



Integrating RSA SecurID with Citrix NFuse Elite 1.0

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 © 2002 Citrix Systems, Inc., 851 West Cypress Creek Road, Ft. Lauderdale, Florida 33309-2009 U.S.A. All rights reserved.

Version History		
Sept 26, 2002	Citrix Consulting Services	Version 1.0

Table of Contents

TABLE OF CONTENTS	III
INTRODUCTION.....	1
DOCUMENT OVERVIEW	1
CITRIX NFUSE ELITE	1
RSA SECURID	1
ARCHITECTURE.....	2
CITRIX NFUSE ELITE	2
AUTHENTICATION IN NFUSE ELITE	2
CITRIX NFUSE ELITE WITH RSA SECURID	3
LOGIN PROCESS	4
RSA SECURID NOT INTEGRATED WITH NFUSE ELITE	4
RSA SECURID INTEGRATED WITH NFUSE ELITE.....	5
APPLICATION INSTALLATION AND INTEGRATION	7
REQUIRED COMPONENTS	7
CONFIGURATIONS	7
<i>NFuse Elite</i>	7
<i>RSA SecurID</i>	7
CODE MODIFICATIONS.....	9
<i>Useridandpasscode.htm</i>	9
<i>Silentlogin.htm</i>	12
SUMMARY	15
CONSIDERATIONS AND RECOMMENDATIONS.....	15
<i>Internal versus External Access</i>	15
<i>Network Security</i>	15
<i>Portal Access via a Published Browser</i>	15
RSA CONTACT INFORMATION	15
ADDITIONAL INFORMATION	15

Introduction

Document Overview

An important concern when implementing a Citrix NFuse® Elite Portal is making the portal and associated resources available to authorized users through an intranet, a wide area network (WAN), or even the Internet. Using two-factor authentication, RSA SecurID provides additional login security to prevent unwelcome access to the portal. However, RSA SecurID also has the potential to increase the number of logins required to access the NFuse Elite Portal, thus diminishing the overall user satisfaction level.

This document outlines an integrated solution to provide two-factor authentication and to reduce the number of required logins to access an NFuse Elite Portal while retaining the advanced security features of RSA SecurID. The following topics are presented, and code samples are provided where appropriate:

- Solution Components
- Architecture
- Login Process
- Installation and Integration

It is assumed that the reader has basic knowledge of Citrix NFuse Elite and RSA SecurID. Moreover, it is assumed that the reader is familiar with the content of the *Citrix NFuse Elite Guide to NFuse Elite*, the *Citrix NFuse Elite Quick Start Guide*, the *RSA Ace Server 5.0 for Windows NT and Windows 2000 Installation Guide*, and the *RSA ACE Agent 5.0 for Windows Installation and Administration Guide*.

Citrix NFuse Elite

Citrix NFuse Elite is part of Citrix's access product line that enables secure delivery of content and applications through an intranet, a WAN, or even the Internet.

On the user side, NFuse Elite provides a simple and convenient solution that gives users access to aggregated applications and content as well as easy, point-and-click browser-based access along with role-based presentation of applications and content to increase user productivity. Additionally, NFuse Elite delivers the access that the mobile workforce needs to access applications and content from any remote or distributed location.

On the business side, Citrix NFuse Elite provides streamlined installation and configuration, centralized administration, and security for information and applications. Also, fast deployment capabilities and ease of management help companies achieve a rapid return on investment.

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 are combined with a 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 personal computers (PCs), personal digital assistants (PDAs), and wireless phones), and smart cards. The RSA ACE Server is the network authentication engine that controls an organization's security policy regarding who accesses which resources. For more information about RSA SecurID, visit the RSA web site.

Architecture

Citrix NFuse Elite

The Citrix NFuse Elite Portal Server Farm contains several components: State Server, Database Server, Agent Server(s), and Web Server(s). While the term, server farm, implies multiple servers, a single server can be used to host each of these components for prototyping and testing. Additionally, multiple load-balanced Agent Servers and Web Servers can be utilized to scale the NFuse Elite Portal solution.

