SafeNet Authentication Service

Integration Guide

Using SafeNet Authentication Service with Citrix XenApp 6.5

Document Information

Document Part Number	007-012649-001, Rev. A
Release Date	March 2014

Trademarks

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Introduction

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Citrix® XenApp.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

About SafeNet Authentication Service

SafeNet Authentication Service (SAS) delivers a fully automated, versatile, and strong authentication-as-a-service solution. With no infrastructure required, SafeNet Authentication Service provides smooth management processes and highly flexible security policies, token support, and integration APIs.

Citrix XenApp 6.5 is a secure application and data access solution that gives IT administrators a single point to manage access control and to limit actions within sessions based on both user identity and the endpoint device. New threats, risks, and vulnerabilities, as well as evolving business requirements, underscore to the need for a strong authentication approach based on multi-factor authentication.

This document provides guidance for deploying a multi-factor authentication option in Citrix XenApp 6.5, using a number of authentication methods managed by SafeNet Authentication Service.

This document describes how to configure Citrix XenApp 6.5 to work with SafeNet Authentication Service. It also describes the various authentication methods (Grid, MobilePASS, SMS OOB) and how to configure each to work with XenApp and SAS.

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—SafeNet's cloud-based authentication service.
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**—A server version of SAS that is used by service providers to deploy instances of SafeNet Authentication Service.
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—A server version of SAS that is used to deploy the solution on-premises in an organization.

Audience

This document is targeted to system administrators who are familiar with Citrix XenApp 6.5 and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

Prerequsites

This document assumes that Citrix XenApp 6.5 is deployed in the organization. It will guide you through the process of adding multi-factor authentication capabilities to Citrix XenApp 6.5 using SafeNet Authentication Service.

While there are a number of methods through which Citrix XenApp 6.5 can be configured to support multi-factor authentication, for the purpose of working with SafeNet Authentication Service, the RADIUS protocol will be used.

The deployment of multi-factor authentication support using SafeNet Authentication Service with Citrix XenApp 6.5 requires completion of the following steps:

- Configure RADIUS communication between the Citrix Web Interface and SafeNet Authentication Service (applies to all SafeNet Authentication Service versions, including SAS, SAS-SPE, and SAS-PCE).
- Synchronize the Citrix Web Interface with the SAS User Store.
- Assign authenticators to users.
- Test the authentication solutions.

NOTE: This document assumes that the XenApp 6.5 environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

RADIUS-based Authentication Using SAS

SafeNet Authentication Service (SAS) communicates with a large number of VPN and access-gateway solutions using the RADIUS protocol.

Figure 1 illustrates the data flow of a multi-factor authentication transaction for Citrix XenApp 6.5.

1 - The user attempts to log in to the Citrix published resource via the Citrix Web Interface.

2 - Citrix Web Interface sends a RADIUS request with the user's credentials to SAS.

3 - 4 - SAS validates the credentials.

5 - The SAS reply (approving or declining access) is sent back to the Citrix Web Interface.

6 - The user is granted or denied access to the Citrix XenApp 6.5 server published application.

