



Integrating RSA SecurID with Citrix NFuse 1.6 and Project Columbia 6.00.030

By Citrix Consulting Services

Citrix Systems, Inc.



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 NON-INFRINGEMENT. CITRIX SYSTEMS, INC. ("CITRIX"), SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR DIRECT, INCIDENTAL, CONSEQUENTIAL OR ANY OTHER DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS PUBLICATION, EVEN IF CITRIX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

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

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

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

Copyright © 2001 Citrix Systems, Inc., 6400 NW 6th Way, Ft. Lauderdale, Florida 33309 U.S.A. All rights reserved.

Version History		



Table of Contents

INTRODUCTION	1
DOCUMENT OVERVIEW	1
CITRIX NFUSE	1
PROJECT COLUMBIA	2
RSA SECURID	2
CITRIX SECURE GATEWAY	2
ARCHITECTURE	4
NFUSE ARCHITECTURE WITH PROJECT COLUMBIA	4
NFUSE ARCHITECTURE WITH THE PROJECT COLUMBIA, RSA SECURID, AND CITRIX SECURE GATEWAY	5
<i>External Access</i>	6
<i>Internal Access</i>	7
LOGIN PROGRESS	9
RSA SECURID NOT INTEGRATED WITH NFUSE	9
RSA SECURID INTEGRATED WITH NFUSE	10
<i>External User Login</i>	11
<i>Internal User Login</i>	13
APPLICATION INSTALLATION AND WEB SITE CREATION	15
REQUIRED COMPONENTS	15
CONFIGURATION FILE CHANGES	15
<i>Web Site Creation and Configuration</i>	15
<i>Virtual Web Site Creation</i>	15
<i>RSA SecurID Configurations</i>	16
CODE MODIFICATIONS	17
<i>Useridandpasscode.htm</i>	17
<i>Login.asp</i>	22

Introduction

Document Overview

An important concern when implementing a Citrix NFuse application portal Web site is making published applications and other resources available to authorized users through an intranet, a WAN or even the Internet. Using two-factor authentication, RSA SecurID provides additional login security to prevent unwelcome access to an application portal. However, RSA SecurID also has the potential to increase the number of logins required to access the NFuse Web site, thus diminishing a user's overall satisfaction with an NFuse solution.

Another important concern with an NFuse implementation is that a MetaFrame environment can be left open to people who can make a direct ICA connection to published applications through the Internet or through other means. Furthermore, pre-FR1 for MetaFrame XP servers do not provide the functionality to encrypt traffic to and from clients utilizing SSL, and the MetaFrame servers' addresses have to be visible from outside the firewall. In an effort to secure ICA communication, the Citrix Secure Gateway can be implemented in conjunction with NFuse and RSA SecurID.

This document outlines an integrated solution to provide secure encrypted communication and to reduce the number of required logins to access an NFuse Web site implemented with Project Columbia 6.00.030 while retaining the advanced security features of RSA SecurID. The following topics are discussed:

- Solution components
- Architecture
- Login Progress
- Application Installation and Web Site Creation

It is assumed that the reader has knowledge of the Citrix Secure Gateway or has read the Citrix Secure Gateway Administrator Guide.

Citrix NFuse

The Citrix NFuse application portal allows organizations and application service providers (ASPs) to publish unmodified interactive applications to a standard Web browser. Customers can integrate and publish interactive applications into any standard Web browser. Administrators retain all the robust features and benefits of Citrix MetaFrame while getting business and productivity applications across the Web to users quickly and cost-effectively.

NFuse has the following benefits:

- Improved application management
- Faster deployment
- Reduced administrative costs
- Leverage of existing infrastructure
- Increased user productivity
- Security (SSL, encryption, ticketing)

On the client side, users benefit from the ease of using a familiar Web browser as their central interface to all published applications, as well as other portal content, tools and resources. With NFuse, all these systems can be viewed and interacted with as if they were a single system. Furthermore, NFuse can accommodate any level of personalization from a presentation (look) standpoint to an organization (feel) standpoint.

On the server side, Citrix MetaFrame provides single-point control, allowing applications and application content to be customized by user or by group. Application management is centralized through the deployment of applications in a controlled and monitored server environment as opposed to individual desktop deployments.

Project Columbia

Project Columbia 6.00.030 is a sample NFuse Web site that has been customized by Citrix Technical Support to address common features that may be desired by clients. The Web pages and files included in Project Columbia are based on the default example site included with NFuse, but they have been customized to implement these additional features.

Project Columbia 6.00.030 allows you to implement the following features, without requiring additional development of the example Web scripts:

- Override the Web server's default MetaFrame server farm address
- Identify multiple XML services per server farm for fault tolerance and load-balancing
- Merge application sets from multiple server farms
- Serve internal users and external users connecting through Network Address Translation from the same Web site
- Route ICA client sessions through client-side SOCKS Proxy servers
- Route users to multiple internal MetaFrame servers through a single external IP address using Port Address Translation
- Allow users to change expired NT4 or Active Directory domain passwords
- Force the installation of ICA clients to Windows users who do not already have an ICA client installed
- Hide applications or folders by name
- Alter the size and layout of application icons
- Offer the user a menu of Domains during login

Refer to the Project Columbia 6.00.030 help.htm file for additional details.

RSA SecurID

RSA Security, Inc., produces a popular suite of computer security hardware and software known as RSA SecurID. RSA SecurID tokens are portable, hand-held devices that generate a unique, one-time numeric code every sixty seconds that you combine with your secret PIN when logging into protected resources. A broad range of easy-to-use authentication form factors is available – including hardware tokens, software tokens (resident on PCs, PDAs, and wireless phones), and smart cards. The RSA ACE/Server is the authentication engine on the network that controls an organization's security policy regarding who accesses which resources. For more information about RSA SecurID, visit the [RSA Web site](#).

Citrix Secure Gateway

Citrix Secure Gateway is a secure Internet gateway for ICA traffic into and out of a MetaFrame enabled corporate environment over existing public networks, such as the Internet, or in some cases through a corporate WAN. Citrix Secure Gateway safely and easily extends access to Citrix server farms over the Internet to remote workers and telecommuters in a simplified, cost effective and secure manner. Citrix Secure Gateway leverages existing Citrix technologies, and security infrastructure to provide an ICA specific security layer to protect Citrix client-server communications on your network.

Citrix Secure Gateway works with Citrix NFuse to provide a single, secure, encrypted point of access through the Internet, to Citrix servers on internal corporate networks. This means office workers can access corporate information remotely, without compromising network security from anywhere in the world, from any device and at all times. Citrix Secure Gateway can also operate in a corporate environment to secure internal data communications on a LAN or WAN. Whether Citrix Secure Gateway is used for internal or remote access, this service transparently encrypts and authenticates all ICA connections to protect against eavesdropping and data tampering.