The following diagram displays the high-level architecture of a Citrix NFuse Elite Portal solution:

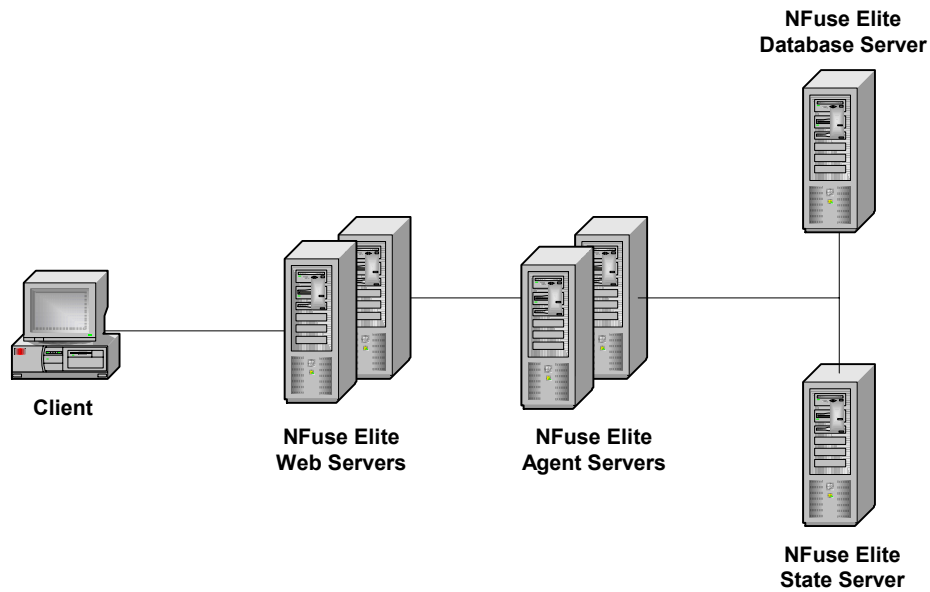


Figure 1. NFuse Elite Architecture.

For information regarding platform requirements, refer to the *NFuse Elite Installation Requirements* section of the *Citrix NFuse Elite Guide to NFuse Elite*. In addition, for scalability and performance consideration, refer to *Capacity Sizing and Performance Issues* section of the *Citrix NFuse Elite Guide to NFuse Elite*.

Authentication in NFuse Elite

Authentication to an NFuse Elite portal is done via a standard HTML form produced by the login CDA. When a user submits the login form, the `host.dll` (an ISAPI DLL residing on the web server) receives the request, encrypts the user's password, creates an XML message, and sends the message to an available Agent Server. The Agent Server processes the login request message by passing user credentials to the Security Broker for validation. The Security Broker is a DLL that communicates with the Windows operating system to determine whether the credentials are valid. If the credentials provided are valid, NFuse Elite will log on the user and draw the user's default page. If the credentials provided are invalid, NFuse Elite redraws the login page with an error message.

Citrix NFuse Elite with RSA SecurID

The RSA Web Access Authentication architecture is the RSA authentication method used for the NFuse Elite and RSA SecurID integration. The RSA SecurID infrastructure used to secure an NFuse Elite Portal is composed of two components: RSA ACE Server and RSA ACE Agent(s). The RSA ACE Agent is installed on each of the NFuse Elite Web Servers and secures the web site by intercepting requests to protected resources. The RSA ACE Server provides the engine to service authentication requests and manage user security credentials.

The following diagram displays the high-level architecture of the NFuse Elite and RSA SecurID integrated solution:

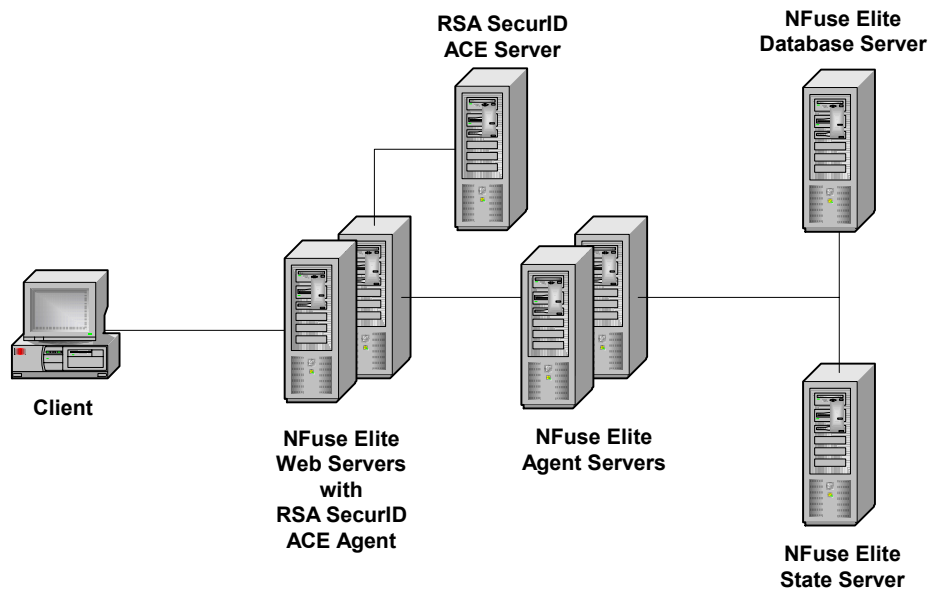


Figure 2. NFuse Elite and RSA SecurID Integrated Architecture.