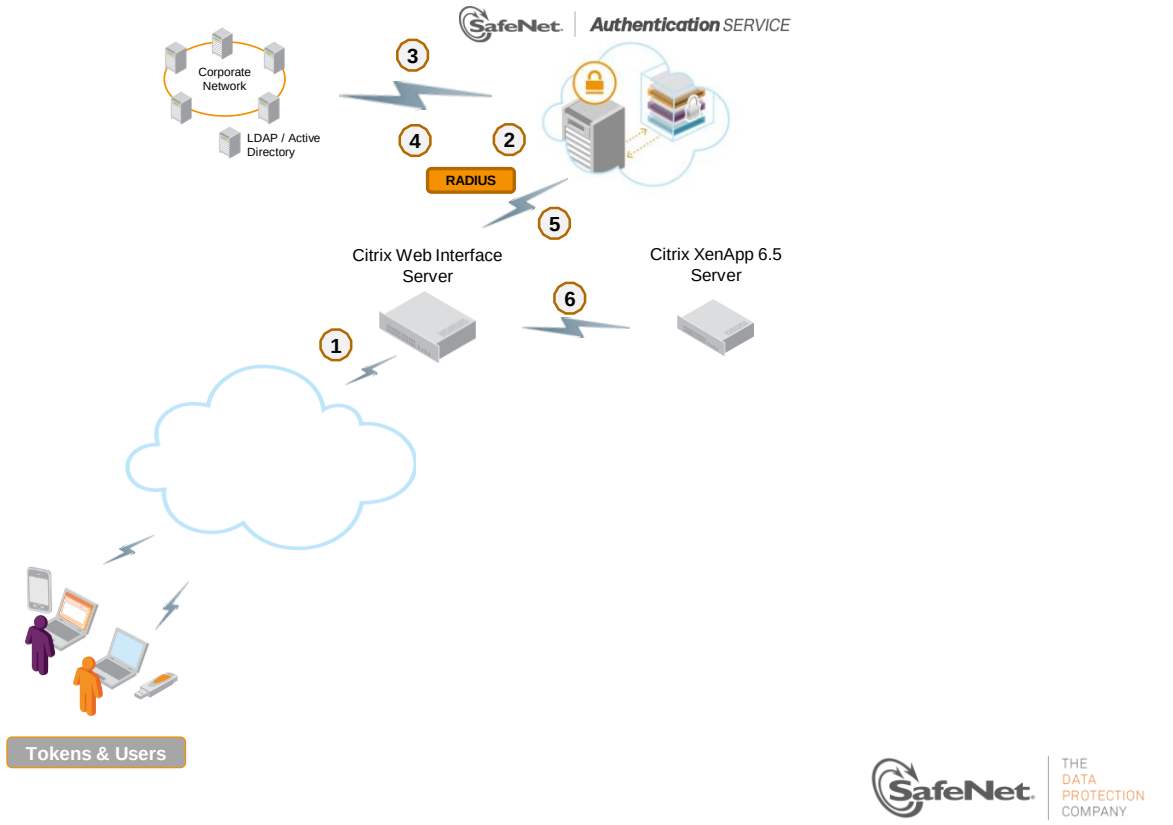


Figure 1: Data flow of RADIUS-based authentication

RADIUS-based Authentication Using SAS-SPE and SAS-PCE

In addition to the pure cloud-based offering, SafeNet Authentication Service comes with two on-premises versions:

- **SafeNet Authentication Service – Service Provider Edition (SPE)**—An on-premises version of SAS targeted at service providers interested in hosting SAS in their data center.
- **SafeNet Authentication Service – Private Cloud Edition (PCE)**—An on-premises version of SAS targeted at organizations interested in hosting SAS in their private cloud environment.

For both on-premises versions, SafeNet Authentication Service can be integrated with Microsoft Network Policy Server (MS-NPS) or with the legacy Microsoft Internet Authentication Service (MS-IAS). Both solutions serve as local RADIUS servers. SAS is integrated with the local RADIUS servers using a special on-premises agent called SafeNet Agent for NPS.

For more information on how to install and configure SafeNet Agent for NPS, refer to the following SafeNet link:

http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-Agents-IASNPS.pdf

Data Flow of RADIUS-based Authentication in an On-Premises Solution

The following steps describe the data flow of RADIUS-based authentication in an on-premises solution:

1. The user attempts to log in to the Citrix Web Interface with the user's credentials, including the second-factor authentication credentials.
2. The Citrix Web Interface sends a RADIUS request that is transferred using Microsoft NPS and SafeNet NPS Agent.
3. The RADIUS request with the user's credentials is sent to SAS for validation.
4. The SAS response (approving or declining access) is sent back to Microsoft NPS.
5. The response is forwarded to the Citrix Web Interface, which redirects the user to the published XenApp application, to which the user is granted or denied access.

Setting RADIUS Connection between Citrix Web Interface and SAS

To enable SafeNet Authentication Service (in a cloud-based deployment) to receive RADIUS requests from the Citrix Web Interface, the following prerequisite steps are required:

- Ensure that end users can authenticate through the Citrix Web Interface to the XenApp server environment with a static password before configuring the Citrix Web Interface to use RADIUS authentication.
- Ensure ports 1812/1813 are open to the Citrix Web Interface.
- Add a RADIUS entry in the SAS **Auth Nodes** module to prepare it to receive RADIUS authentication requests from the Citrix Web Interface. You will need the IP address of Citrix Web Interface and the shared secret that will be used by both SAS and the Citrix Web Interface.
- Create a valid user account in SAS with a token to be used when testing RADIUS authentication.

