

Symantec™ Validation & ID Protection Service

Integration Guide for Citrix® NetScaler

Symantec VIP Integration Guide for Citrix® NetScaler

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Last updated [December 7, 2015](#)

Legal Notice

Copyright © 2015 Symantec Corporation. All rights reserved

Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction, release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement. This document may describe features and/or functionality not present in your software or your service agreement. Contact your account representative to learn more about what is available with this Symantec® product.

Symantec Corporation

350 Ellis Street Mountain View, CA 94043

<http://www.symantec.com>

<https://www.symantec.com/contactsupport>

Chapter 1	Introduction	1
	Partner Information	1
	Integration Overview	1
	VIP Features Checklist	2
	Remote Access Integration Architecture	3
	Authentication Method 1: User Name - Security Code	3
	Authentication Method 2: User Name - LDAP Password - Security Code or User Name - LDAP Password - Security Code (Access Challenge Mode)	4
Chapter 2	Installation and Configuration	5
	Integration Summary	5
	Installing and Configuring VIP Enterprise Gateway	5
	Configuring the Citrix NetScaler Device with VIP Enterprise Gateway	5
	Authentication Method 1: User Name - Security Code mode Integration	6
	Authentication Method 2: User Name - LDAP Password - Security Code or User Name - LDAP Password - Security Code (Access Challenge Mode)	9
	Supporting Selective Two-Factor Authentication for a Specific Set of Users	16
Chapter 3	VIP JavaScript Integration for Citrix NetScaler	17
	Configuring JavaScript with VIP Components	17
	Integrating JavaScript with Citrix NetScaler 10.x	17
	Generating JavaScript Code from VIP Manager	17
	Updating the Citrix NetScaler Sign-In Page	18
	Integrating JavaScript with Citrix NetScaler 11.0	19
	Updating JavaScript Integration Code for Citrix NetScaler 11.0	19
	Testing the JavaScript Integration	22
Appendix A	Adding LDAP Authentication Server and Policy	23
	Adding LDAP Authentication Server	23
	Adding the LDAP Authentication Policy	24
Appendix B	Customizing the Citrix NetScaler Login Page	25

Introduction

This chapter includes the following topics:

- [“Partner Information”](#) on page 1
- [“Integration Overview”](#) on page 1
- [“VIP Features Checklist”](#) on page 2
- [“Remote Access Integration Architecture”](#) on page 3

Symantec™ Validation & ID Protection Service Integration Guide for Citrix® NetScaler describes how to integrate the Citrix NetScaler device with VIP Enterprise Gateway to allow the following authentication methods:

- **Authentication Method 1: User Name - Security Code**
In this authentication method, the first factor is validated by your user store (AD/LDAP), and the second factor is validated by VIP Enterprise Gateway.
- **Authentication Method 2: User Name - LDAP Password - Security Code or User Name - LDAP Password - Security Code (Access Challenge Mode)**
In these authentication methods, both the first and second factors are validated by VIP Enterprise Gateway.

Partner Information

The following procedures have been tested on the following platforms:

Table 1-1 Partner Information

Partner Name	Citrix
Product Name	Citrix® NetScaler
Product Version	9.x, 10.x, 11.0

Integration Overview

Table 1-2 Integration Overview

Authentication Methods Supported	<ul style="list-style-type: none">■ User Name - Security Code■ User Name - Password - Security Code■ User Name - Password - Security Code (Access Challenge Mode)■ Intelligent Authentication (IA)/Push
Client Integration - Security Code	VIP Enterprise Gateway (EG) 8.x or higher

VIP Features Checklist

The following table lists the VIP Enterprise Gateway features that are supported with Citrix NetScaler:

Table 1-3 VIP Supported Features

VIP Feature	Support
First-factor authentication	
AD/LDAP password using VIP Enterprise Gateway	Yes
VIP PIN	No
Second-factor authentication	
VIP Push	Yes
SMS	Yes
Voice	Yes
Selective strong authentication	
End user-based	Yes
Risk-based	Yes
General authentication	
Multi-domain	Yes
Anonymous user name	Yes
Legacy authentication provider integration (delegation)	Yes
AD password reset	Yes
Integration Method	
VIP JavaScript	Yes
VIP Login	No
RADIUS (Native)	Yes

Remote Access Integration Architecture

Authentication Method 1: User Name - Security Code

The following diagram illustrates the configuration of User Name - Security Code authentication scheme for the Citrix NetScaler with VIP Enterprise Gateway. In this scheme, the first factor is validated by your user store (AD/LDAP), and the second factor is validated by VIP Enterprise Gateway.