Citrix Secure Gateway has the following benefits:

- Denies direct access to internal resources from the Internet

- Can use two-factor authentication without touching MetaFrame servers
- Provides simplified client firewall traversal
- Not susceptible to man-in-the-middle attacks
- Requires fewer certificates than ICA/SSL client/server
- Works with different internal and external DNS namespaces

Architecture

NFuse Architecture with Project Columbia

The NFuse Web server functions as a Web-based Program Neighborhood interface for connecting to a Citrix server farm. The NFuse Web server queries the MetaFrame server farm for application set information and then formats the results into HTML pages that a user can view in a Web browser.

To communicate with the Citrix server farm, the NFuse Web server contacts the Citrix XML Service running on one or more MetaFrame servers. The Citrix XML Service is a MetaFrame component that provides published application information to ICA clients and NFuse Web servers using TCP/IP. This service functions as the contact point between the server farm and NFuse's Web server component. The Citrix XML Service is installed with MetaFrame XP for Windows systems, and Citrix MetaFrame 1.1 Feature Release 1 for UNIX Operating Systems on UNIX systems.

The Web server in an NFuse system hosts the NFuse Java objects and Web server-side scripts. The NFuse Java objects provide the following services:

- Authenticate users to a Citrix server farm
- Retrieve application information, including a list of applications a user can access
- Provide administrators the ability to modify the properties of individual applications before presenting them to users

NFuse Java objects are added to the Web server during NFuse installation. This installation program also adds Web pages and configuration files.

In the context of NFuse, an ICA client device is any computing appliance capable of executing an ICA client and a Web browser. ICA client devices include desktop PCs and network computers, among others.

In an ICA client device, the Web browser and ICA client work together as a viewer and engine. The Web browser lets users view application sets (created by server-side scripting on the NFuse Web server) while the ICA client acts as the engine that launches published applications.

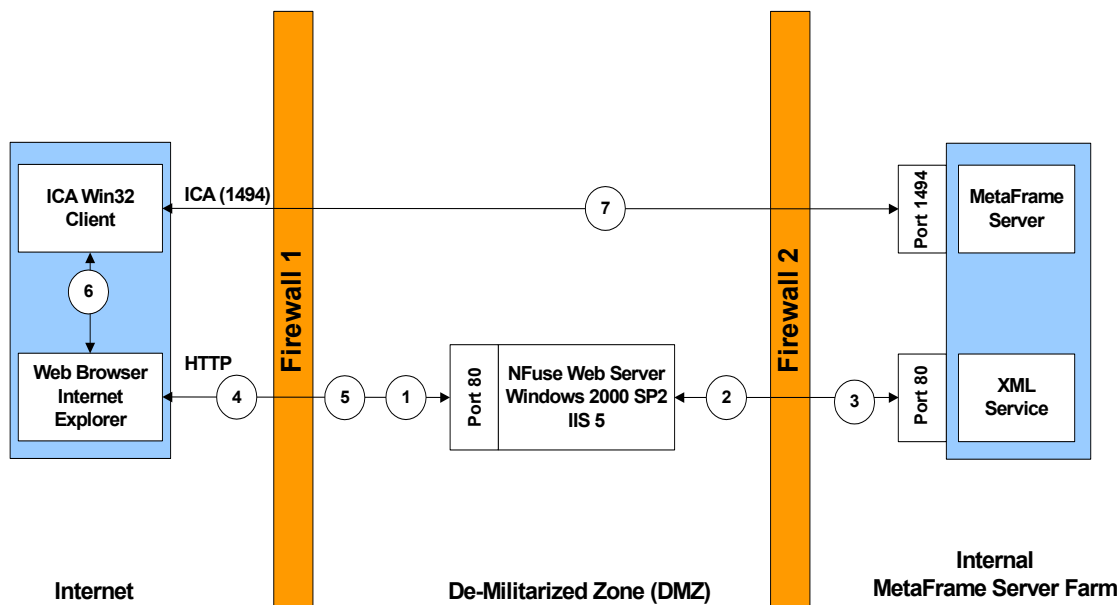



Figure 1: Citrix NFuse Architecture

As illustrated in Figure 1, the following communications take place among the Citrix NFuse components before a secure connection is established.

NOTE: The figure shows NFuse being run on a Windows 2000 Server with IIS 5.0. However, NFuse can also be run using IIS 4.0 on Windows NT 4.0 Server and Windows NT 4.0 Server, Terminal Server Edition.

1. An ICA client device user uses a Web browser to view the NFuse login page and enters his or her user credentials. The credentials are sent as a standard HTTP request over the default HTTP port 80.

NOTE: Although HTTP is the default, it is recommended that SSL (HTTPS) be used to secure the communication between the client and NFuse Web server.

-  2. The Web server reads the user's information and uses the NFuse Java objects to forward the information to the Citrix XML Service on a Citrix server in the server farm. The designated server acts as a broker between the Web server and the Citrix server farm.
3. The Citrix XML Service on the designated server then retrieves from the farm a list of applications that the user can access. These applications comprise the user's *application set*. XML Service retrieves the application set from the Independent Management Architecture (IMA) system and Program Neighborhood Service, respectively.

The Citrix XML Service then forwards the user's application set information to the NFuse Java objects running on the Web server.
4. The Web server uses the NFuse Java objects to generate an HTML page containing links to the applications in the user's application set. Each hyperlink in the HTML page points to a template file stored on the Web server. This file serves as a template from which NFuse can dynamically generate ICA files. ICA files are text files containing parameters that configure ICA session properties such as the application to run in the session, the address of the server that will execute the application, and the properties of the window in which to display the application. ICA files are written in .ini file format and have an .ica extension.
5. The user initiates the next step by clicking one of the hyperlinks in the HTML page. The Web browser sends a request to the Web server to retrieve an ICA file for the selected application.

The Web server passes this request to the NFuse Java objects, which retrieve the template ICA file. The template file contains substitution tags. The Java objects replace the substitution tags in the template ICA file with information specific to the user and desired application. The Java objects then send the customized ICA file to the Web browser.
6. The Web browser receives the ICA file and passes it to the ICA client device.
7. The ICA client receives the ICA file and initiates an ICA session with a Citrix server according to the ICA file's connection information.

NFuse Architecture with the Project Columbia, RSA SecurID, and Citrix Secure Gateway

As with any Web site, the NFuse Web site can be secured using RSA SecurID. The appropriate RSA ACE client or equivalent software needs to be installed on the NFuse Web server and then configured to secure NFuse Web site. If Microsoft Internet Information Server is used, then the RSA ACE client will add an additional tab to the "Properties" dialog box in the Information Services Manager. Security can be set on an individual Web site as well as on a particular required section of Web site. With RSA SecurID, a Web site can be set up explicitly for users who want to access NFuse externally from the Internet. Users who access NFuse externally would be required to provide their RSA SecurID passcode along with their user credentials on a single login page. A separate Web site can also be set up for users who to access NFuse from an internal LAN.