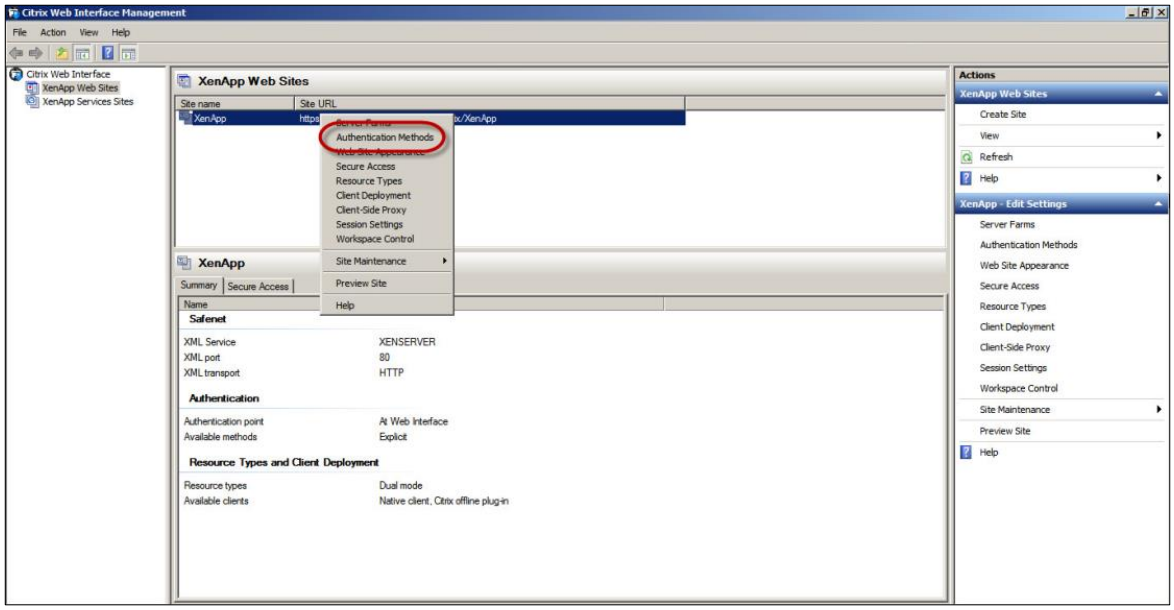
Setting RADIUS Connection between Citrix NetScaler Access Gateway and SAS-PCE

To enable SafeNet Authentication Service-Private Cloud Edition (SAS-PCE) to receive RADIUS requests from the Citrix Web Interface, do the following:

1. Ensure that users can authenticate through the Citrix Web Interface with a static password before configuring the Citrix Web Interface to use RADIUS authentication.
2. Install Microsoft's Network Policy Server (NPS) on-premises. NPS allows organizations to create and enforce network access policies for authentication and authorization.
3. Ensure ports 1812/1813 are open from NPS to the Citrix Web Interface.
4. Add a RADIUS client entry in NPS to prepare it to receive RADIUS authentication requests from the Citrix Web Interface. You will need the IP address of the Citrix Web Interface and the shared secret that will be used by both NPS and the Citrix Web Interface.
5. Install the SafeNet Agent for NPS and configure it to forward authentication requests to SAS-PCE.

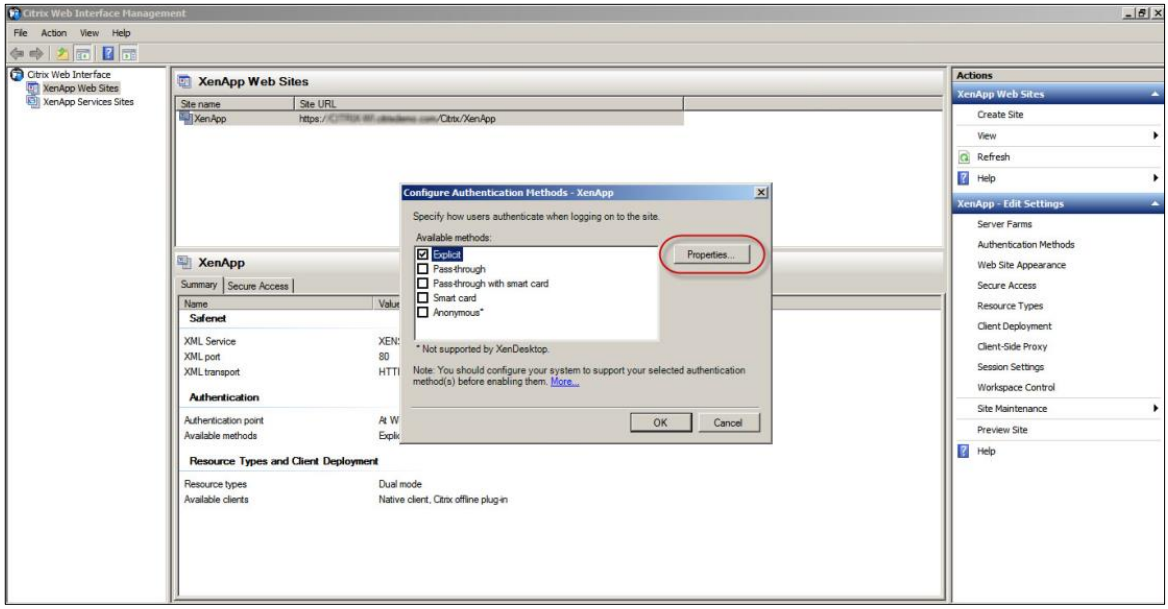
Configuring RADIUS Authentication in Citrix Web Interface