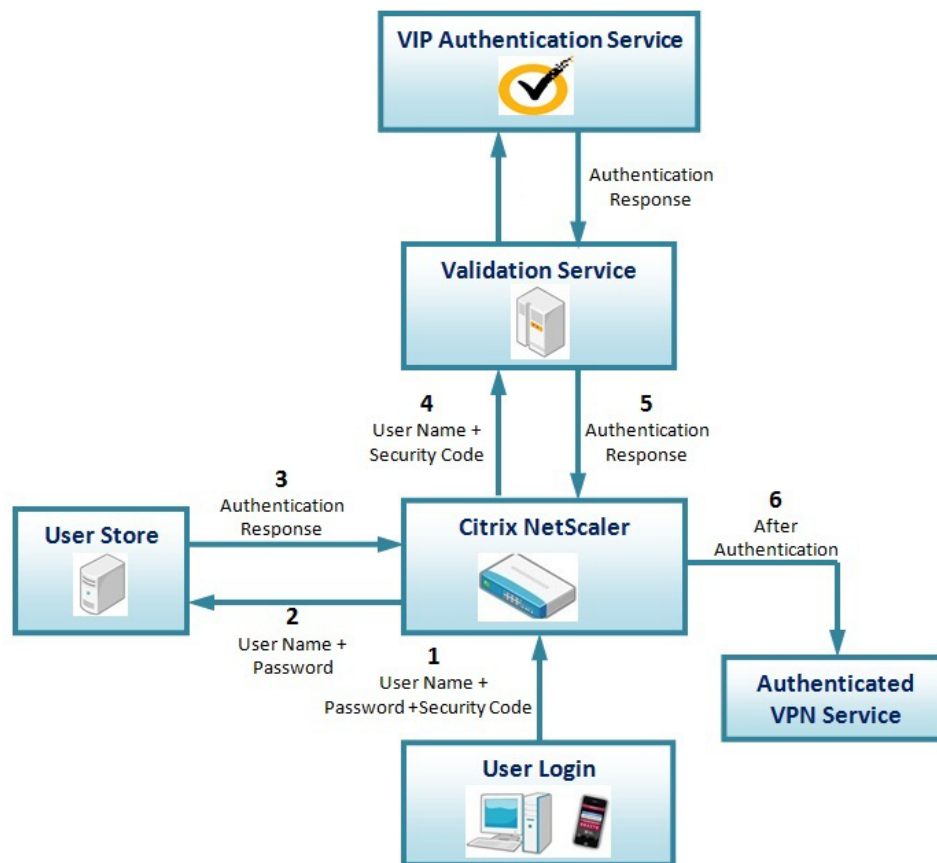


Figure 1-1 Authentication Process for User Name - Security Code Authentication Method

- 1 The user enters a user name, password, and a security code.
- 2 As the first part of the two-factor authentication process, the user name and password are sent to the AD/LDAP by the Citrix NetScaler device.
- 3 If the user name and password are authenticated, the AD/LDAP will return group permission details to the Citrix NetScaler device, along with the authentication response.
- 4 The Citrix NetScaler device sends the user name and security code to the Validation Service for authentication. This is the second part of the two-factor authentication process.
- 5 The Validation Service authenticates the user name and security code with the VIP Authentication Service.
- 6 If the user name and security code are successfully authenticated, the Validation Service returns an Access-Accept Authentication response to the Citrix NetScaler device.
- 7 Based on this response, the user is allowed access to resources.

Authentication Method 2: User Name - LDAP Password - Security Code or User Name - LDAP Password - Security Code (Access Challenge Mode)

The following diagram illustrates how the User Name - Password -Security Code authentication scheme is configured for the Citrix NetScaler with VIP Enterprise Gateway. In this scheme, both the first and second factors are validated by VIP Enterprise Gateway.

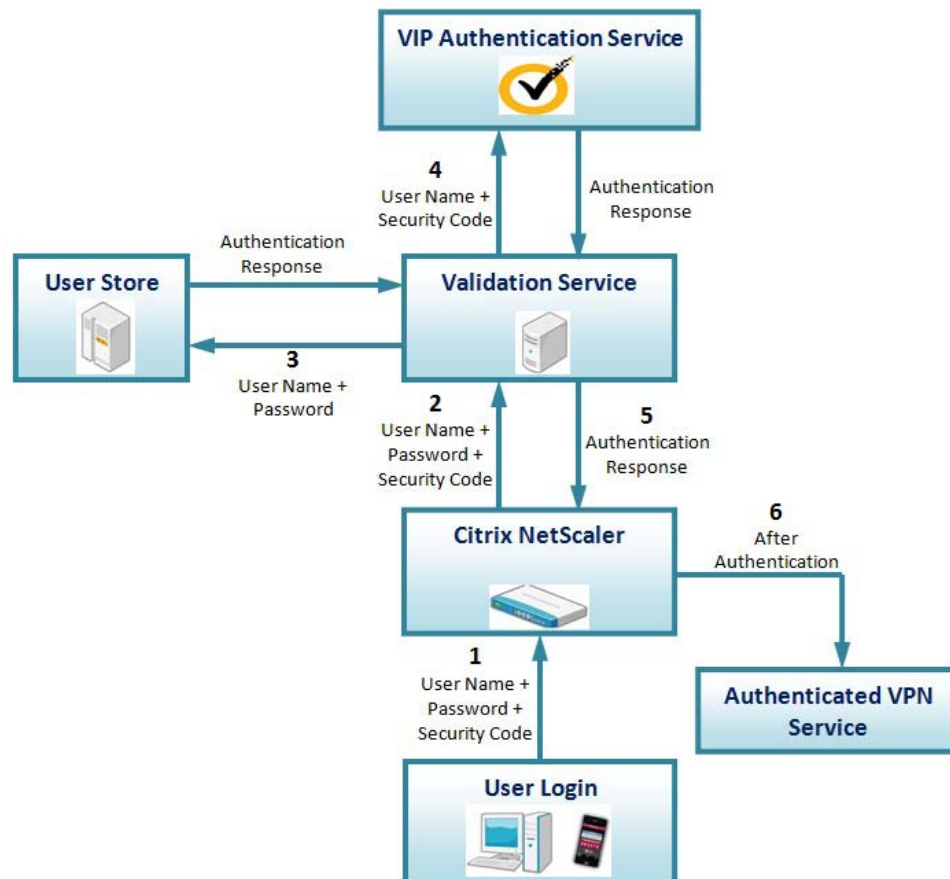


Figure 1-2 Authentication process for User Name - Password -Security Code Authentication Method

- 1 User enters a user name, password, and a security code. For both user name - password - security code mode and user name - password - security code (access challenge mode), the user enters the user name - password first, followed by a security code entered on the next page.
- 2 The user name, password, and security code are sent to the Validation Service by Citrix NetScaler.
- 3 The user name and password are authenticated by the Validation Service against your user store (AD/LDAP). This is the first part of the two-factor authentication process. If the user name and password are authenticated, the authentication response will include group permission details.
- 4 The Validation Service authenticates the user name and security code with the VIP Authentication Service. This is the second part of the two-factor authentication process.
- 5 If the user name and security code are successfully authenticated, the Validation Service returns an Access-Accept Authentication response to Citrix NetScaler.
- 6 Based on this response, the user is allowed access to the VPN service(s).