In order to secure ICA traffic coming in over the Internet, the Citrix Secure Gateway can be installed in the DMZ (de-militarized zone) as a security perimeter that protects MetaFrame resources and applications on the corporate intranet. Citrix Secure Gateway works with NFuse to provide a single, secure, encrypted point of access through the Internet to MetaFrame servers on internal corporate networks.

The integrated solution involves the following network components:

- MetaFrame XP or MetaFrame 1.1 for UNIX server farm
- A Citrix Secure Gateway server
- A Citrix NFuse 1.6 enabled Microsoft IIS 5.0 Web server with two virtual Web sites defined, one for internal access and one for external access.
- Project Columbia 6.00.030 or above installed on the NFuse Web server
- RSA ACE/Agent 5.0 for Windows installed on the NFuse Web server
- A Secure Ticket Authority (STA) server, a component of the Citrix Secure Gateway solution
- A client device with the ICA Win32 client, version 6.20 or higher, and Internet Explorer 4.x or above with high encryption

The next two sections illustrate how the various components interact to provide security for users accessing an NFuse Web site both externally and internally to a network

External Access

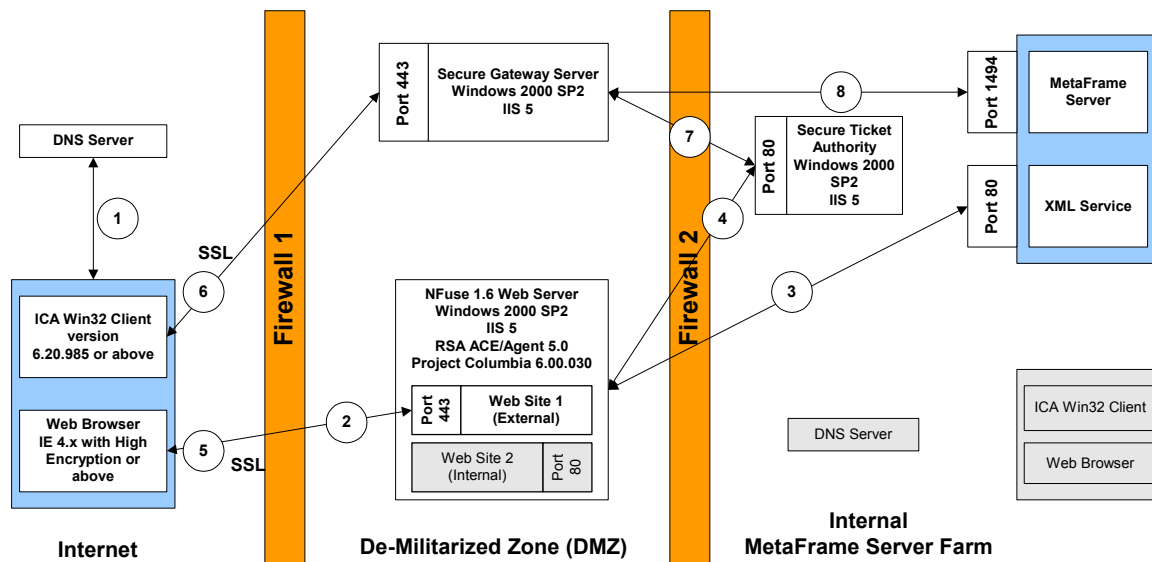


Figure 2: External Web Site Communication Path

As illustrated in the figure above, the following communication takes place to establish a secure connection using the external virtual Web site.

1. A remote user launches a Web browser with a specified URL. The client queries an external DNS service, which replies with the address of the external Web site.
2. The user connects to the external Web site on the NFuse Web server on port 80 (HTTP) or port 443 (HTTPS) and is presented with a login screen. Security can be increased by the deployment of a secure NFuse Web server (HTTPS). The NFuse Web page requires the user to authenticate using his or her user credentials.

The Web site can be further secured with RSA SecurID. Securing an NFuse Web site with RSA SecurID redirects the initial Web page request from an NFuse login page to an RSA SecurID login page. Once authenticated, the user is redirected back to the NFuse login page. The RSA SecurID login page can be combined with the RSA login and NFuse login page into a single Web page to simplify the user experience. The user is authenticated against RSA SecurID and, if authentication is successful, automatically logs in to NFuse.

3. NFuse uses the user's credentials to contact the XML Service on a MetaFrame server and obtain a list of applications that the user is authorized to access. NFuse then populates the Web page with the list of published applications that the user is authorized to access.
4. When the user clicks on a published application link, NFuse sends the IP address for the requested MetaFrame server to the STA and requests a Citrix Secure Gateway ticket for the user. The STA saves the IP address and issues the requested Citrix Secure Gateway ticket to NFuse.
5. NFuse generates an ICA file containing the ticket issued by the STA and sends it to the client browser.
6. The client browser passes the ICA file to the ICA client, which then launches an SSL (Secure Socket Layer) connection to the Citrix Secure Gateway. Initial SSL handshaking is performed to establish the identity of the Citrix Secure Gateway server.
7. The Citrix Secure Gateway server accepts the ticket from the ICA client and uses information contained in the Citrix Secure Gateway ticket to identify and contact the STA for verification. If the STA is able to validate the ticket, it returns an IP address of the MetaFrame server on which the requested application resides. If the ticket is invalid, or has expired, the STA informs the Citrix Secure Gateway server, and a client error message is displayed.
8. On receipt of the IP address for the MetaFrame server, the Citrix Secure Gateway server establishes an ICA connection between the ICA client and the MetaFrame server. The Citrix Secure Gateway server monitors data flowing through the connection, and encrypts/decrypts client-server communications.