1. Open the Citrix Web Interface Management console.
2. In the **XenApp Web Sites** section (as shown below), right-click on the **XenApp** website and select **Authentication Methods**.



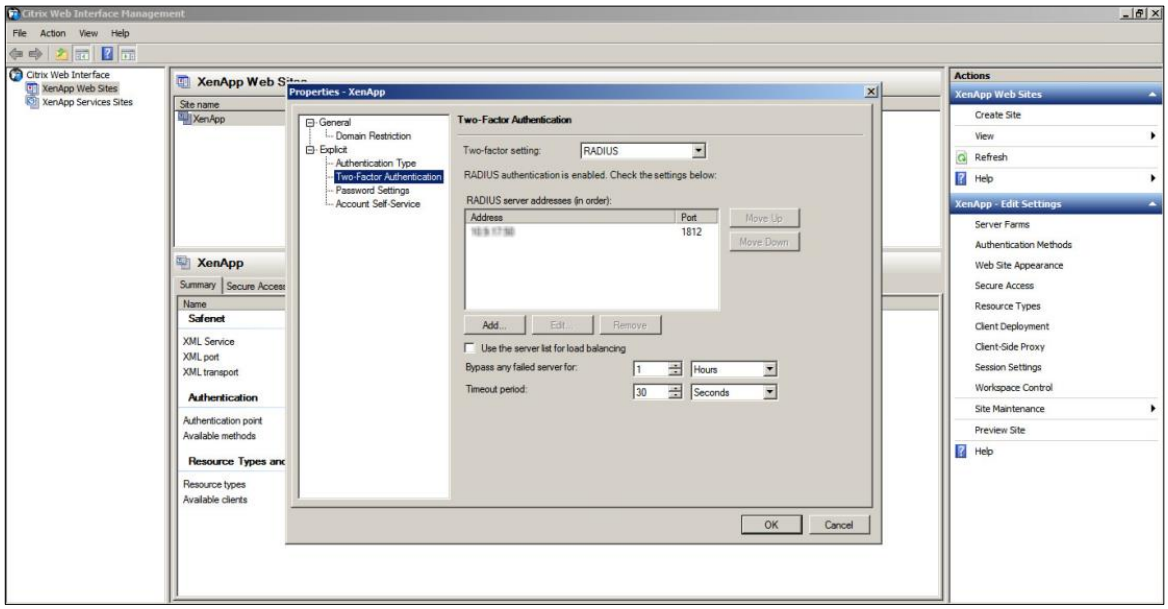
(The screen image above is from Citrix® Systems, Inc. software. Trademarks are the property of their respective owners.)