Installation and Configuration

Integration Summary

The following summary of procedures describes how to configure the Citrix NetScaler device for two-factor authentication through VIP Enterprise Gateway.

Step 1: [“Installing and Configuring VIP Enterprise Gateway”](#) on page 5

Step 2: [“Configuring the Citrix NetScaler Device with VIP Enterprise Gateway”](#) on page 5

Installing and Configuring VIP Enterprise Gateway

You must do the following:

- Install and Configure VIP Enterprise Gateway.
- Add the Validation Server in one of the following modes:
 - User Name - Security Code
 - User Name - Password - Security Code
 - User Name - Password - Security Code (Access Challenge)

Note: You can configure the RADIUS-LDAP mapping in **User Name- Password- Security code or Access challenge mode** in the Validation server only if you want to authorize the user according to the LDAP Groups. For more information on these tasks, see *VIP Enterprise Gateway Installation and Configuration Guide*.

Configuring the Citrix NetScaler Device with VIP Enterprise Gateway

Complete the procedures in this section to configure the NetScaler device. These procedures apply for both authentication schemes, unless otherwise specified. See the NetScaler product documentation for specific details.

Note: The screen examples within these procedures have been captured from Citrix NetScaler VPX (Version NS 11.0). Refer to the product documentation provided for your version of the NetScaler device for specific screen captures and procedures.

Authentication Method 1: User Name - Security Code mode Integration

Prerequisite

Add the LDAP authentication server and policy if they do not already exist. For more information, see the Citrix documentation or see [“Adding LDAP Authentication Server and Policy”](#) on page 23.

Adding the RADIUS Authentication Server

- 1 In the navigation pane, expand **System** > **Authentication** and select **RADIUS**.
- 2 From the **Servers** tab, click **Add**.
- 3 In the Create Authentication Server dialog box, type a name for the server in the **Name** field.
- 4 In the **Server** section, specify values for each parameter:
 - **IP Address:** Enter the IP address of the Validation Server.
 - **Port:** Enter the port number of the Validation Server.
 - **Time-out:** Enter a value in seconds.
 - **Secret Key:** Enter the secret key and confirm it. Be sure the **Secret Key** and the VIP RADIUS Shared Secret Key are the same.

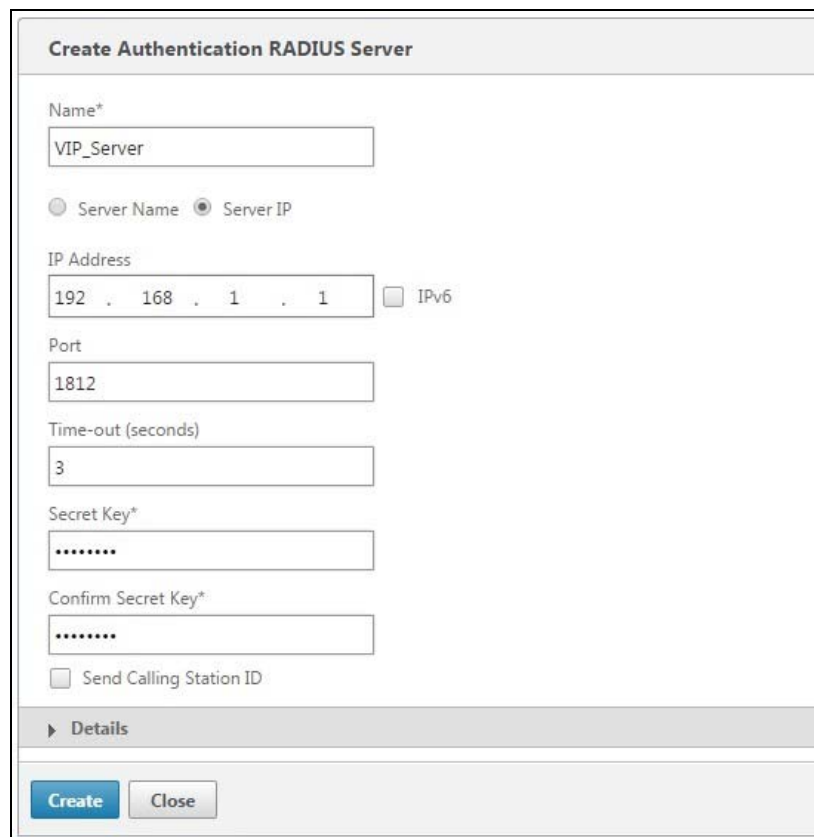


Figure 2-1 Create User Name - Security Code Authentication Server

- 5 Click **Create** to create the RADIUS Server.

Adding the RADIUS Authentication Policy

- 1 From the **Policies** tab, click **Add**.
- 2 In the Create Authentication Policy dialog box, type a name for the policy in the **Name** field.
- 3 From the **Server** drop-down list, select the VIP RADIUS server created previously (for example: **VIP_Server**).

The screenshot shows a web-based configuration interface for creating a RADIUS authentication policy. The dialog box has a title bar 'Create Authentication RADIUS Policy'. Inside, there are three main sections: 'Name*' with a text input field containing 'VIP_Policy'; 'Server*' with a dropdown menu showing 'VIP_Server' and two small icons (a plus sign and a pencil); and 'Expression*' with a large text area containing 'ns_true'. Above the text area are three tabs: 'Operators', 'Saved Policy Expressions', and 'Frequently Used Expressions', along with a 'Clear' button. At the bottom of the dialog are two buttons: 'Create' (highlighted in blue) and 'Close'.