Internal Access

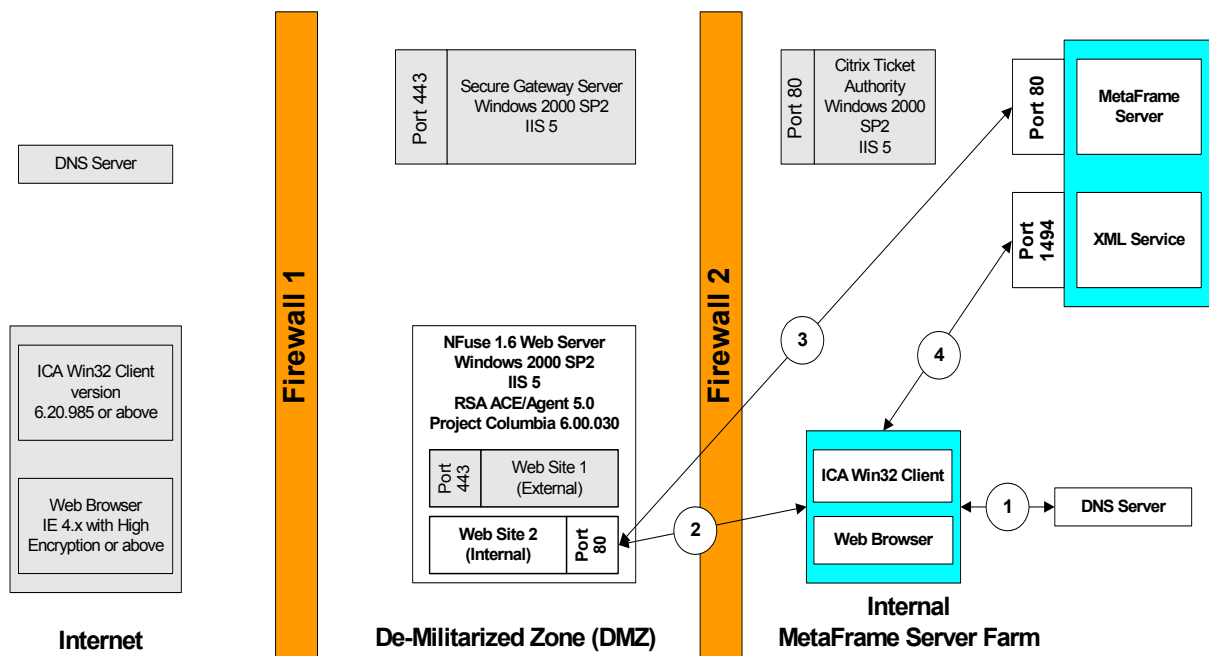


Figure 3: Internal Web Site Communication Path

As illustrated in the figure above, the following communications take place before a connection is established using the internal virtual Web site.

1. A user on the LAN launches a Web browser with a specified URL. The client queries an internal DNS service, which replies with the address of the internal Web site.
2. The user connects to the NFuse Web server on port 80 (HTTP) and is presented with a login screen. The NFuse Web page requires the user to authenticate using his or her user credentials.
3. NFuse uses the user credentials to contact the XML Service on a MetaFrame server and obtain a list of applications that the user is authorized to access. NFuse then populates the Web page with the list of published applications that the user is authorized to access. Columbia 6.00.030 configuration settings exist that allow the declaration of internal IP address ranges that would bypass the Citrix Secure Gateway.
4. The user initiates the next step by clicking one of the hyperlinks in the HTML page. The Web browser sends a request to the Web server to retrieve an ICA file for the selected application. The Web browser receives the ICA file and passes it to the ICA client device. The ICA client receives the ICA file and initiates an ICA session with a Citrix server via port 1494 according to the ICA file's connection information.

Login Progress

RSA SecurID Not Integrated with NFuse

With a standard configuration, the RSA ACE client adds an initial RSA login page that is presented on a user's first attempt to access the NFuse Web site.

RSA SecurID User Name and PASSCODE Request

The page you are attempting to access requires you to authenticate using your SecurID token.

Enter your User Name and SecurID PASSCODE in the following fields, and then click "Send." If you make a mistake, use "Reset" to clear the fields.

Username:

PASSCODE:

Figure 4: RSA SecurID Login Page

This RSA SecurID login page is displayed *before* NFuse login page. It is here that the user keys in the unique passcode generated from the SecurID token device. From the user's point of view, it appears to be a double login, since the user is prompted once again to access the NFuse Web site.

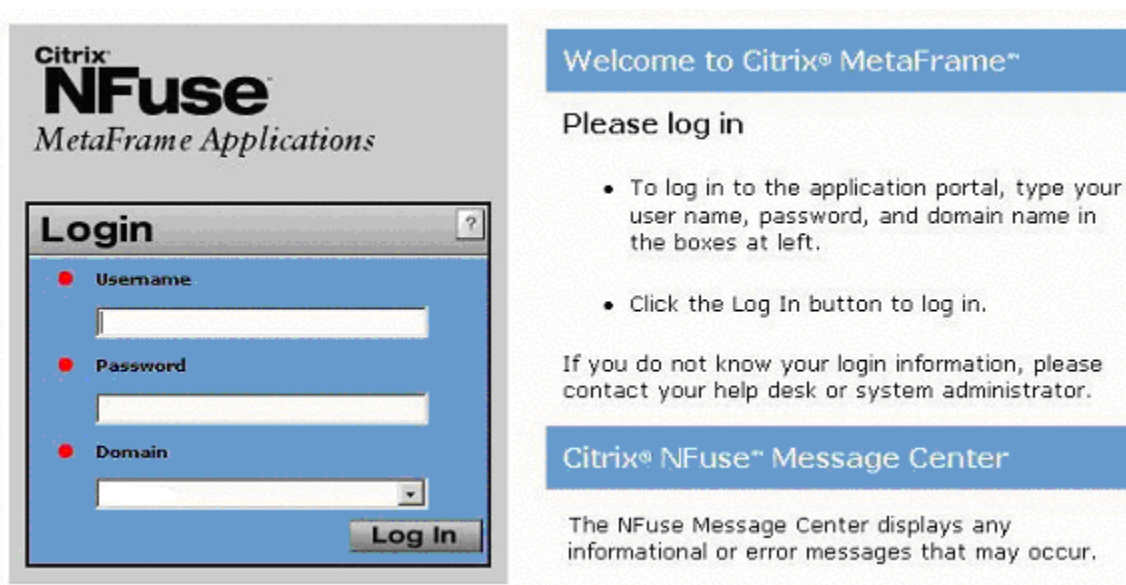


Figure 5: Citrix NFuse Login Page

This double login is undesirable because it diminishes the user's overall experience. The double login problem, however, can be resolved by creating custom login page that will ask for all required information for both RSA and NFuse authentication.

RSA SecurID Integrated with NFuse

In order to have a single login page, the NFuse credential fields need to be incorporated to the RSA login page. Because some of the fields (user name, for example) are typically the same for both the RSA and NFuse logins, it is possible to use a single input field for this type of information.

Because of the specifics of RSA login page processing, only user name and the RSA SecurID passcode should be submitted for login processing. The rest of the fields should be saved somehow for NFuse login processing that will take place right after successful RSA login. One of the possible ways to achieve this is to make RSA login page save entered NFuse credentials in a temporary cookie on the client. After RSA login processing occurs, NFuse login page is invoked. NFuse reads the saved credentials from the cookie to skip the default NFuse login page. At the same time the cookie with NFuse login credentials is destroyed.

If the RSA login fails, RSA login page will be re-displayed, and this page can immediately destroy the cookie with the NFuse credentials. Even if the connection terminates after the RSA login occurs, and the cookie is not destroyed by NFuse pages, the cookie will be automatically destroyed by the Web browser as soon as the browser is closed. In other words, the cookie is never stored in the client's persistent storage.

