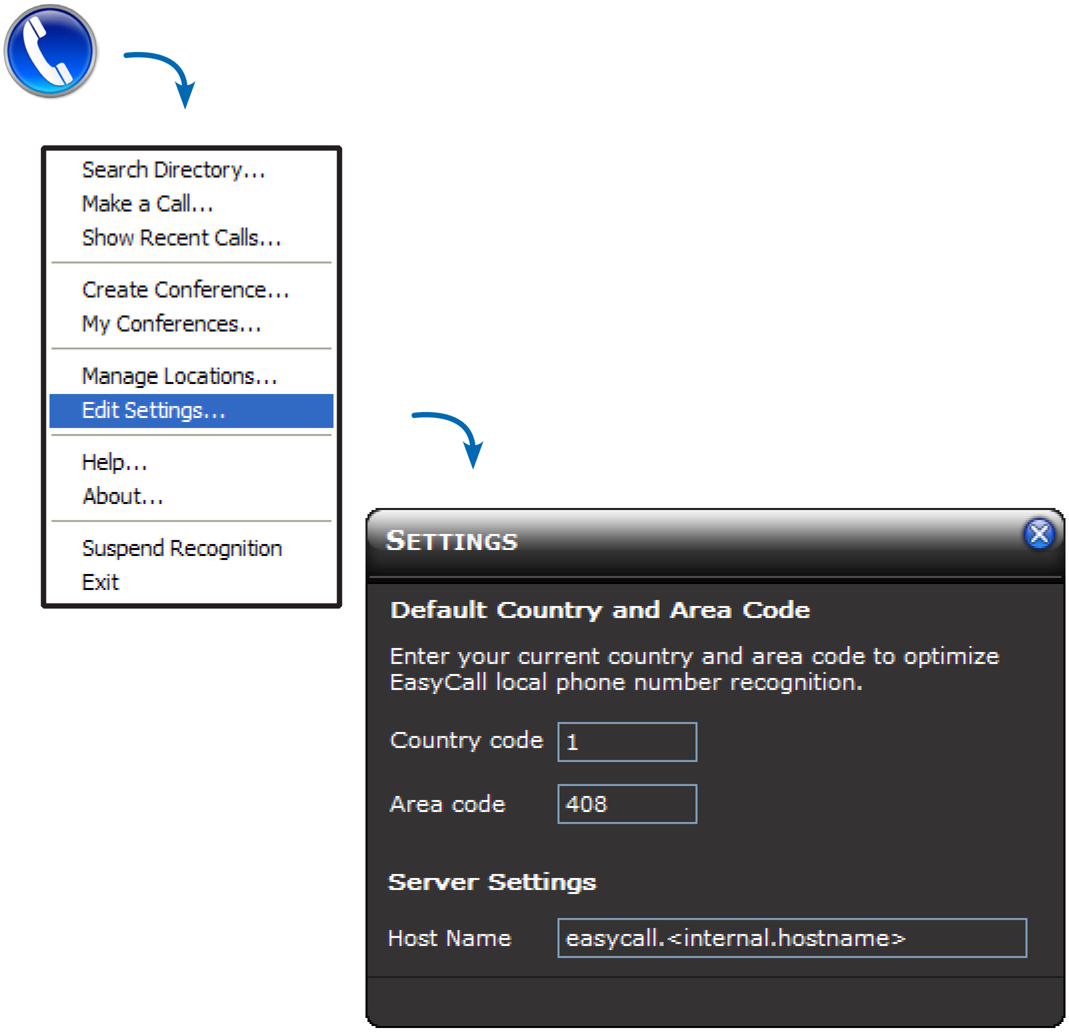
Select 'Submit'.

Citrix EasyCall Conferencing Client

EasyCall Conferencing Client Configuration

From the System Tray in the bottom right corner of the internal users computer, right click ➥ Edit Settings ➥ Enter the internal (private network) hostname of the EasyCall Gateway.

Close the Settings dialog box.



SETTINGS

Default Country and Area Code

Enter your current country and area code to optimize EasyCall local phone number recognition.