Figure 2-2 Create Policy for User Name - Security Code Authentication Server

- 4 Under **Expression**, you can add your own expression according to the policy.

Note: For test purposes only, “ns_true” was added as the Expression. Add the appropriate policy according to your enterprise requirement.

- 5 Click **Create**.

Configuring NetScaler Gateway Virtual Server

- 1 In the navigation pane, expand **NetScaler Gateway > Virtual Servers**, and click **Add to new virtual server** or **Open the existing virtual server**. Ignore [Step 2](#) to [Step 4](#) if the LDAP server is already configured as the primary authentication server.
- 2 Under the **Authentication** section, click the + button.
- 3 From the **Choose Policy** drop-down list, select **LDAP** as the **Policy** and **Primary** as the **Type**, and click **Continue**.
- 4 Click **Bind** to select your LDAP policy and then click **Insert**.
- 5 Under the **Authentication** section, click the + button.
- 6 From the **Choose Policy** drop-down list, select **RADIUS** as the **Policy** and **Secondary** as the **Type**, and click **Continue**.
- 7 Click **Bind** to select your RADIUS policy and then click **Insert**.
- 8 Click **OK**.

Certificates

1 Server Certificate

No CA Certificate

Authentication

Primary Authentication

1 LDAP Policy

Secondary Authentication

1 RADIUS Policy

Policies

Request Policies

4 Cache Policies

Figure 2-3 Create NetScaler Gateway Virtual Server

Testing an End User

Users can access the Citrix Access Gateway in the following two ways:

- Browser-based Logon
- Form-based Logon

Browser-based Logon

- 1 Type the name of the Access Gateway Virtual Server (For example, <https://mycitrix.com>).
The Logon page displays three fields – **User Name**, **Password**, and **Security Code**.

NetScaler with
Unified Gateway

Please log on

User name

Password

Security Code

Log On

Figure 2-4 Browser-based Logon Page

Note: For details on updating the login page **password 2** field, see [Appendix B, “Customizing the Citrix NetScaler Login Page.”](#)

- 2 Enter the **User name**, **Password**, and **Security Code** to gain access. If the credentials are correct, you are redirected to the home page.

Form-based Logon

For form-based logon, complete the following steps:

- 1 Double-click the Access Gateway Plugin icon.
- 2 Enter your **User name** and **Password**.
- 3 Right-click for advanced options to enable the **Secondary Password**. Enter the security code and then click **Connect**. If the credentials are correct, you are redirected to the home page.



Figure 2-5 Form-based Logon (Secondary Password Field)

Authentication Method 2: User Name - LDAP Password - Security Code or User Name - LDAP Password - Security Code (Access Challenge Mode)

Adding the Authentication Server

- 1 In the navigation pane, expand **System > Authentication**, and select **RADIUS**.
- 2 From the **Servers** tab, click **Add**.
- 3 In the Create Authentication Server dialog box, type a name for the server in the **Name** field.
- 4 In the **Server** section, specify values for each parameter:
 - **IP Address**: Enter the IP address of the Validation Server.
 - **Port**: Enter the port number of the Validation Server.
 - **Time-out**: Enter a value in seconds.
 - **Secret Key**: Enter the secret key and confirm it. Be sure the **Secret Key** and the VIP RADIUS Shared Secret Key are the same.

Create Authentication RADIUS Server

Name*

VIP_Server_1

☐ Server Name

☒ Server IP

IP Address

192 . 168 . 1 . 4

☐ IPv6 ?

Port

1813

Time-out (seconds)

3

Secret Key*

Confirm Secret Key*

☐ Send Calling Station ID

Details

Create

Close

Figure 2-6 Create (User Name - LDAP Password - Security Code) Access Challenge Mode Authentication Server

- 5
- Click **Details** to expand the advanced configuration and enter a value in the **Group Attribute Type** field. This value must match the **RADIUS Mapping Attribute** value that you had entered when configuring the RADIUS-LDAP mapping in the VIP Enterprise Gateway validation server. Ignore this step if you do not want to authorize a user based on the LDAP group.

Note: In this example, the Validation server **RADIUS Mapping Attribute** is selected as **Class**. The Class value of 25 was entered as the **Group Attribute Type** in the Citrix authentication server. Refer to the RFC for the RADIUS attribute numeric value.

▼ Details

NAS ID

☐ Enable NAS IP address extraction

Group Vendor Identifier

Group Prefix

Group Attribute Type

25

Group Separator

IP Address Vendor Identifier

IP Address Attribute Type

Password Vendor Identifier

Password Attribute Type

Password Encoding*

pap ▼

Accounting*

ON ▼

Default Authentication Group

Create

Close

Figure 2-7 Create (User Name - LDAP Password - Security Code) Access Challenge Mode Authentication Server

Adding the Authentication Policy

- 1 From the **Policies** tab, and click **Add**.
- 2 In the Create Authentication Policy dialog box, type a name for the policy in the **Name** field.
- 3 From the **Server** field, select the server created previously (for example, VIP_Server_1).

Create Authentication RADIUS Policy

Name*

VIP_Policy_1

Server*

VIP_Server_1

Expression*

Expression Editor

Operators

Saved Policy Expressions

Frequently Used Expressions

Clear

ns_true

Create

Close

Figure 2-8 Create (User Name - LDAP Password - Security Code) Access Challenge Mode Authentication Policy

- 4 Under **Expression**, you can add your own expression according to the policy.

Note: For test purposes only, **ns_true** was added as the **Expression**. Add the appropriate policy according to your enterprise requirement.

- 5 Click **Create**.