For information regarding platform requirements, refer to the RSA ACE Server 5.0 for Windows NT and Windows 2000 Installation Guide and the RSA ACE Agent for Windows Installation and Administration Guide.

Login Process

RSA SecurID Not Integrated with NFuse Elite

With a standard configuration, the RSA ACE client adds an initial RSA login page that is presented when attempting to access the NFuse Elite Portal.

RSA SecurID User Name and PASSCODE Request

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

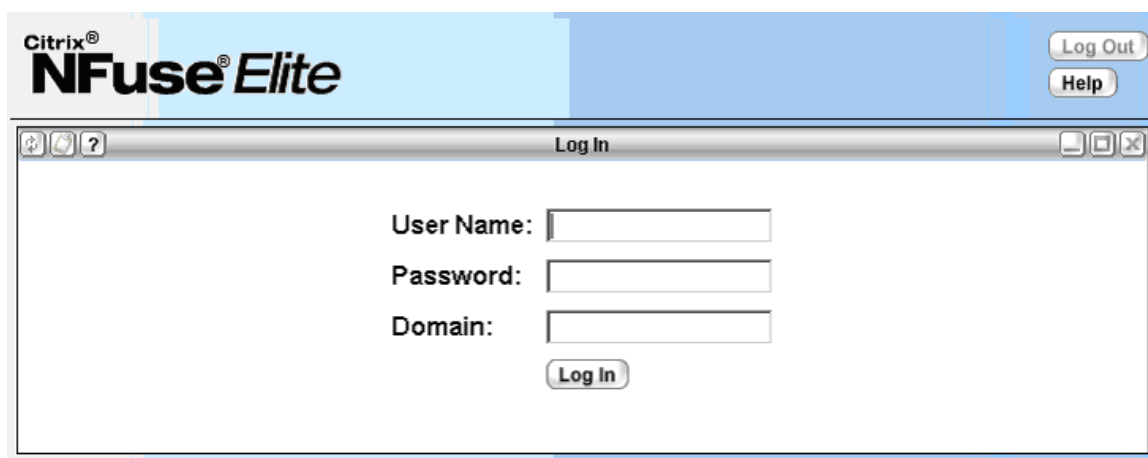
Enter your User Name and SecurID PASSCODE in the following fields, and then click "Send." If you make a mistake, use "Reset" to clear the fields.

Username:

PASSCODE:

Figure 3. RSA SecurID Login Page.

This RSA SecurID login page is displayed *before* the NFuse Elite Portal login page. It is here that the user keys in the unique passcode generated from the SecurID token device.



Citrix®
NFuse® Elite

Log Out
Help

Log In

User Name:

Password:

Domain:

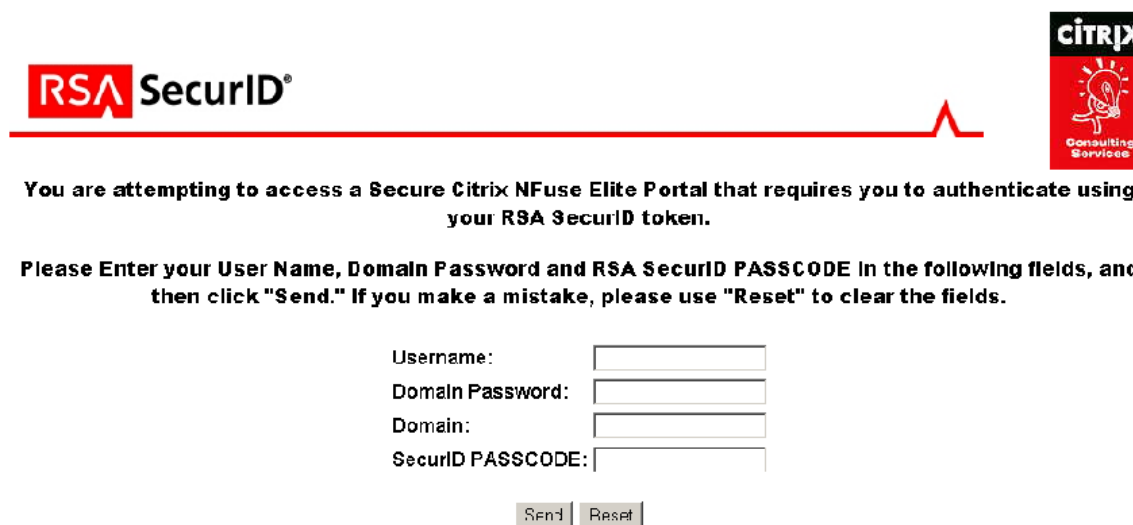
Log In

Figure 4. NFuse Elite Login Page.

Once the RSA SecurID authentication has occurred, the NFuse Elite login page will be displayed. From the end-user perspective, it appears to be a double login, since the user must enter security credentials a second time. This double login is undesirable because it diminishes the overall user experience. The double login problem, however, can be resolved by creating a custom login page that will ask for all required information for both RSA and NFuse Elite authentication.

RSA SecurID Integrated with NFuse Elite

In order to have a single login page, the NFuse Elite credential fields need to be incorporated into the RSA login page. Because some of the fields, for example username, 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.



RSA SecurID®

You are attempting to access a Secure Citrix NFuse Elite Portal that requires you to authenticate using your RSA SecurID token.

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

Username:

Domain Password:

Domain:

SecurID PASSCODE:

Figure 5. Integrated Login Page.

The RSA login page process is very specific, requiring that only the username and the SecurID passcode should be submitted for login processing. The rest of the fields have to be saved for future use in the NFuse Elite login processing that occurs after a successful RSA login. One of the ways to achieve this is to use the RSA login page to save entered NFuse credentials in a temporary cookie on the client. After the RSA login processing occurs, a second web page, the Silent Login web page, can be invoked. The Silent Login web page reads the saved credentials from the cookie and passes the credentials into the NFuse Elite Login Content Delivery Agent (CDA). At the same time the cookie with the login credentials is destroyed.

During a successful login attempt, the cookie exists for a matter of seconds. 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 but prior to the NFuse Elite login attempt, and the cookie is not destroyed by Silent Login web page, the cookie will be automatically destroyed when the web 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 Elite from the perspective of the user:

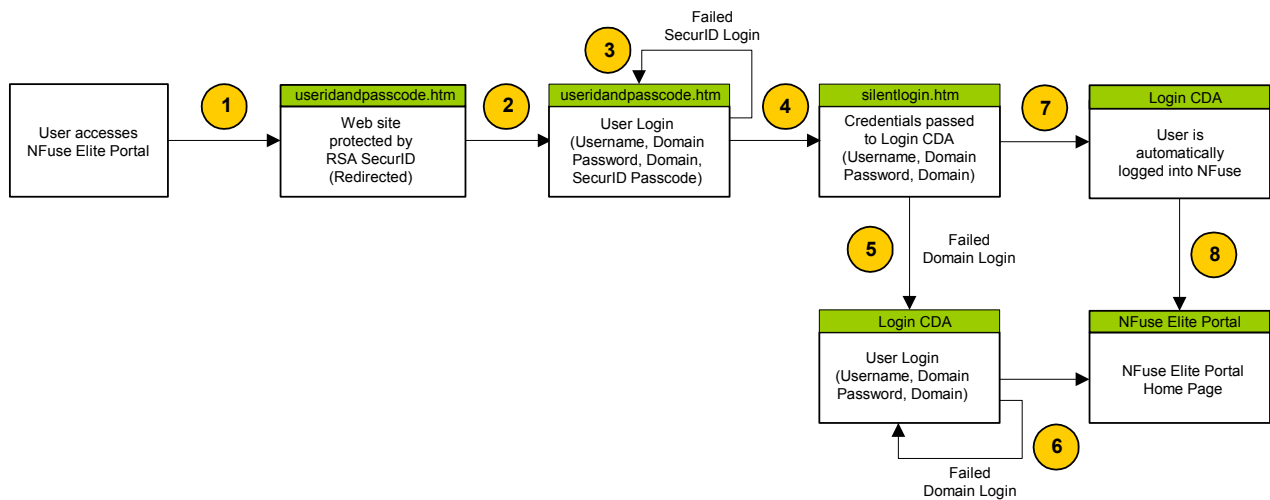


Figure 6. Integrated Login Process Flow.