Country code: 1

Area code: 408

Server Settings

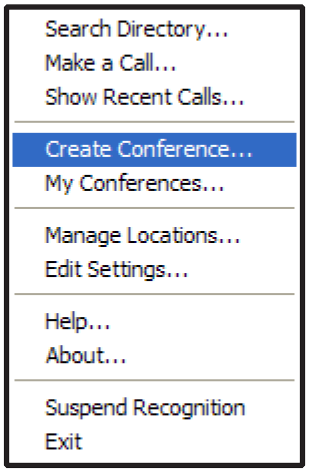
Host Name: easycall.<internal.hostname>

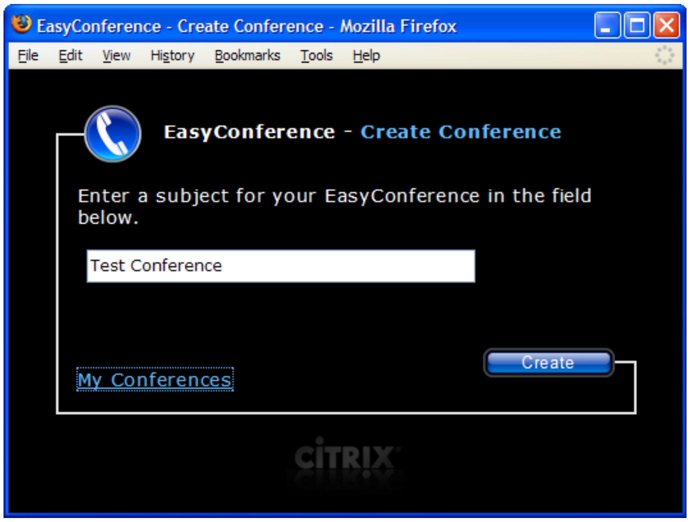
EasyCall Conferencing Conference Creation

The Citrix EasyCall Conferencing is created from the EasyCall Client on the internal users computer.

From the System Tray in the bottom right corner of the internal users computer, right click ➥ Create Conference ➥ Enter the Conference Call Subject.

Select ‘Create’.




EasyConference - Create Conference - Mozilla Firefox
File Edit View History Bookmarks Tools Help
EasyConference - Create Conference

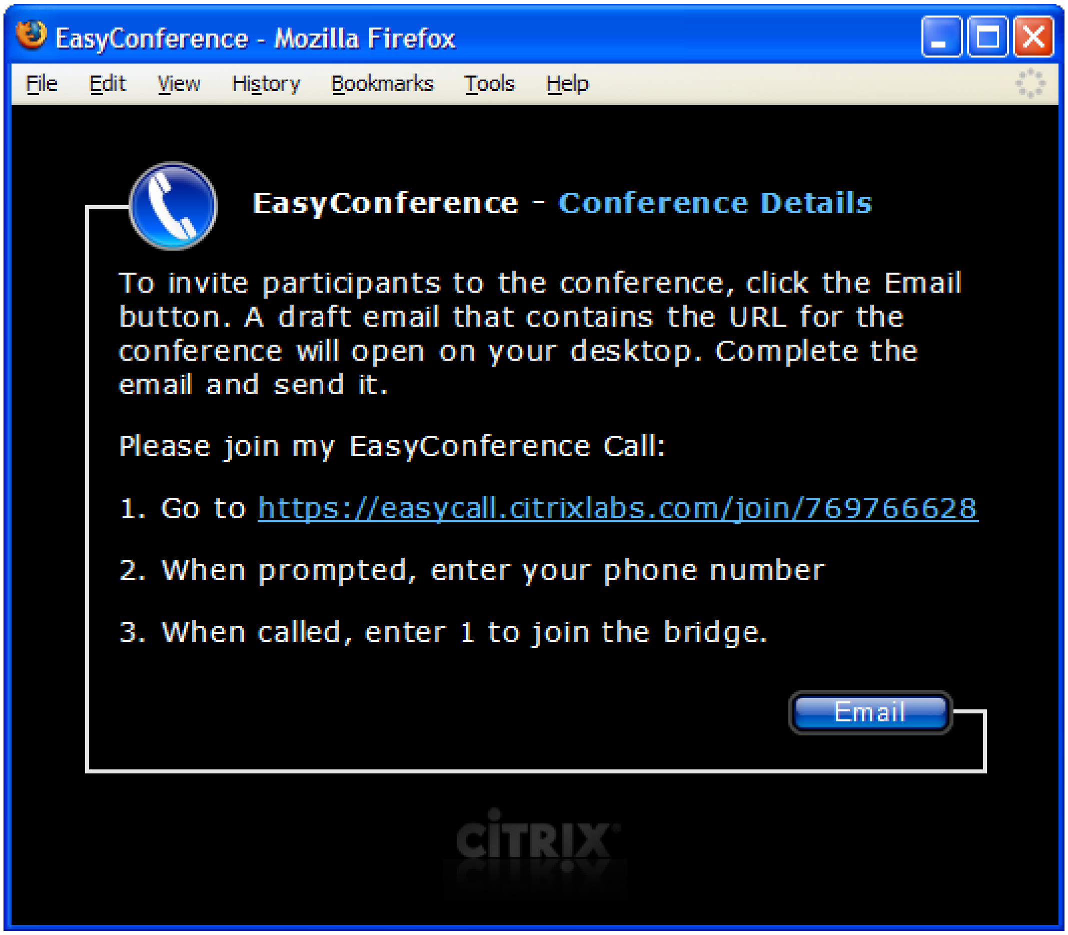
Enter a subject for your EasyConference in the field below.