Configuring Netscaler Gateway Virtual Server

- 1 In the navigation pane, expand **Netscaler Gateway > Virtual Servers**.
- 2 Click **Open the existing virtual server**. If any other server is configured as the primary server, remove it.
- 3 Under the **Authentication** section, click the + button.
- 4 From the **Choose Policy** drop-down list, select **RADIUS** as the **Policy** and **Primary** as the **Type**, and click **Continue**.
- 5 Click **Bind** to select your RADIUS policy and then click **Insert**.
- 6 Click **OK**.

The screenshot shows a configuration window with two main sections: **Authentication** and **Policies**. The **Authentication** section has a '+' button in the top right and lists 'Primary Authentication' followed by '1 RADIUS Policy' with a right arrow. The **Policies** section has '+' and 'X' buttons in the top right, lists 'Request Policies' followed by '4 Cache Policies' with a right arrow, and a 'Done' button at the bottom left.

Figure 2-9 Create (User Name - LDAP Password - Security Code) Access Challenge Mode Virtual Server

Testing an End User

Authentication Method: User Name - LDAP Password - Security Code

For browser-based logon, perform the following steps:

- 1 Access the Access Gateway (for example, <https://mycitrix.com>).
- 2 The Logon page displays two fields: **User name** and **Password - Security Code**.

The screenshot shows the NetScaler Unified Gateway logon page. It has a dark green background with the text 'NetScaler with Unified Gateway' on the left. On the right, under the heading 'Please log on', there are two input fields: 'User name' and 'Password+Security C...'. Below these fields is a 'Log On' button.

Figure 2-10 Logon Page for User Name - Password - Security Code Mode

Note: For details on updating the login page password fields, see [Appendix B, “Customizing the Citrix NetScaler Login Page.”](#)

For form-based logon, perform the following steps:

- 1 Double-click the Access Gateway Plugin icon.
- 2 Enter your user name in the **User name** field, and password + security code in the **Password** field.
- 3 Click **Connect**. If the credentials are correct, you will be redirected to the home page.



Figure 2-11 Form-based Logon (Without Secondary Password Field)

Note: Do not right-click for advanced options to enable the **Secondary Password** field. The security code should be entered after the password within the **Password** field.

Authentication Method: User Name - LDAP Password - Security Code (Access Challenge Mode)

For browser-based logon, perform the following steps:

- 1 Access the Access Gateway (for example: <https://mycitrix.com>).
- 2 The Logon page displays two fields: **User name** and **Password**.

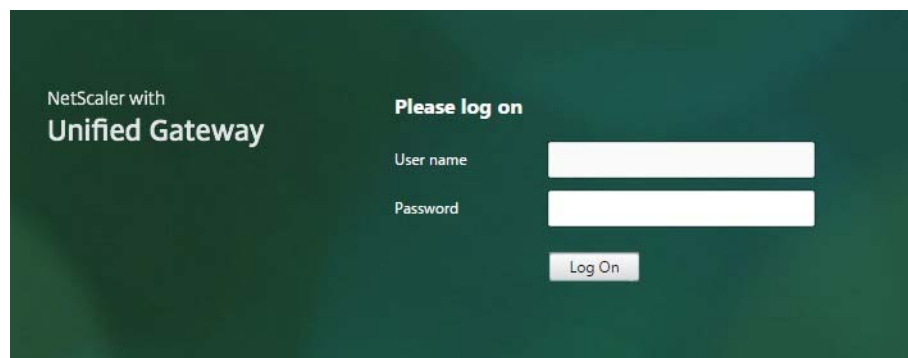


Figure 2-12 The Logon Page for User Name - LDAP Password - Security Code (Access Challenge) Mode

- 3 After successful authentication, the user is directed to the Access Challenge Mode.
- 4 For the Access Challenge, enter the security code.

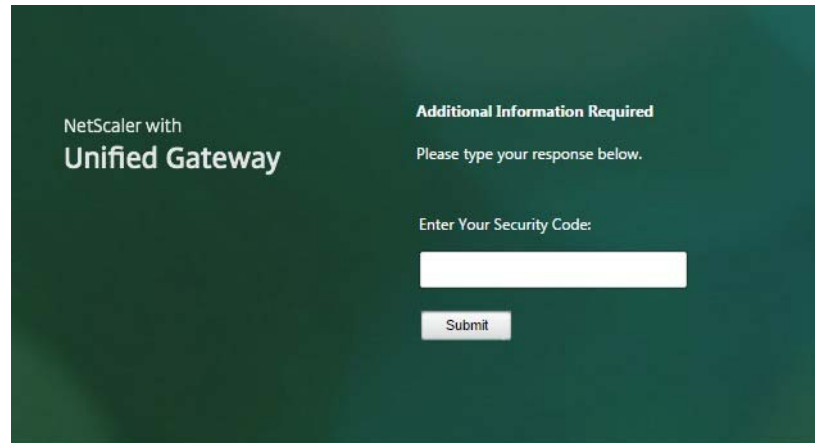


Figure 2-13 Access Challenge Screen for User Name - LDAP Password - Security Code (Access Challenge) Mode

5 Users can access assigned resources once they have successfully authenticated with a security code.

For form-based logon, perform the following steps:

- 1 Double-click the Access Gateway Plugin icon.
- 2 Enter your **User Name** and **Password**.
- 3 Click **Connect**.



Figure 2-14 Form-based Logon for Access Challenge Mode

4 After successful authentication, enter your **Security Code** in the displayed dialog box.

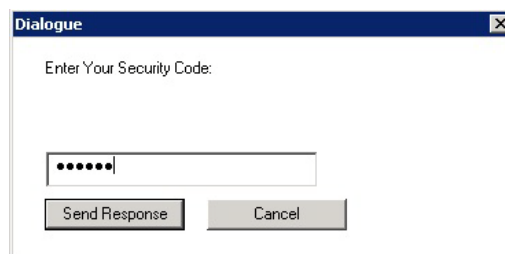


Figure 2-15 Form-based Access Challenge

5 Click **Send Response**. You are allowed to access resources based on role.

Supporting Selective Two-Factor Authentication for a Specific Set of Users

You can define distinct authentication or authorization policies in your corporate LDAP environment based on user Distinguished Names (DN) or group information. You can selectively provide highly secure two-factor authentication to a set of users. For example, a company can enable two-factor authentication for the system administrators who typically have higher privileges. The rest of the employees of the company may not have to use two-factor authentication.