The following steps outline the login process flow:

1. End user visits the NFuse Elite Portal. RSA SecurID protects the NFuse Elite Portal web site. As a result, the request is intercepted and the end user is redirected to a customized integrated login web page.
2. The end user is prompted to enter their username, domain password, domain, and SecurID passcode.
3. If the user enters an incorrect username or SecurID passcode, the user fails the SecurID login and is returned to the integrated login page.
4. If the user successfully authenticates to SecurID, the user is redirected to the customized silent login web page. The silent login page automatically passes the security credentials into the NFuse Elite Login CDA.
5. If the user's domain credentials, domain or domain password, are incorrect, the user fails the NFuse Elite login. As a result, the user is redirected to just the NFuse Elite login page. This is the standard NFuse Elite Login CDA web page.
6. If the end user once again fails to authenticate to NFuse Elite, the user is returned to the NFuse Elite login page.
7. If the end user enters all credentials correctly, the user is automatically logged into the NFuse Web site.
8. The user is directed to the NFuse Elite Portal home page.

Application Installation and Integration

Required Components

The following components are required when integrating Citrix NFuse Elite and RSA SecurID:

- Citrix NFuse Elite
- RSA SecurID
 - ACE Agent 5.0
 - ACE Agent 4.1

It is also assumed that the RSA Secure ACE Server infrastructure is in place. For specific requirements and installation instructions of each component, refer to the appropriate component's administrator guide and supplemental documentation.

Configurations

NFuse Elite

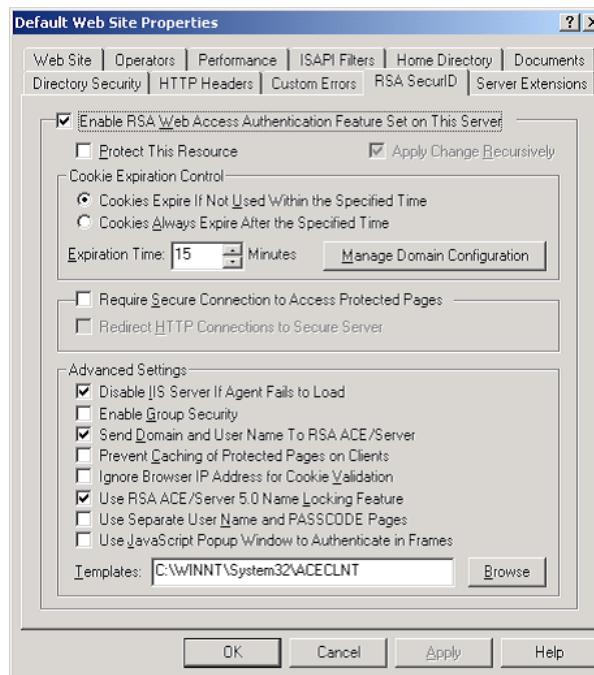
The NFuse Elite portal configurations are not modified in this example. While some solutions for integrating RSA SecurID and NFuse Elite can require modifications to the NFuse Elite Portal, specifically the Login CDA, this solution was chosen because it does not require any special NFuse Elite configurations.

The given solution modifies components on the web servers only. The implementation of the NFuse Elite and RSA SecurID integration would not affect users connecting via another unaltered web server. This can be useful when implementing different access points for both internal and external users.

RSA SecurID

The RSA ACE Agent protects the NFuse Elite Portal web site. The software intercepts access requests and requires designated users or groups — whether local or remote — to authenticate to the RSA ACE/Server software with an RSA SecurID authenticator prior to gaining access to protected resources. The following RSA Agent configuration settings need to be made for the portal web site maintained on the NFuse Elite web server:

1. Within the **Internet Services Manager**, open the properties page of the Default Web Site.
2. Select the RSA SecurID tab.