3. On the **Configure Authentication Methods – XenApp** window, select **Explicit**, and then click **Properties**.



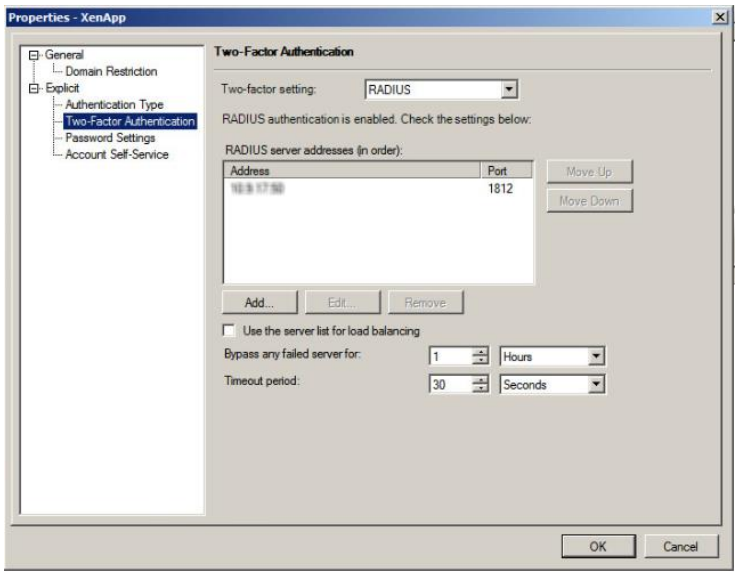
(The screen image above is from Citrix® Systems, Inc. software. Trademarks are the property of their respective owners.)

4. On the **Properties - XenApp** window, in the left pane, select **Explicit > Two-Factor Authentication**.



(The screen image above is from Citrix® Systems, Inc. software. Trademarks are the property of their respective owners.)

5. In the **Two-factor setting** field, select **RADIUS**.
6. Under **RADIUS server addresses**, click the **Add** button.



7. On the **Add RADIUS Server** window, complete the following fields:

Server address	Type the address of the RADIUS server.
Server port	Type the port number of the RADIUS server.

Click **OK**.

8. Next, you must configure the RADIUS shared secret. A shared secret file must be manually created for the RADIUS server defined under the **Two-Factor Authentication** method.
   a. On the Citrix Web Interface server, browse to the **\inetpub\wwwroot\Citrix\sitepath\conf** directory.
      - Create a file called **radius_secret.txt** that contains the RADIUS shared secret.
   b. Browse to the directory **\inetpub\wwwroot\Citrix\sitepath\conf**.
   c. Use a text editor to open the file **web.config** and do the following:
      - Search for **RADIUS_NAS_IDENTIFIER** and, for the value, enter **citrixwi**.
      - Search for **RADIUS_NAS_IP_ADDRESS** and, for the value, enter the IP address assigned to the Citrix Web Interface server.
      - Save and close the file.

Synchronizing User Stores

Before SafeNet Authentication Service (SAS) can authenticate any user in your organization, you must create a SAS User Store that reflects the users who need to use multi-factor authentication. User records can be created in the SAS User Store via a number of methods. It is important to use the method that fits the configuration used with Citrix NetScaler Access Gateway. The following table lists Citrix NetScaler Access Gateway authentication methods and the recommended SafeNet Authentication Service methods.

Citrix NetScaler Access Gateway Authentication Method	SAS User Store Method
Local Users Currently using Access Gateway's internal User Store.	**Manual** Create users in a SAS User Store manually, either one user at a time or by importing user records via a flat file.
LDAP An external user directory is being used.	**Automated** Users are updated automatically by synchronizing the Active Directory/LDAP server using the SAS LDAP Synchronization Agent.
RADIUS A legacy multi-factor authentication solution was deployed.	**Automated** Contact SafeNet support to inquire about SAS migration guides.

For additional information on importing users to SAS, refer to the *SafeNet Authentication Service Subscriber Account Operator Guide*, which can be found at the following link:

http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-SPE-SubscriberAccountOperatorGuide.pdf

All SafeNet Authentication Service documentation can be found in the Knowledge Base on the SafeNet website. See "Support Contacts" on page 16.

Assigning Authenticators to Users

SafeNet Authentication Service supports a number of authentication methods that can be used as second-factor authentication for users who are authenticating through Citrix NetScaler Access Gateway.

The following authentication methods are supported:

- SafeNet RB, KT Series
- SafeNet eToken, Silver, Gold, Platinum, Alpine
- Third-party OATH Tokens
- MobilePASS
- OOB
- GrID tokens

Refer to the *SafeNet Authentication Service Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in a SAS User Store. This document can be found at the following link:

http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-SPE-SubscriberAccountOperatorGuide.pdf

Configuring SMS OOB Authentication

SafeNet Authentication Service supports OOB authentication through an SMS token. In order to use this method, SAS must be configured for SMS OOB authentication.