You can configure Citrix NetScaler in the cascade authentication mode for enabling a subset of users for two-factor authentication.

Complete the following steps to configure selective two-factor authentication:

- 1 In your organization's LDAP/AD, make sure that you have grouped the users who use two-factor authentication. In Citrix NetScaler, configure the RADIUS and AD/LDAP server.
 - a In VIP Enterprise Gateway, configure your user store filter in such a way that the group of users who use VIP authentication only can be searched.
 - b In Citrix NetScaler, configure your LDAP/AD user filter in such a way that the users who are authenticated by AD password alone can be searched.
- 2 In the virtual server, add a new server or open the server that you want to update.
- 3 Navigate to the **Authentication** tab. Insert User Name - LDAP Password - Security Code mode VIP RADIUS server policy followed by the LDAP or AD policy.

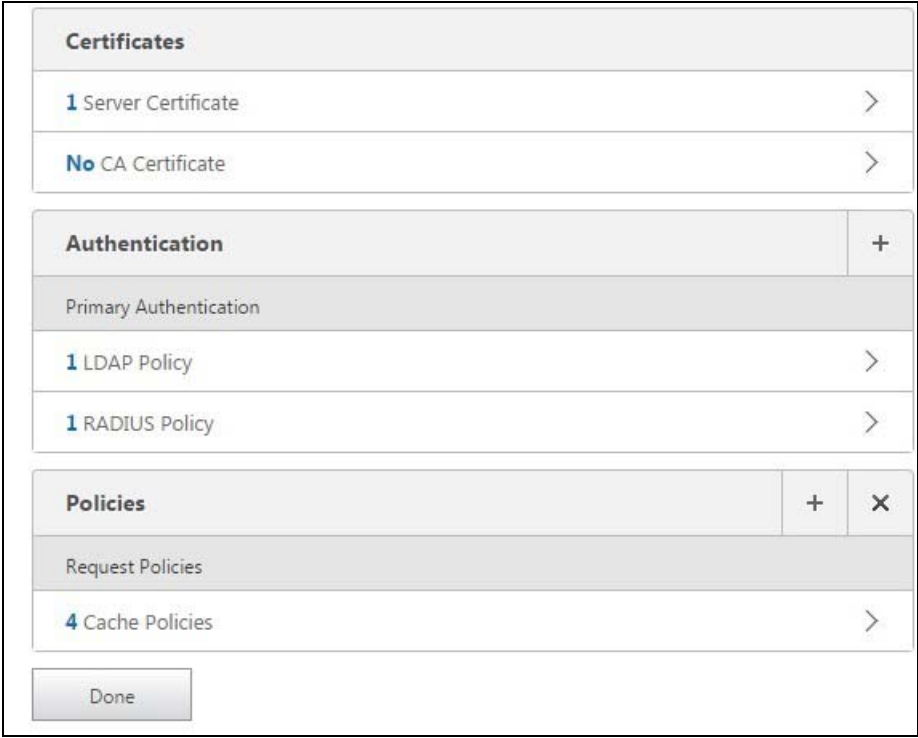


Figure 2-16 Network Policies

- 4 Click **Done** to save the changes.

VIP JavaScript Integration for Citrix NetScaler

This chapter describes how to integrate VIP JavaScript with Citrix NetScaler. There are separate procedures applicable for Citrix NetScaler versions 10.x and 11.0.

The following topics are explained:

- [“Configuring JavaScript with VIP Components”](#) on page 17
- [“Integrating JavaScript with Citrix NetScaler 10.x”](#) on page 17
- [“Integrating JavaScript with Citrix NetScaler 11.0”](#) on page 19
- [“Testing the JavaScript Integration”](#) on page 22

Configuring JavaScript with VIP Components

You must configure VIP JavaScript with VIP Manager before you update the sign-in page of the integration module. For details, refer to *Symantec VIP Intelligent Authentication Enterprise Integration Guide* (IA_Enterprise_Integration.pdf), which you can download from VIP Manager.

This configuration is required, irrespective of your installed version of Citrix NetScaler.

Integrating JavaScript with Citrix NetScaler 10.x

This sections describes the procedures for generating JavaScript code from VIP Manager, and updating the Citrix NetScaler sign-in page.

Generating JavaScript Code from VIP Manager

Perform the following steps in VIP Manager:

- 1 Log into VIP Manager and navigate to **Account → VIP Policy Configuration → Account → Edit**.
- 2 Click the **VIP Integration Code for JavaScript** link to generate code.
- 3 If Citrix NetScaler is configured with the **User Name - LDAP Password - Security Code** authentication mode, select the **Simplified** method to generate the VIP integration code.

- 4 If Citrix NetScaler is configured with the **User Name - Security Code** authentication mode, select the **Manual** method. Then, you must select the **User Name + Security Code** authentication mode to generate the VIP integration code. If you are unsure about the value for the user name, password, security code, and form name fields, use the following values:

- User Name Field Name: **login**
- Password Field Name: **passwd**
- Security Code Field Name: **passwd1**
- Form Name: **Log_On**

Note: These values are retrieved from Citrix NetScaler 10.5. If you are using a different version of Citrix NetScaler, you must refer to the Sign-In page of your Citrix NetScaler module for the correct values.

IA does not support the User Name - LDAP Password - Security Code (Access Challenges Mode) authentication mode.