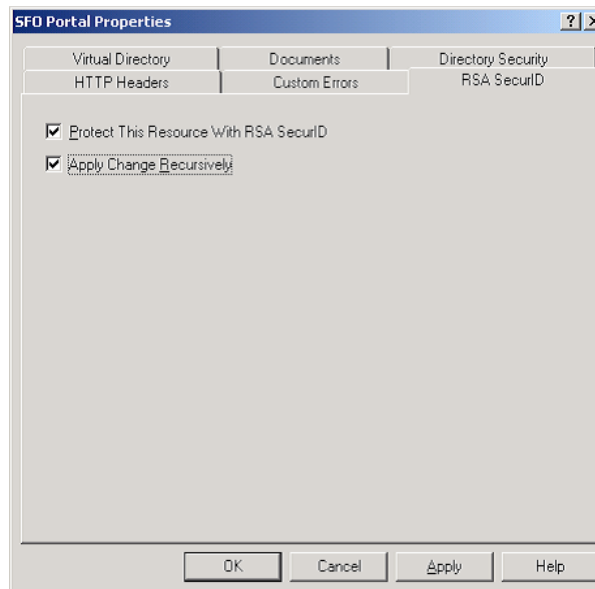
3. Select the Enable RSA Web Access Authentication Feature Set on This Server checkbox.

Note: These instructions assume that the only resource on the web server to be protected using RSA SecurID will be the NFuse Elite Portal virtual directory. The contents of the entire Default Web Site can be protected by enabling the **Protect This Resource** and **Apply Change Recursively** checkboxes. For information on other configuration options, please refer to the *RSA ACE Agent 5.0 for Windows Installation and Administration Guide*.

4. Do not select the Protect This Resource checkbox.
5. Ensure that the Use Separate User Name and PASSCODE Pages checkbox is *not* selected.
6. Click **Apply**.

Note: The remaining steps are not necessary when protecting the contents of the entire Default Web Site.

7. Within the **Internet Services Manager**, open the properties page of the NFuse Elite Portal virtual directory.
8. Select the **RSA SecurID** tab.



9. Check the Protect This Resource With RSA SecurID and the Apply Change Recursively checkboxes. Click OK.

Code Modifications

In order to implement the RSA SecurID and NFuse Elite Portal integrated login, the `useridandpasscode.htm` file, located in the `%systemroot%\system32\aceInt` directory by default, used by RSA SecurID requires customizations. Additionally, the `silentlogin.htm` file should be added to the root of the NFuse Elite Portal virtual directory.

Useridandpasscode.htm

The `useridandpasscode.htm` page is the web page that the user is redirected to when they visit the NFuse Elite Portal. This page has been modified to prompt the user to enter their username, domain password, domain, and RSA SecurID passcode. Additionally, the page has been modified to automatically redirect to the `silentlogin.htm` page after completing the SecurID authentication process.

Clicking the Send button after the security credentials have been entered initiates the login process. Once the login process has been invoked, the RSA SecurID authentication is first initiated, while the username, domain password, and domain values entered by the user are written to a temporary cookie for later use by the `silentlogin.htm` page for the NFuse Elite login process.

Built into RSA HTML files are substitution macro in the form of `@@sub`. For example, you can use RSA substitution macros, such as `@@URL?GetPic?image`, to place images in the `useridandpasscode.htm` page. With HTML, the images must be JPEGs. Also, 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>NFuse Elite - RSA SecurID Login</TITLE>
    <META http-equiv=Content-Type content="text/html; charset=iso-8859-1">
    <META content="MSHTML 6.00.2715.400" name=GENERATOR>
  </HEAD>
  <BODY>
    <TABLE border="0" width="100%">
      <TR>
        <TD width="100%">
          <TABLE border="0" width="100%">
            <TR>
              <TD width="50%"><IMG src="@URL?GetPic?image=securid_banner" ALIGN="left"></TD>
              <TD width="50%"><IMG src="@URL?GetPic?image=citrix" ALIGN="right"></TD>
            </TR>
            <TR>
              <TD width="100%" colspan="2">
                <P align="center"><font face="Arial Black">You are attempting to access a Secure Citrix NFuse Elite Portal that requires you to authenticate using your RSA SecurID token.</font></P>
                <P align="center"><font face="Arial Black">Please Enter your User Name, Domain Password and RSA SecurID PASSCODE in the following fields, and then click &quot;Send.&quot; If you make a mistake, please use &quot;Reset&quot; to clear the fields.</font></P>
              </TD>
            </TR>
          </TABLE>
        </TD>
      </TR>
    </TABLE>
    <FORM NAME="Form2">
      <CENTER>
        <TABLE>
          <TR>
            <TD><B><font face="Arial">Username:</font></B></TD>
            <TD><INPUT TYPE=TEXT NAME="username" VALUE="" MAXLENGTH=32></TD>
          </TR>
          <TR>
            <TD><B><font face="Arial">Domain Password:</font></B></TD>
            <TD><INPUT TYPE=PASSWORD NAME="password" VALUE="" MAXLENGTH=32></TD>
          </TR>
          <TR>
            <TD><B><font face="Arial">Domain:</font></B></TD>
            <TD><INPUT TYPE=TEXT NAME="domain" VALUE="sfo-w2k" MAXLENGTH=32></TD>
          </TR>
          <TR>
            <TD><B><font face="Arial">SecurID PASSCODE:</font></B></TD>
            <TD><INPUT TYPE=PASSWORD NAME="passcode" VALUE="" MAXLENGTH=16></TD>
          </TR>
        </TABLE>
        <P>
          <INPUT TYPE="BUTTON" NAME="SendButton" VALUE="Send" OnClick="processSend2()"
LANGUAGE="JavaScript" >
```