The following diagram depicts the integration of RSA SecurID with NFuse and the Citrix Secure Gateway from the perspective of the user:

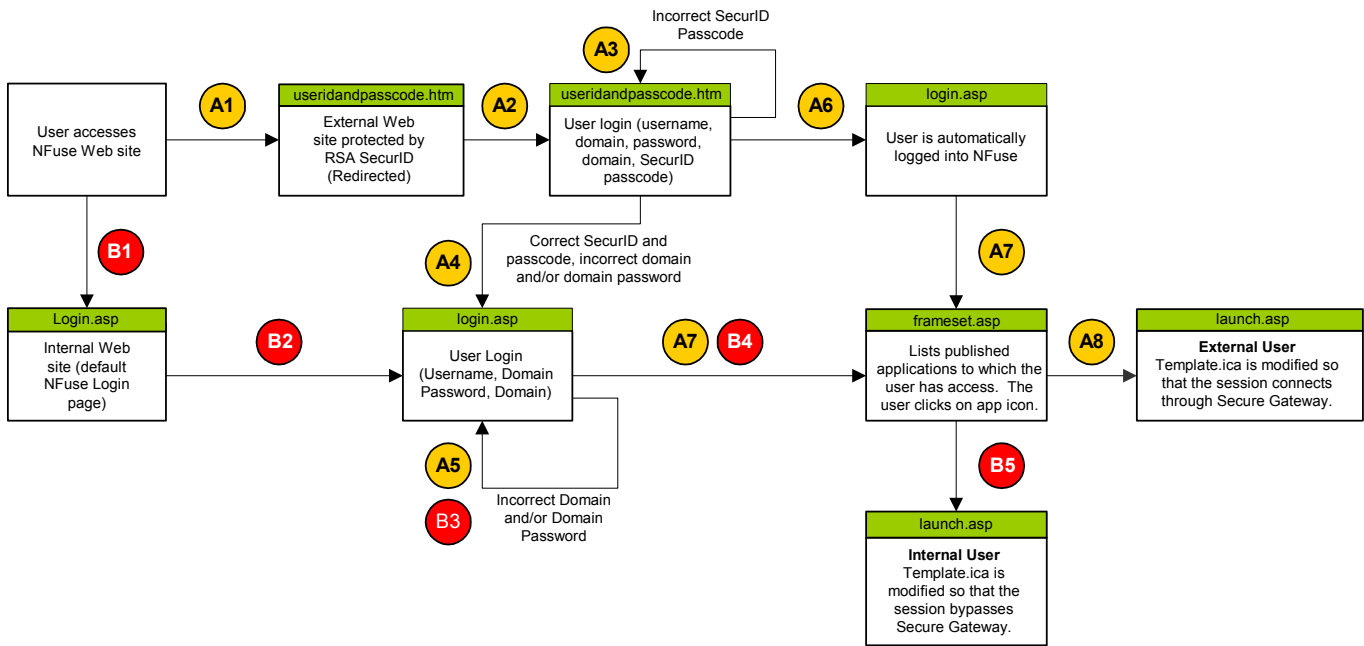


Figure 6: RSA SecurID Integration with NFuse

External User Login

The following steps outline the possible process flows that may be experienced by an external user.

- A1. An external user visits the Web site. RSA SecurID protects the external Web site. As a result, the external user is redirected to a customized single login Web page (`useridandpasscode.htm`).

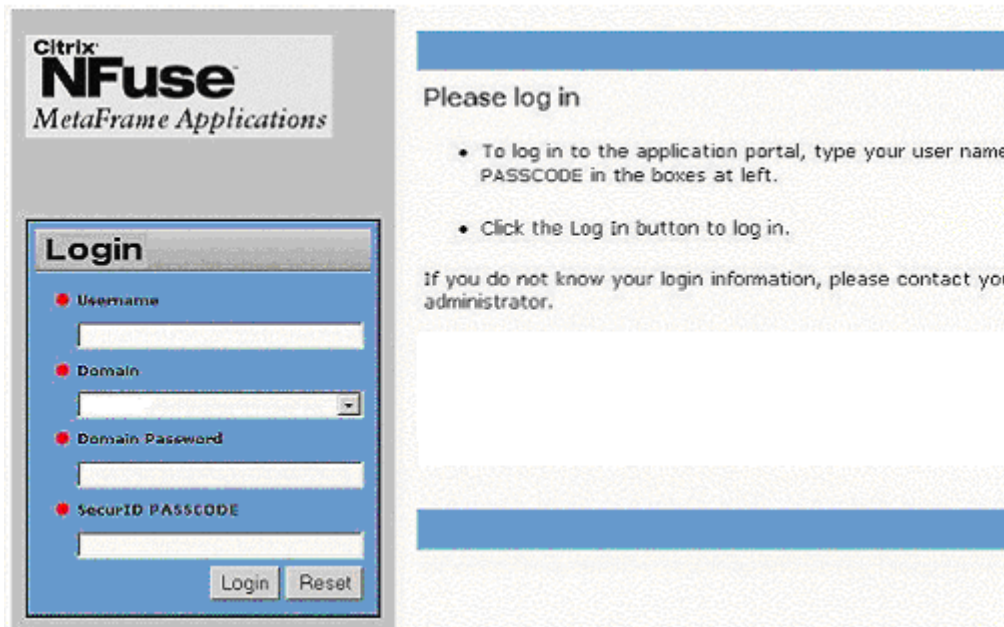


Figure 7: Login page for external access users

- A2. The external user is prompted to enter his or her username, domain password, domain, and SecurID passcode.
- A3. If the external user enters an incorrect SecurID passcode, the user is returned to the single login page.
- A4. If the external user enters the SecurID passcode correctly but had previously entered an incorrect domain and/or domain password, the user is redirected to just the NFuse login page. This is the same NFuse login page that internal users access directly.
- A5. If the external user once again enters either an incorrect domain and/or domain password, the user is returned to the NFuse login page.
- A6. If the external user enters all his credentials correctly, the user is automatically logged into the NFuse Web site.