Updating the Citrix NetScaler Sign-In Page

Note: You can find the Citrix NetScaler Sign-In page at `/Netscaler/ns_gui/vpn/index.html`. Back up the Sign-In page file (`index.html`) before you paste the VIP integration code.

Perform the following steps to update the sign-in page of the module:

- 1 If you have generated the VIP integration code for the Citrix NetScaler module that is configured with the **User Name - LDAP Password - Security Code** authentication mode, you must copy the VIP integration code that you have generated in VIP Manager and paste it just before the `</BODY>` tag at the end of the `index.html` file.
- 2 If you have generated the VIP integration code for the Citrix NetScaler module that is configured with the **User Name - Security Code** authentication mode, you must do the following:
 - a Copy the VIP integration code that you have generated in VIP Manager and paste it just before the `</BODY>` tag at the end of the `index.html` file.
 - b In the `login.js` file, add the code that is highlighted in the following sample code to hide the `password2` field:

Note: The `password2` field will be filled automatically after the IA integration with the Citrix NetScaler module.

```
<SPAN style="display:none" class=CTXMSAM_LogonFont>' + _("Password2") + '</SPAN></TD>
<TD colspan=2 style="padding-right:8px;"><input class=CTXMSAM_ContentFont
type="Password" title="' + _("Enter password") + '" name="passwd1" id="passwd1"
size="30" maxlength="32" style="display:none" style="width:100%;"></TD></TR>');
```

Integrating JavaScript with Citrix NetScaler 11.0

This section describes the procedures for integrating JavaScript with Citrix NetScaler.

Updating JavaScript Integration Code for Citrix NetScaler 11.0

If you are using Citrix NetScaler version 11.0, you must update the JavaScript integration code in the following cases:

- “Citrix NetScaler 11.0 configured with User Name–Security Code validation server” on page 19
- “Citrix NetScaler 11.0 configured with User Name–Password–Security Code validation server” on page 21

Citrix NetScaler 11.0 configured with User Name–Security Code validation server

Perform the following steps if you have configured Citrix NetScaler 11.0 with User Name–Security Code validation server:

- 1 Open the `Index.html` file (located at `/netscaler/vpn_gui/vpn/`) and paste the following JavaScript code before the `</head>` tags.

```
<!-- BEGIN VIP integration code -->

<script type="text/javascript" src="https://userservices.vip.symantec.com/
vipuserservices/resources/js/v_1_0/vip?appId=<APPID>&idpURL=https://
<SSP_IDP_Proxy_URL>/dmzssp/DmzListener"> </script>

<script type="text/javascript">

function vipAuth()
{
var securitycodeField = $(' [name="passwd1"] ');
var passwordField = $(' [name="passwd"] ');
var formName = 'vpnForm';
var usernameField = $(' [name="login"] ');
var username = usernameField.val();
var password = passwordField.val();
try{ if (username && password) {
vip.genTicket({user:username, password:password}, function(success, ret) {
try{ if (success) {
securitycodeField.val(ret.ticket);
document.forms[formName].onsubmit=function (event){return true;};
document.forms[formName].submit(); }
else {alert("Fail; " + ret.toString());} }
catch(e){alert("In callback");}
}); } }
catch(e){ alert(e); }
return false;
}

</script>

<!-- END VIP integration code -->
```

- 2 In the earlier JavaScript IA code, update the **APPID** and **SSP_IDP_Proxy_URL** values as follows:
 - a **APPID**: Get the APPID from the VIP Manage Policy Configuration page. To get the APPID, do the following:
 - Log in to VIP Manager and navigate to **Account > VIP Policy Configuration > Account > Edit**.
 - Click the **VIP Integration Code for JavaScript** link to generate the code, select **Simplified** as the method to generate integration code, and then take the APPID.
 - b **SSP_IDP_Proxy_URL**: Provide the fully qualified domain name (FQDN) of the Self Service Portal IDP Proxy.
- 3 Open the `gateway_login_form_view.js` file (located at `/netscaler/vpn_gui/vpn/js`) and do the following:
 - a Search for the following code, and then add `'onClick': 'return vipAuth();'` at the appropriate place in the code:

```
var Login = $("<input type='submit'></input>").attr({'id': 'Log_On', 'value': 'Log On', 'class': 'custombutton login_page', 'disabled': 'disabled'}).appendTo(right_loginbutton);
```

For example:

```
var Login = $("<input type='submit'></input>").attr({'id': 'Log_On', 'value': 'Log On', 'class': 'custombutton login_page', 'disabled': 'disabled', 'onClick': 'return vipAuth();'}).appendTo(right_loginbutton);
```
 - b Search for the following code, and then add `"style": "display: none;"` at the appropriate place in the code to hide the **password2** field:

```
var enter_passwd2 = $("<input type='password'></input>").attr({'id': 'passwd1', 'class': 'prePopulatedCredentials', 'autocomplete': 'off', 'spellcheck': 'false', 'name': 'passwd1', 'size': '30', 'maxlength': '127', 'width': '180px'})
```

For example:

```
var enter_passwd2 = $("<input type='password'></input>").attr({'id': 'passwd1', 'class': 'prePopulatedCredentials', 'autocomplete': 'off', 'spellcheck': 'false', 'name': 'passwd1', 'size': '30', 'style': 'display: none;', 'maxlength': '127', 'width': '180px'})
```
 - c Search for the following code, and then add `$(password2).hide();` next to the code:

```
var password2 = $("<span></span>").addClass('plain input_labels form_text').attr("id", "Password2");
```

For example:

```
var password2 = $("<span></span>").addClass('plain input_labels form_text').attr("id", "Password2");
$(password2).hide();
```
- 4 Save the changes.