Test Conference

My Conferences
Create
CITRIX

The EasyCall Client contacts the EasyCall Gateway, receives the EasyCall Conferencing connection parameters for the EasyCall Conferencing invite and presents them in a browser.

Select 'Email' to send the Conference Call invite to external and/or internal users.



EasyConference - Conference Details

To invite participants to the conference, click the Email button. A draft email that contains the URL for the conference will open on your desktop. Complete the email and send it.

Please join my EasyConference Call:

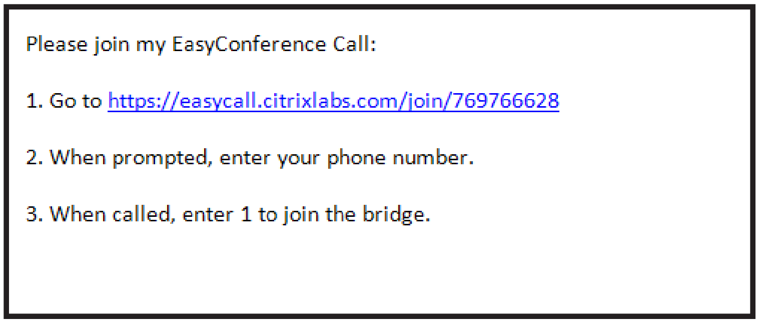
1. Go to https://easycall.citrixlabs.com/join/769766628

2. When prompted, enter your phone number

3. When called, enter 1 to join the bridge.

EasyCall Conferencing Participant Join

The Citrix EasyCall Conferencing participant join operation is simple.



Please join my EasyConference Call:

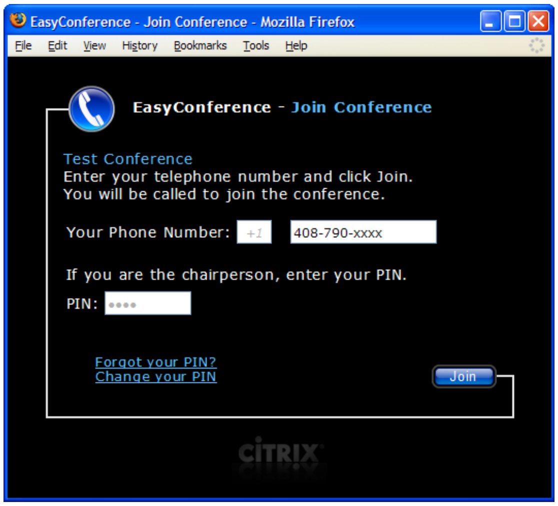
1. Go to https://easycall.citrixlabs.com/join/769766628

2. When prompted, enter your phone number.

3. When called, enter 1 to join the bridge.

The EasyCall Conferencing participant will receive an e-mail with an invite.

Click on the URL link in the email to join the EasyCall Conference.



EasyConference - Join Conference - Mozilla Firefox
File Edit View History Bookmarks Tools Help
EasyConference - Join Conference
Forgot your PIN?
Change your PIN
Join
CITRIX

Test Conference
Enter your telephone number and click Join.
You will be called to join the conference.