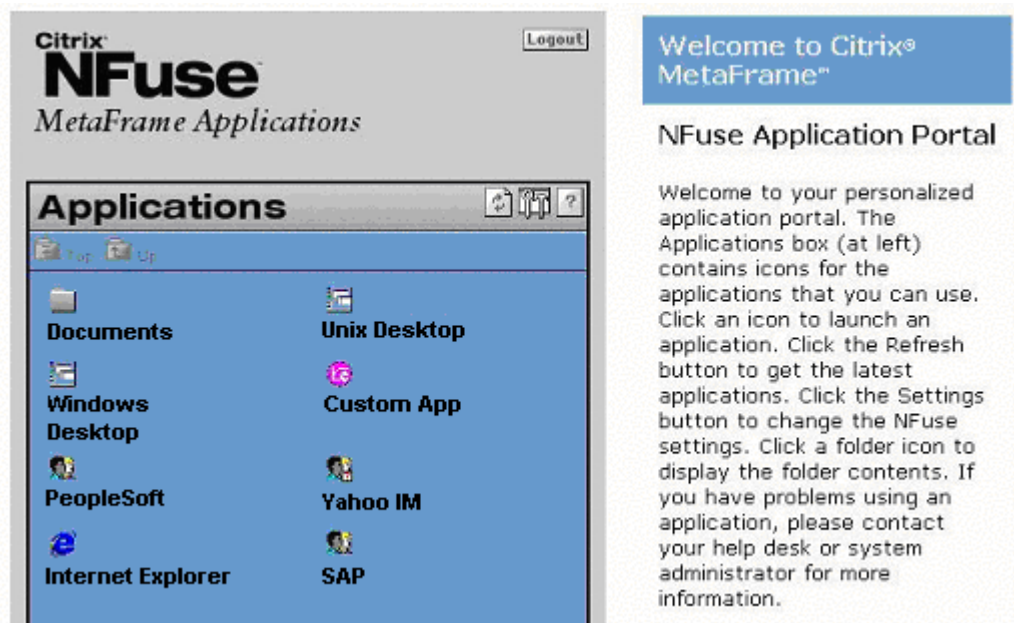


Figure 8: Application list for logged in user

- A7. Once logged into the NFuse Web site, the external user is presented with a list of published applications.
- A8. If the external user launches a published application, that session is connected through the Citrix Secure Gateway server. This will be indicated by the phrase "128-bit SSL in use" when the user performs a mouse-over on the published application in the task bar or when the user launches the ICA Connection Center.

Internal User Login

The following steps outline the process flows that an internal user may experience.

- B1. An internal user visits the Web site. Since RSA SecurID does not protect the internal Web site, the user is directed to the NFuse login page.

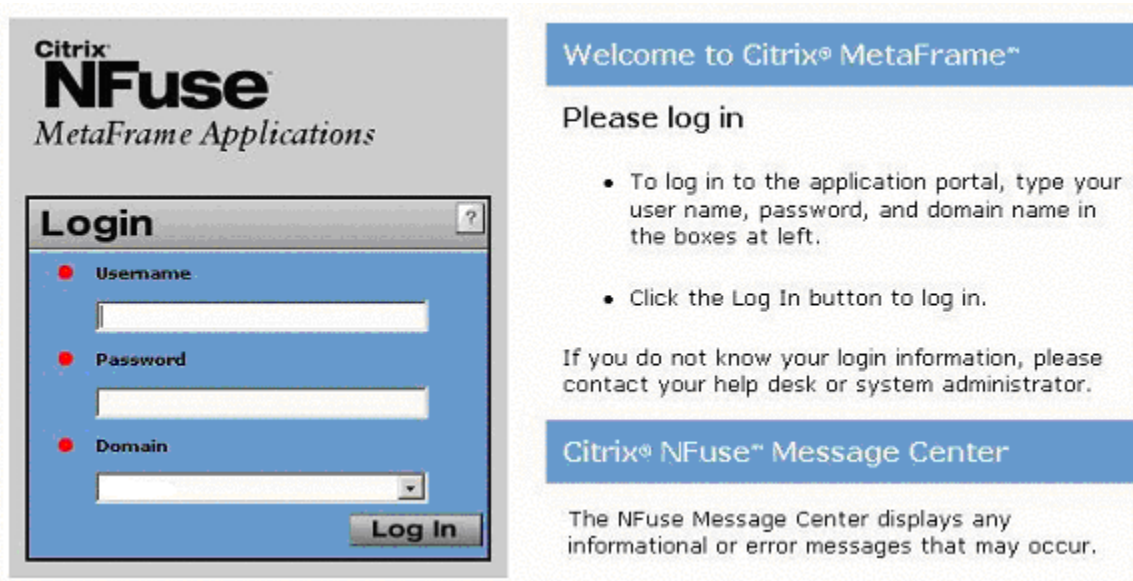


Figure 9: Login page for internal access users

- B2. The internal user is prompted to enter his or her username, domain password, and domain.
- B3. If the internal user enters an incorrect domain and/or domain password, the user is returned to the NFuse login page.
- B4. Once logged into the NFuse Web site, the internal user is presented with the list of published applications.
- B5. If the internal user launches a published application, that session bypasses the Citrix Secure Gateway server.

Application Installation and Web Site Creation

Required Components

The following components are required when integrating RSA SecurID with Citrix NFuse 1.6 and Project Columbia 6.00.030:

- Citrix NFuse 1.6
- Project Columbia 6.00.030
- RSA SecurID
 - ACE Agent 5.0
 - ACE Agent 4.1
- Citrix Secure Gateway

Refer to the appropriate component administrator's guide for installation instructions.

Configuration File Changes

Refer to the Project Columbia 6.00.030 help.htm file for details on how to configure the Columbia 6.00.030 config.txt file located in the Project Columbia NFuse Web site on the NFuse Web Server. This file needs to be updated to include the parameters listed below:

- **CSG_Enable=ON** – This parameter enables the Columbia 6.00.030 to use the Citrix Secure Gateway. The “ON” value is case sensitive.
- **CSG_STA=<server_name>:80** – This parameter indicates the server name and port number for the STA server.
- **CSG_Gateway=<FQDN>:443** – This parameter indicates the FQDN and port number of the Citrix Secure Gateway server.
- **CSG_InternalNetworks=<ip_range>** – This parameter indicates the internal IP address ranges that are not subjected to the Citrix Secure Gateway. As a result, client devices with the defined internal IP addresses do not have their ICA connection protected by the Citrix Secure Gateway server. An example is `CSG_InternalNetworks=10., 198.127`. Therefore, any client device with the 10. or 198.127 IP address range would not be subjected to the Citrix Secure Gateway.

Web Site Creation and Configuration

Virtual Web Site Creation

In order to utilize a single NFuse web site for external and internal access, you will need to create two virtual Web sites on the IIS server. Each web site will have its own IP address and will point back to the same set of Project Columbia files. This section explains how to use Internet Services Manager to create a new virtual Web site that has its own IP address.

Requirements

The following are requirements for a virtual Web site:

- A static Internet Protocol (IP) address for the Web site to use.
- A Windows Web server that is running either Internet Information Server (IIS) 4.0 or Internet Information Services (IIS) 5.0.
- Administrative rights on the server computer.

- The Project Columbia files copied to the wwwroot of the IIS server.