```

<INPUT TYPE=RESET VALUE="Reset">
</P>
</CENTER>
</FORM>

<SPAN style="visibility:hidden">
<P>
<FORM method="POST" NAME="Form1" action="@@URL">
</P>
<TABLE>
  <TR>
    <TD><B>Username:</B></TD>
    <TD><INPUT TYPE=TEXT NAME="username" VALUE="@@USER" MAXLENGTH=32></TD>
  </TR>
  <TR>
    <TD><B>PASSCODE:</B></TD>
    <TD><INPUT TYPE=PASSWORD NAME="passcode" VALUE="" MAXLENGTH=16></TD>
  </TR>
</TABLE>
<P>
<INPUT TYPE="BUTTON" NAME="SendButton" VALUE="Send" OnClick="processSend()"
LANGUAGE="JavaScript" >
  <INPUT TYPE=RESET VALUE="Reset">
</P>

<INPUT TYPE=HIDDEN NAME="stage" VALUE="useridandpasscode">
<!-- <INPUT TYPE="BUTTON" NAME="SendButton" VALUE="Send" OnClick="processSend()"
LANGUAGE="JavaScript" > -->
<INPUT type=hidden value=../SFO%20Portal/SilentLogin.htm name=referrer>
<INPUT TYPE=HIDDEN NAME="sessionid" VALUE="@@SESSIONID">
</FORM>
</SPAN>

<SCRIPT language=JavaScript>
  <!--
  var myForm = document.Form1;
  var myForm2 = document.Form2;

  function processSend() {
    myForm.submit();
  }

  function processSend2() {

    myForm.username.value = myForm2.username.value;
    myForm.passcode.value = myForm2.passcode.value;

    SetCookie("NFESILENTUSER",myForm2.username.value, null, "/");
    SetCookie("NFESILENTPASSWORD",myForm2.password.value, null, "/");
    SetCookie("NFESILENTDOMAIN","sfo-w2k", null, "/");

    myForm.submit();
  }
  -->

```

```

    }

    // Make ENTER work like submit
    function CheckKey()
    {
        if (window.event.keyCode == 13){
            processSend2();
        }
    }

    // Make ENTER work like submit
    function lemmein(keypressed) {
        var key;
        if (document.all)
            key = window.event.keyCode;
        else
            key=keypressed.which;
        if (key==13) myForm.submit();
    }

    //if (navigator.appName == "Netscape")
    //    myForm.passcode.onkeypress = CheckKey();

    var popup_auth = null;
    // when the popup closes attempt to reload this page
    function check_popup() {
        if (popup_auth && popup_auth.open && !popup_auth.closed)
            setTimeout("check_popup()", 500);
        else
            self.document.location.reload(true);
    }

    //Set Cookie
    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" : "");
    }

    //-->
</SCRIPT>
</BODY>
</HTML>

```

Silentlogin.htm

The silentlogin.htm is the web page that the useridandpasscode.htm redirects the user to after the SecurID authentication has been successfully completed. The web page contains no visible components and serves only to retrieve the security credentials from the cookie, destroy the cookie, and automatically forward the login request to the NFuse Elite Login CDA.

The silentlogin.htm file is intended to reside in the root of the NFuse Elite Portal virtual directory. This location is referenced within the useridandpasscode.htm file. It is possible to place the file in another location or include the functionality of the file within another file, for instance the index.htm file that exists by default at the root of the NFuse Elite Portal virtual directory.