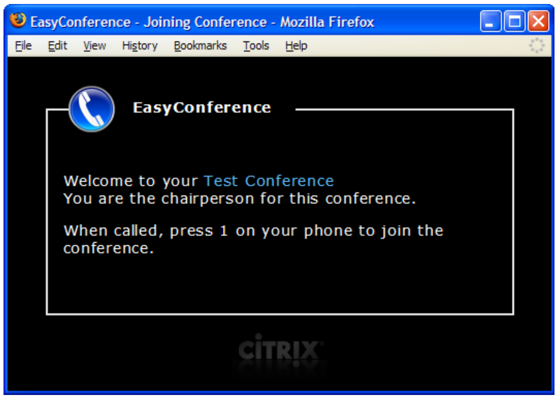
Your Phone Number: +1 408-790-xxxx

If you are the chairperson, enter your PIN.

PIN: ••••

The EasyCall Conferencing participant enter's their callback phone number.

Select 'Join'.



EasyConference - Joining Conference - Mozilla Firefox
File Edit View History Bookmarks Tools Help
EasyConference
CITRIX

Welcome to your Test Conference
You are the chairperson for this conference.

When called, press 1 on your phone to join the conference.

Moments later, the EasyCall Conferencing participant's phone will ring.

Press '1' to join the conference.