How to Create the Virtual Web Site on IIS 5.0

1. To create the virtual Web site on IIS 5.0, use the steps in one of the following sections.
On the **Start** menu, point to **Programs**, point to **Administrative Tools**, and then click **Internet Services Manager**.
2. In the Console tree in the left pane, right-click your computer name, point to **New**, and then click **Web Site**.
3. On the first page of the Web Site Creation Wizard, click **Next**.
4. On the second page, type a name for the site (for example, type **myWebsite**), and then click **Next**.
5. On the third page, in the **Enter the IP address** drop-down list box, click the IP address that you have assigned to this Web site. Leave the **Port** number at the default (which is normally 80), and leave the **Host Header for this site** text box blank. Click **Next**.
6. On the fourth page, click **Browse**. Browse to the content folder (e.g. the wwwroot where the Project Columbia files reside). If this Web site is intended for public use, make sure that the **Allow anonymous access to this Web Site** check box is selected. If this Web site is intended to be available to specific users only, clear this check box. Click **Next**.
7. On the fifth page, select the **Read** and **Run scripts (such as ASP)** check boxes. Make sure that the other boxes are cleared. Click **Next**, and then click **Finish** to complete the wizard.

Refer to Microsoft article Q300991 "HOW TO: Create a New Virtual Web Site with Its Own IP Address" for further details on how to create virtual Web sites.

RSA SecurID Configurations

Web Site (External Access)

The RSA SecurID client protects this Web site. The following RSA client configuration settings need to be made for the external access Web site maintained on the NFuse Web server:

1. Launch the Internet Services Manager on the NFuse Web server.
2. Open the Properties window for the Web site.
3. Select the "RSA SecurID" tab. Below is a screen shot of the RSA configurations tab.

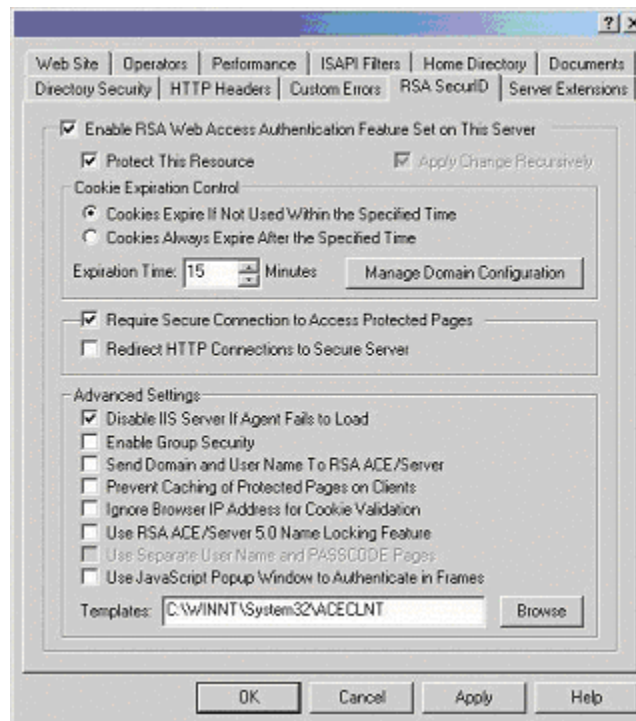


Figure 10: RSA SecurID Settings

4. Check "Enable RSA Web Access Authentication Feature Set on This Server."
5. Check "Protect This Resource."
6. Check "Require Secure Connection to Access Protected Pages" (optional).
7. Check "Disable IIS Server If Agent Fails to Load" (optional).

Since the Web site is protected, RSA SecurID authentication is required before access is allowed to the NFuse Web pages.

Web Site (Internal Access)

The RSA SecurID is not needed to protect this virtual Web site since only internal users will be accessing this site.

Code Modifications

In order to implement the single login RSA SecurID Web site, the `useridandpasscode.htm` (e.g. `%systemroot%\system32\aceclnt`) file used by RSA SecurID and the `login.asp` (e.g. `inetpub\wwwroot`) file used by NFuse need to be customized.

Useridandpasscode.htm

The `useridandpasscode.htm` page is the Web page that the external user is redirected to when he or she visits the NFuse Web site. This page has been modified to prompt the user to enter their username, domain password, domain, and RSA SecurID passcode. The login process is initiated by either selecting the Login button or after the user hits the Enter key once the user has entered a value in the SecurID passcode field. Once login has been invoked, RSA SecurID authentication is initiated first

while the username, domain password, and domain values entered by the user are written to a cookie that would be used by the NFuse login process.

Built into RSA HTML files are substitution macros in the form of `@@sub`. For example, you can use RSA substitution macro such as `@@URL?GetPic?image` to place images in the `useridandpasscode.htm` page. With HTML, the images must be JPEGs. Substitution macros cannot have absolute paths. The images must be in the same directory as the templates, and you must omit the filename extension from the file specification as in the following example:

```
<IMG src="@@URL?GetPic?image=logo" ALIGN="left">
```

Refer to the *RSA ACE/Agent 5.0 for Windows Installation and Administration Guide* for additional information regarding macros.

Below is the code excerpted from the `useridandpasscode.htm` file. Please note that this is sample code and may need to be customized for your environment.

```
<html>
<head>
<title>MetaFrame Application Portal</title>
<style type="text/css">
<!--
.loginEntries { font-family: Verdana, Arial, Helvetica, sans-serif; font-size: 8pt; color: #000000; width: 200px}
A.appLinks
{  FONT-SIZE: 8pt;
  FONT-WEIGHT: bold;
  TEXT-DECORATION: none
  COLOR: #000000
  FONT-FAMILY: Verdana, Arial, Helvetica, sans-serif;}
A.appLinks:hover
{  COLOR: #CCCCCC }
-->
</style>
</head>
<body bgcolor="#C0C0C0" LANGUAGE=javascript onload="return loginForm.username.focus()">
<div align="center">
<table width="100%" height="100%" border="0" cellspacing="0" cellpadding="0">
<tr align="center" valign="middle">
<td>
<table border="1" cellspacing="0" cellpadding="20" bordercolor="#000000" bgcolor="#FFFFFF">
<tr>
<td>
<table border="0" cellspacing="0" cellpadding="10">
<tr>
<td bgcolor="#C0C0C0">
</td>
<td rowspan="2" valign="top">
<table border="0" cellpadding="0" cellspacing="0" bordercolor="#111111">
<tr>
<td>
<table border="0" cellpadding="5" cellspacing="5" bordercolor="#111111">
<tr>
```

```

<td width="100%" bgcolor="#6699CC">
<font face="Verdana, Arial, Helvetica, sans-serif" size="3" color="#FFFFFF">
<b>MetaFrame Application Portal</b></font></td>
</tr>
<tr>
<td>
<font face="Verdana, Arial, Helvetica, sans-serif" size="4">
<b><font size="3">Please log in </font></b></font>
<ul>
<li>
<font face="Verdana, Arial, Helvetica, sans-serif" size="2">
<p>To log in to the application portal, type your user
name, Domain password, and SecurID PASSCODE in the boxes at
left.</p>
</li>
<li>
<p>Click the Log In button to log in.</p>
</li>
</ul>
<p>If you do not know your login information, please
contact your help desk or system administrator.</p></td>
</tr>
<tr><td>&nbsp;</td></tr>
<tr>
<td bgcolor="#6699CC">&nbsp;</td>
</tr>
<tr>
<td align="right">
<P align=left><FONT color=red><b>@@MSG</b></FONT></P>
</td>
</tr>
</table>
</td>
</tr>
</table>
</td>
</tr>
<tr>
<td bgcolor="#C0C0C0">
<table border="1" cellpadding="0" cellspacing="0" bordercolor="#111111">
<tr>
<td>
<table border="0" cellpadding="0" cellspacing="5" bordercolor="#111111" bgcolor="#6699CC">
<tr>
<td colspan="2" background="@@URL?GetPic?image=greygrad" bgcolor="#CCCCCC">

</tr>
<tr>
<td>
<table border="0" cellpadding="0" cellspacing="5" bordercolor="#111111">
<form name="loginForm">