```

<HTML>
  <HEAD>
    <TITLE>NFuse Elite - RSA SecurID Redirect</TITLE>
  </HEAD>
  <BODY language="JavaScript">
    <SCRIPT language="JavaScript">

      var strNFEUN = GetCookie('NFESILENTUSER');
      var strNFEPW = GetCookie('NFESILENTPASSWORD');
      var strNFEDM = GetCookie('NFESILENTDOMAIN');
      var strNFEDMUN = strNFEDM + "\\\" + strNFEUN;

      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 getCookieVal (offset) {
        var endstr = document.cookie.indexOf (";", offset);
        if (endstr == -1)
          endstr = document.cookie.length;
        return unescape(document.cookie.substring(offset, endstr));
      }

    </SCRIPT>

    <FORM id="Silent_Login_form" name="Silent_Login_form" method="post" action="http://sfo-cpq-03/sfo%20portal/cds/host.xps?page=login&category=&rqid=&cmd=login&amp;cdainstanceid=cda34d6fd2ea9c04e3580399d7ad5245f0b&amp;encryptFields=Citrix_CDS_Login_Password_Field">
      <SCRIPT language="JavaScript">
        document.write("<input type='hidden' id='Citrix_CDS_Login_Password_Field' name='Citrix_CDS_Login_Password_Field' value=" + strNFEPW + ">" )
        document.write("<input type='hidden' id='Citrix_CDS_Login_User_Name_Field' name='Citrix_CDS_Login_User_Name_Field' value=" + strNFEDMUN + ">" )
      </SCRIPT>

    </FORM>

    <SCRIPT language="JavaScript">

```

```
function DelCookie(name,path,domain) {
    document.cookie = name + "=" +
        ((path) ? "; path=" + path : "") +
        ((domain) ? "; domain=" + domain : "") +
        "; expires=Thu, 01-Jan-00 00:00:01 GMT";
}

DelCookie('NFESILENTUSER', "/");
DelCookie('NFESILENTDOMAIN', "/");
DelCookie('NFESILENTPASSWORD', "/");
Silent_Login_form.submit();

</SCRIPT>
</BODY>
</HTML>
```

Summary

Considerations and Recommendations

Internal versus External Access

When deploying NFuse Elite considerations should be made for internal users versus external users. Typically, a scenario that involves both internal and external users accessing the same NFuse Elite Portal would have multiple web servers.

In this scenario, internal users would access an internal web server while external users access a web server located in the Demilitarized Zone (DMZ). This architecture also works when the situation calls for some users to use two-factor authentication, external users for example, while others only require domain authentication, such as internal users. Since the NFuse Elite Portal can only maintain a single virtual directory on a single web server, a single NFuse Elite Web Server is not able to provide both RSA SecurID protected content and unprotected content. Therefore, in order to provide a solution that allows both types of access, unsecured and RSA SecurID secured, two NFuse Elite Web Servers should be utilized.

Network Security

RSA SecurID secures your network by requiring users to identify themselves with two unique factors —something they know and something they have — before they are granted access. Each RSA SecurID authenticator has a unique symmetric key that is combined with an algorithm to generate a new code every 60 seconds. Because the number is unpredictable and dynamic, it would be extremely difficult for a hacker to guess the correct number at any given time. When logging on, the user simply enters this number plus a secret PIN to be successfully authenticated.

In order to provide additional security when allowing access to web content, such as an NFuse Elite Portal, it is advisable to secure the HTTP traffic using Secure HTTP (HTTPS). The RSA SecurID Web Access Authentication architecture used for the NFuse Elite – RSA SecurID Integration provides the ability to protect both HTTP and HTTPS requests. Providing additional network security is especially important when allowing access over public networks, such as the Internet.

Portal Access via a Published Browser

An alternative method of accessing an NFuse Elite portal is through use of a browser, published from a MetaFrame server. In this case, access can be secured by integrating RSA SecurID with Citrix Secure Gateway and NFuse Classic or integrating RSA with a VPN and using the Program Neighborhood client to access the published browser.

In both of these instances, the published browser will typically be accessing an internal web server to access the portal. Since the NFuse Elite web server is internal, it is not necessary to protect the NFuse Elite web server with RSA SecurID.

RSA Contact Information

For more information about RSA and RSA SecurID visit their website at <http://www.rsasecurity.com/>.

Additional Information

For additional information about integrating Citrix NFuse with RSA SecurID see the white paper “Integrating RSA SecurID with Citrix NFuse 1.6 and Project Columbia 6.00.030” available from the Citrix Knowledge Base (<http://knowledgebase.citrix.com/>).



**851 West Cypress
Creek Road**

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.