Appendix A - NetScaler Configuration

NetScaler

```
set ns config -IPAddress 10.217.105.52 -netmask 255.255.255.0

enable ns feature LB CMP SSL CF

set interface 1/2 -speed AUTO -flowControl RX -autoneg ENABLED -haMonitor ON -trunk OFF -lacpMode DISABLED -throughput 0 -bandwidthHigh 0 -bandwidthNormal 0

set interface 1/8 -speed AUTO -flowControl RX -autoneg ENABLED -haMonitor ON -trunk OFF -lacpMode DISABLED -throughput 0 -bandwidthHigh 0 -bandwidthNormal 0

add ns ip 10.217.105.92 255.255.255.0 -type MIP -vServer DISABLED

add ns ip 67.97.253.79 255.255.255.0 -vServer DISABLED

add vlan 67

bind vlan 67 -ifnum 1/8

bind vlan 67 -IPAddress 67.97.253.79 255.255.255.0

add server 10.217.93.200 10.217.93.200

add cs policy app_cs22 -rule “SYS.EVAL_CLASSIC_EXPR(\”REQ.HTTP.HEADER Host == easycall.citrixlabs.com\”)”

add service EasyCallGateway 10.217.93.200 SSL 443 -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA YES -TCPB YES -CMP YES

add filter action Forbidden errorcode 403 “403 Forbidden”

add cmp policy cmp_easycall -rule ns_true -resAction COMPRESS

add filter policy EasyCallAuthHostPol -rule ns_true -reqAction Forbidden

add filter policy EasyCallAuthURLPol -rule “REQ.HTTP.URL NOTCONTAINS /join && REQ.HTTP.URL NOTCONTAINS /images && REQ.HTTP.URL NOTCONTAINS /includes” -reqAction Forbidden

add filter policy EasyCallDefaultForbidden -rule ns_true -reqAction Forbidden

add lb vserver EasyCallSSLVIP SSL 67.97.253.92 443 -persistenceType NONE -cltTimeout 180

add lb vserver app_0_ApplicationsEasyConference HTTP 0.0.0.0 0 -persistenceType NONE -cltTimeout 180 -downStateFlush DISABLED

add lb vserver app_u_EasyConferenceEasyCallGateway HTTP 0.0.0.0 0 -persistenceType NONE -cltTimeout 180 -downStateFlush DISABLED

add lb vserver app_o_EasyConferencedefault HTTP 0.0.0.0 0 -persistenceType NONE -cltTimeout 180 -downStateFlush DISABLED

add cs vserver EasyCallSSLVIP_public SSL 67.97.253.91 443 -cltTimeout 180

add cache policy easycall_cache_pol -rule TRUE -action CACHE -storeInGroup DEFAULT

add cache policy cache_easycall -rule TRUE -action CACHE -storeInGroup DEFAULT

add cache policy easycall_cache_def -rule TRUE -action CACHE -storeInGroup DEFAULT

add cache policylabel easycall_cache_label -evaluates REQ

bind cache policylabel easycall_cache_label -policyName easycall_cache_pol -priority 100 -gotoPriorityExpression END

bind lb vserver EasyCallSSLVIP EasyCallGateway

bind lb vserver app_0_ApplicationsEasyConference EasyCallGateway
bind lb vserver app_u_EasyConferenceEasyCallGateway EasyCallGateway
bind lb vserver app_o_EasyConferencedefault EasyCallGateway
bind lb vserver EasyCallSSLVIP -policyName EasyCallAuthHostPol -priority 10
bind lb vserver EasyCallSSLVIP -policyName EasyCallAuthURLPol -priority 20
bind lb vserver app_u_EasyConferenceEasyCallGateway -policyName cmp_easycall
bind lb vserver app_u_EasyConferenceEasyCallGateway -policyName EasyCallAuthURLPol -priority 20
bind lb vserver app_o_EasyConferencedefault -policyName cmp_easycall
bind lb vserver app_o_EasyConferencedefault -policyName EasyCallDefaultForbidden
bind lb vserver app_u_EasyConferenceEasyCallGateway -policyName cache_easycall -priority 100 -gotoPriorityExpression END -type REQUEST
bind lb vserver app_o_EasyConferencedefault -policyName easycall_cache_def -priority 100 -gotoPriorityExpression END -type REQUEST
bind cs vserver EasyCallSSLVIP_public app_u_EasyConferenceEasyCallGateway -policyName app_cs22 -priority 100
bind cs vserver EasyCallSSLVIP_public app_o_EasyConferencedefault
add ssl certKey NSCA.keypair -cert NSCA.cer -key NSCA.key
add ssl certKey NSServer.keypair -cert NSServer.cer -key NSServer.key
add ssl certKey VerisignIntermediateCA.keypair -cert SecureSiteTrialRootCACertificate.cer
add ssl certKey NSECServer.keypair -cert EasyCallTrialCertificate2.cer -key EasyCallTrialCertificate2.key
set ssl service EasyCallGateway -eRSA DISABLED -sessReuse ENABLED -sessTimeout 600 -cipherRedirect DISABLED -sslv2Redirect DISABLED
set ssl vserver EasyCallSSLVIP -sessReuse ENABLED -sessTimeout 600
bind ssl vserver EasyCallSSLVIP -certkeyName NSECServer.keypair
bind ssl vserver EasyCallSSLVIP -certkeyName VerisignIntermediateCA.keypair -CA
bind ssl vserver EasyCallSSLVIP_public -certkeyName NSECServer.keypair
bind ssl vserver EasyCallSSLVIP_public -certkeyName VerisignIntermediateCA.keypair -CA
set uiinternal EXPRESSION app_0_ApplicationsEasyConference -uiinfo “P%Applications^ET%PE^CS%EasyCallSSLVIP_public^”
set uiinternal EXPRESSION app_u_EasyConferenceEasyCallGateway -uiinfo “P%app_0_ApplicationsEasyConference^PR%100^P%app_0_ApplicationsEasyConference^CS%EasyCallSSLVIP_public^ET%PE^” -rule “REQ.HTTP.HEADER Host == easycall.citrixlabs.com”
set uiinternal EXPRESSION app_o_EasyConferencedefault -uiinfo “ET%PE^P%app_0_ApplicationsEasyConference^P%app_0_ApplicationsEasyConference^CS%EasyCallSSLVIP_public^”
```

Appendix B - Content Filtering Configuration

The Citrix NetScaler Application Switch will be configured to filter all HTTP Requests going to the EasyCall Gateway. Essentially the logic looks like the following:

From the NetScaler GUI, select NetScaler ➥ Protection Features ➥ Filter ➥ Add.