1. In the SAS Administrator Console, provision an SMS token for an existing user.
2. In the Citrix Web Interface, go to the **Web Interface** directory (for example, **C:\inetpub\wwwroot\Citrix**).
3. In the **Web Interface** directory, go to the **app_data\include** folder.
4. Create a backup copy of the file **LoginMainForm.inc**.
5. Edit the original **LoginMainForm.inc** file using a text editor, such as Notepad. Note that this code exists twice in the file and must be changed in both instances. Make the following changes:
   a. Locate the section shown below:

```
<tr><td class='labelCell'>
    <label id='lblPasscode' for='<%=Constants.ID_PASSCODE%>'
      <%=viewControl.getExplicitDisabledStr()%> >
      <%=wiContext.getString("Passcode")%>
    </label>
</td>
<% if (Include.isCompactLayout(wiContext)) { %>
</tr><tr>
<% } %>
<td>
    <input type='password' name='<%=Constants.ID_PASSCODE%>' id='<%=Constants.ID_PASSCODE%>'
     class='loginEntries<%=viewControl.getExplicitDisabled()?" loginEntriesDisabled":""%>'
     maxlength='<%=Constants.LOGIN_ENTRY_MAX_LENGTH%>' <%=viewControl.getExplicitDisabledStr()%>>
</td>
</tr>
```

   b. Add the text highlighted in yellow:

```
<tr><td class='labelCell'>
    <label style='display:none' id='lblPasscode' for='<%=Constants.ID_PASSCODE%>'
      <%=viewControl.getExplicitDisabledStr()%> >
      <%=wiContext.getString("Passcode")%>
    </label>
</td>
<% if (Include.isCompactLayout(wiContext)) { %>
</tr><tr>
<% } %>
<td>
    <input style='display:none' type='text' value='1' name='<%=Constants.ID_PASSCODE%>' id='<%
=Constants.ID_PASSCODE%>'
     class='loginEntries<%=viewControl.getExplicitDisabled()?" loginEntriesDisabled":""%>'
     maxlength='<%=Constants.LOGIN_ENTRY_MAX_LENGTH%>' <%=viewControl.getExplicitDisabledStr()%>>
</td>
</tr>
```

c. Repeat the previous steps for the second instance of this code.

d. Save the file.

With these changes, a value of 1 is added to the **Passcode** field, and then the field is hidden from the **Log on** screen. When a user provides his/her AD credentials during login, the single character will be sent to SAS and will force an SMS challenge/response action. To log in to Citrix XenApp using SMS OOB authentication, refer to "Running the Solution – SMS OOB Authentication" on page 14.

Running the Solution

Running the Solution - MobilePASS Token

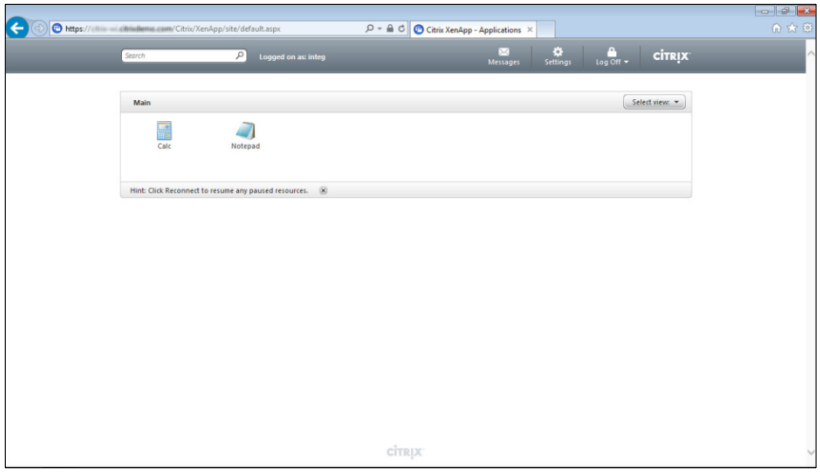
1. Log in to the Citrix Web Interface.

(The screen image above is from Citrix® Systems, Inc. software. Trademarks are the property of their respective owners.)

2. On the **Log on** window, complete the following fields:

User name	Enter your user name.
Password	Enter your password.
Domain	Enter the XenApp domain name to which you are connecting. This information can be obtained from the system administrator.
PASSCODE	Enter your SafeNet OTP passcode.