Citrix NetScaler 11.0 configured with User Name–Password–Security Code validation server

Perform the following steps if you have configured Citrix NetScaler 11.0 with User Name–Password–Security Code validation server:

- 1 Open the `Index.html` file (located at `netScaler/vpn_gui/vpn/`) and paste the following JavaScript code before the `</head>` tags.

```
<!-- BEGIN VIP integration code -->
<script type="text/javascript" src="https://userservices.vip.symantec.com/
vipuserservices/resources/js/v_1_0/vip?appId=<APPID>&idpURL=https://
<SSP_IDP_Proxy_URL>/dmzssp/DmzListener"> </script>
<script type="text/javascript">
function vipAuth()
{
var passwordField = $(' [name="passwd"] ');
var formName = 'vpnForm';
var usernameField = $(' [name="login"] ');
var username = usernameField.val();
var password = passwordField.val();
try{ if (username && password) {
vip.genTicket({user:username, password:password}, function(success, ret) {
try{ if (success) {
passwordField.val(password + ret.ticket);
document.forms[formName].onsubmit=function (event){return true;};
document.forms[formName].submit(); }
else {alert("Fail; " + ret.toString());} }
catch(e){alert("In callback");}
}); } }
catch(e){ alert(e); }
return false;
}
</script>
<!-- END VIP integration code -->
```

- 2 In the above JavaScript code, update the **APPID** and **SSP_IDP_Proxy_URL** values as follows:
 - a **APPID**: Get the APPID from the VIP Manage Policy Configuration page. To get the APPID, do the following:
 - Log in to VIP Manager and navigate to **Account > VIP Policy Configuration > Account > Edit**.
 - Click the **VIP Integration Code for JavaScript** link to generate the code, select **Simplified** as the method to generate integration code, and then take the APPID.
 - b **SSP_IDP_Proxy_URL**: Provide the IP address or name of the Self Service Portal IDP Proxy.
- 3 Open the `gateway_login_form_view.js` file (located at `/netScaler/vpn_gui/vpn/js`) and do the following:
 - Search for the following code, and then add `'onClick': 'return vipAuth();'` at the appropriate place in the code:

```
var Login = $("<input type='submit'></input>").attr({'id': 'Log_On', 'value': 'Log
On', 'class': 'custombutton login_page', 'disabled': 'disabled'}).
appendTo(right_loginbutton);
```

For example:

```
var Login = $("<input type='submit'></input>").attr({'id':'Log_On','value':'Log On','class':'custombutton login_page','disabled':'disabled','onClick':'return vipAuth();'}).appendTo(right_loginbutton);
```

- 4 Save the changes.

Testing the JavaScript Integration

Perform the following steps to test the JavaScript integration:

- 1 Access the Citrix NetScaler VPN URL.
- 2 Enter a valid user name and password.
- 3 Click **Continue**. The Confirm Your Identity window is displayed.



Figure 3-1 Confirm Your identity window

- 4 Enter a valid security code.
- 5 Select the **Remember this private device** check box, and click **Continue**.

You can access the protected resource after successful authentication. In the next login, you will not be prompted for the security code as you have opted to remember the device.

Adding LDAP Authentication Server and Policy

This appendix describes the following topics:

- [“Adding LDAP Authentication Server”](#) on page 23
- [“Adding the LDAP Authentication Policy”](#) on page 24

Adding LDAP Authentication Server

Perform the following steps to add the LDAP Authentication Server:

- 1 In the navigation pane, expand **System > Authentication** and select **LDAP**.
- 2 From the **Servers** tab, click **Add**.
- 3 In the Create Authentication Server dialog box, type a name for the server in the **Name** field (for example, "NetScaler_AD").
- 4 In the **Server** section, enter the following:
 - IP address for the LDAP server
 - Port
 - Time-out value in seconds
- 5 Under **Connection Settings**, enter the **Base DN**, **Administrator Bind DN**, and **Administrator Password**. Confirm your **Administrator Password**.
- 6 Under **Other Settings**, enter the **Server Logon Name Attribute**, **Search Filter**, **Group Attribute**, and **Sub Attribute Name**.
- 7 For **Security Type**, select **Plain Text**, and select the **Authentication** and **User Required fields** check boxes.
- 8 Click **Create**.

Adding the LDAP Authentication Policy

Perform the following steps to add the LDAP Authentication Policy:

- 1 From the **Policies** tab, click **Add**.
- 2 In the Create Authentication Policy dialog box, type a name for the policy in the **Name** field.
- 3 Select the authentication server created previously (for example, “NetScaler_AD”).
- 4 Under **Expression**, you can add your own expression according to the policy.

Note: For test purposes only, **ns_true** was added as the **Expression**. Add the appropriate policy according to your enterprise requirement.

- 5 Click **Create**.

Customizing the Citrix NetScaler Login Page

This appendix describes how you can customize the login page for Citrix NetScaler.

Customizing the Login Page for Citrix NetScaler 11.0

Perform the following steps to customize the login page for Citrix NetScaler version 11.0:

- 1 Log in to the Citrix NetScaler Admin console and navigate to **Configuration > NetScaler Gateway > Portal Themes**.
- 2 Click **Add** to add a new theme, enter the new theme name, select the theme template (for example, GreenBubble), and then click **OK** to save the changes.
- 3 Click **OK** on the Portal Theme page to save the changes, and click **Back** to return to the Portal Theme page.
- 4 Select the theme that you created, and click **Edit**.
- 5 In **Advanced** settings, click the Login page, change the **password** and **password2** field labels as per your requirement, and click **OK** to save the changes.
- 6 Click the **click to bind and view configured theme** link to verify the changes, and then click **Done**.
- 7 Save the NetScaler configuration.

Customizing the Login Page for Citrix NetScaler 10.x

To customize the login page for Citrix NetScaler version 10.x, refer to the following article – <http://support.citrix.com/article/CTX126206>