```



```

                <td colspan="2">&nbsp;  </td>
                <td>
                    <input type="password" name="passcode" class="loginEntries" MAXLENGTH="254" size="20"
onkeypress="CheckKey()"/></td>
                </tr>
                <tr>
                <td colspan="3">
                    <p align="right">
                        <input type="button" value="Login" name="login" onclick="DoNFuseLogin()" language="JavaScript">&nbsp;  <input
TYPE="RESET" VALUE="Reset"/></td>
                    </tr>
                </form>
            </table>
        </td>
    </tr>
</table>
</td>
</tr>
</table>
</td>
</tr>
</table>
</td>
</tr>
</table>
</td>
</tr>
</table>
</td>
</tr>
</table>
</td>
</tr>
</table>
</div>
<span style="visibility:hidden">
<p>@@MSG</p>
<form name="securIDForm" method="POST" action="@@URL">
<p></p>
<center>
<table>
<tr>
<td><b>Username:</b></td>
<td>
<input TYPE="TEXT" NAME="username" VALUE="%s" MAXLENGTH="32" size="20"></td>
</tr>
<tr>
<td><b>PASSCODE:</b></td>
<td><input TYPE="PASSWORD" NAME="passcode" VALUE MAXLENGTH="32" size="20"></td>
</tr>
</table>
</center><hr><center>
<p><input TYPE="submit" VALUE="Send"> <input TYPE="RESET" VALUE="Reset"/></p>
</center><input TYPE="HIDDEN" NAME="referrer" VALUE="@@REFERRER">
<input TYPE="HIDDEN" NAME="stage" VALUE="useridandpasscode">
<input TYPE="HIDDEN" NAME="sessionid" VALUE="@@SESSIONID">
</form>
</span>

```

```

<script language="JavaScript">
<!--
var securForm = document.forms.securIDForm;
var nfuseForm = document.forms.loginForm;

function DoNFuseLogin()
{
    securForm.username.value = nfuseForm.username.value;
    securForm.passcode.value = nfuseForm.passcode.value;

    SetCookie("NFuseData_NFuse_User", nfuseForm.username.value, null, "");
    SetCookie("NFuseData_NFuse_Domain", nfuseForm.domain.value, null, "");
    SetCookie("NFuseData_NFuse_Password", nfuseForm.domainPassword.value, null, "");

    securForm.submit();
}

function focus_UPD(loginForm) {
    if (loginForm.LoginType && loginForm.LoginType[1]) {
        loginForm.LoginType[1].checked = true;
    }
}

function SetCookie(name, value, expires, path, domain, secure)
{
    document.cookie = name + "=" + escape (value) +
        ((expires) ? "; expires=" + expires.toGMTString() : "") +
        ((path) ? "; path=" + path : "") +
        ((domain) ? "; domain=" + domain : "") +
        ((secure) ? "; secure" : "");
}

function CheckKey()
{
    if (window.event.keyCode == 13)
    {
        DoNFuseLogin();
    }
}
//-->
</script>
</body>
</html>

```

Login.asp

The login.asp file of NFuse needs to be modified to support the functionality added by the integration of the RSA SecurID login. Below are three sections of source code that need to be added. Please note that this is a sample code and may need to be customized for your environment. This section of code obtains and reads the values inside the cookie.

```

function getCookieVal(offset) {
    var endstr = document.cookie.indexOf(";", offset);
    if (endstr == -1)

```

```

    endstr = document.cookie.length;
    return unescape(document.cookie.substring(offset, endstr));
}

function GetCookie(name) {
    var arg = name + "=";
    var alen = arg.length;
    var clen = document.cookie.length;
    var i = 0;
    while (i < clen) {
        var j = i + alen;
        if (document.cookie.substring(i, j) == arg)
            return getCookieVal (j);
        i = document.cookie.indexOf(" ", i) + 1;
        if (i == 0) break;
    }
    return null;
}

function SetCookie(name,value,expires,path,domain,secure) {
    document.cookie = name + "=" + escape (value) +
        ((expires) ? "; expires=" + expires.toGMTString() : "") +
        ((path) ? "; path=" + path : "") +
        ((domain) ? "; domain=" + domain : "") +
        ((secure) ? "; secure" : "");
}

```

1. This code section determines, upon loading of the NFuse Web page by the browser, if a populated cookie exists. If a populated cookie exists, then the login.asp file reads the values in that cookie and automatically attempts to log into NFuse. If a populated cookie does not exist, then the automatic login into NFuse does not occur, and the user is prompted to enter values for username, domain, and domain password.

```

function window_onload() {
    var user = GetCookie("NFuseData_NFuse_User");
    var domain = GetCookie("NFuseData_NFuse_Domain");
    var domainPassword = GetCookie("NFuseData_NFuse_Password");

    SetCookie("NFuseData_NFuse_User", "", null, "/");
    SetCookie("NFuseData_NFuse_Domain", "", null, "/");
    SetCookie("NFuseData_NFuse_Password", "", null, "/");

    if (user && user.length > 0)
    {
        document.forms.NFuseForm.user.value = user;
        if (domain && document.forms.NFuseForm.domain)
        {
            document.forms.NFuseForm.domain.value = domain;
        }
        document.forms.NFuseForm.password.value = domainPassword;
        NFuseForm.submit();
    }
}

```

2. This section of code is how the function mentioned above is called.

```
<body bgcolor="#CCCCCC" LINK="#000000" VLINK="#000000" ALINK="#000000" LANGUAGE=javascript onload="return window_onload()">
```



6400 NW 6th Way

Fort Lauderdale, FL 33309

954-267-3000



<http://www.citrix.com>

Copyright © 2000 Citrix Systems, Inc. All rights reserved. Citrix, WinFrame and ICA are registered trademarks, and MultiWin and MetaFrame are trademarks of Citrix Systems, Inc. All other products and services are trademarks or service marks of their respective companies. Technical specifications and availability are subject to change without prior notice.