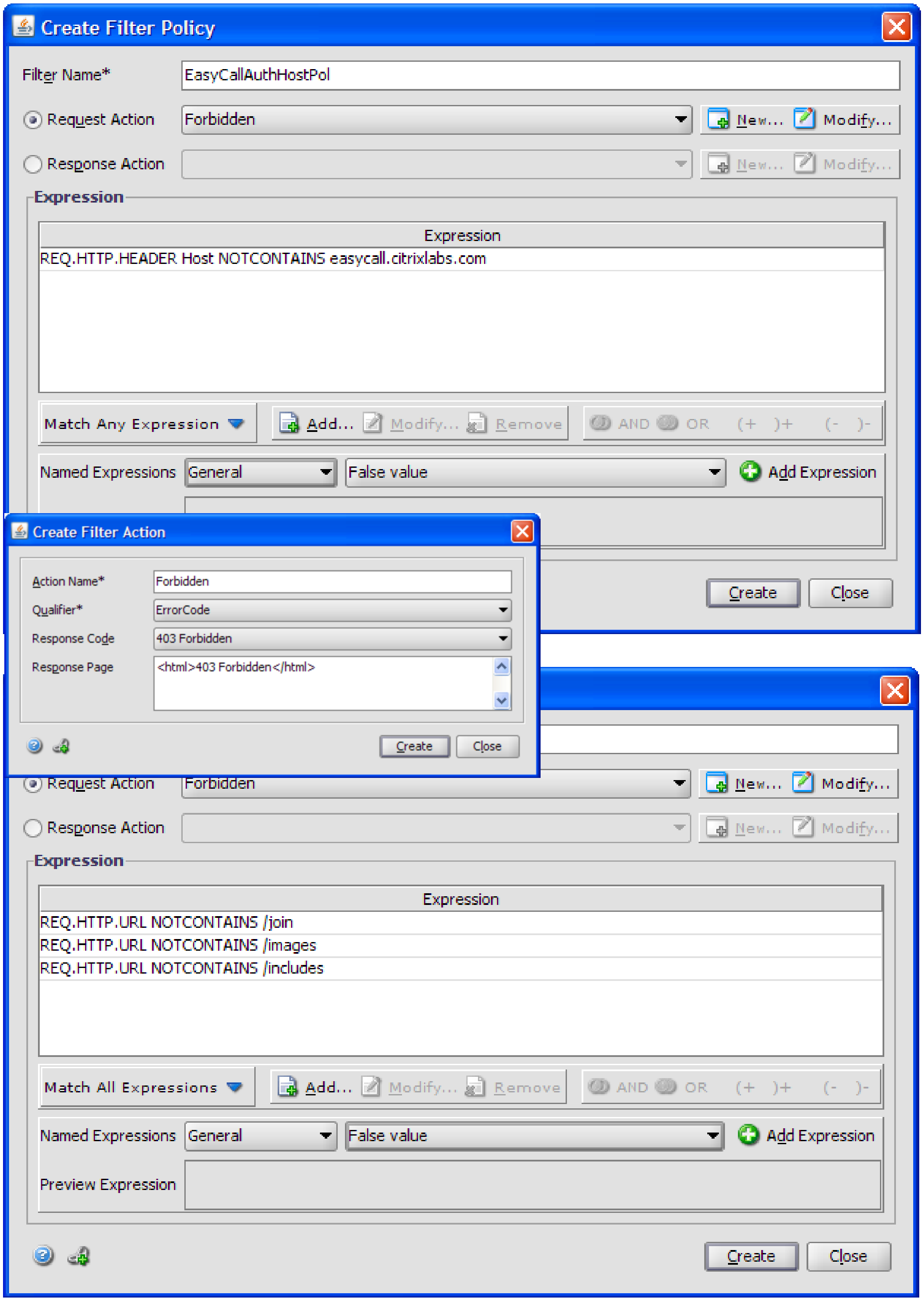
For Response Action, Select New, and create an “error code” response named “Forbidden” for code 403.

This Filter Policy checks the Hostname.

The Policy Expression should return a 403 Forbidden HTML page for any request not destined to the EasyCall Gateway “easycall.citrixlabs.com” which resolves to the public IP Address of 67.97.253.91.

This Filter Policy checks the URL and only allows URL’s destined to /join, /images and /includes on the EasyCall Gateway.

All other URL’s will return a 403 Forbidden HTML page.



Create Filter Policy

Filter Name*: EasyCallAuthHostPol

● Request Action: Forbidden

○ Response Action:

Expression

Expression
REQ.HTTP.HEADER Host NOTCONTAINS easycall.citrixlabs.com

Match Any Expression

Named Expressions: General — False value

Create Filter Action

Action Name*: Forbidden

Qualifier*: ErrorCode

Response Code: 403 Forbidden

Response Page: <html>403 Forbidden</html>

● Request Action: Forbidden

○ Response Action:

Expression

Expression
REQ.HTTP.URL NOTCONTAINS /join
REQ.HTTP.URL NOTCONTAINS /images
REQ.HTTP.URL NOTCONTAINS /includes

Match All Expressions

Named Expressions: General — False value

Preview Expression:

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.