3. Click **Log On**. The **Citrix XenApp Main** window is displayed.



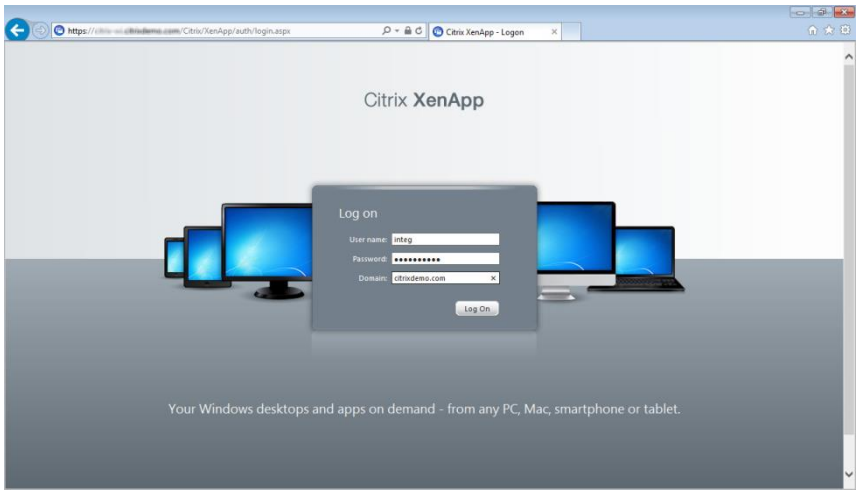
(The screen image above is from Citrix® Systems, Inc. software. Trademarks are the property of their respective owners.)

Running the Solution – SMS OOB Authentication

An SMS token has been provisioned for each existing LDAP user. An SMS token code will be required for this login method and will be sent to the mobile number specified in the SAS User Store for your SMS token.

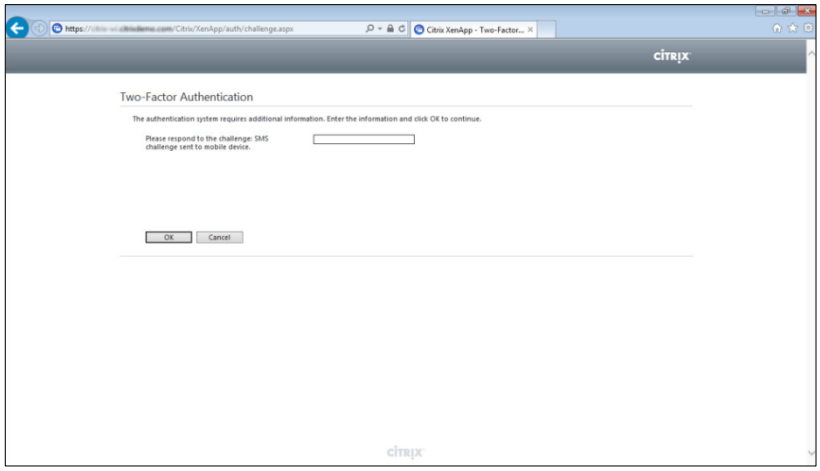
1. Open the Citrix XenApp Web Interface.
2. On the **Log on** window, complete the following fields:

User name	Enter your LDAP user name.
Password	Enter your LDAP password.
Domain	Enter the domain name to which you are connecting. This information can be obtained from the system administrator.



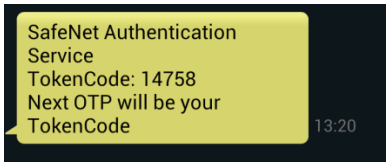
(The screen image above is from Citrix® Systems, Inc. software. Trademarks are the property of their respective owners.)

3. Click **Log On**. The **Two-Factor Authentication** window is displayed, informing you that additional authentication is required in the form of an SMS challenge code. This code will be sent to the mobile phone number specified in the SAS User Store for your SMS token.

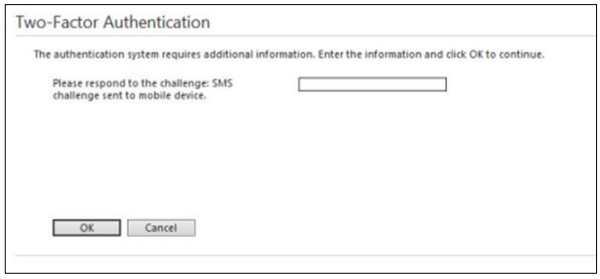


(The screen image above is from Citrix® Systems, Inc. software. Trademarks are the property of their respective owners.)

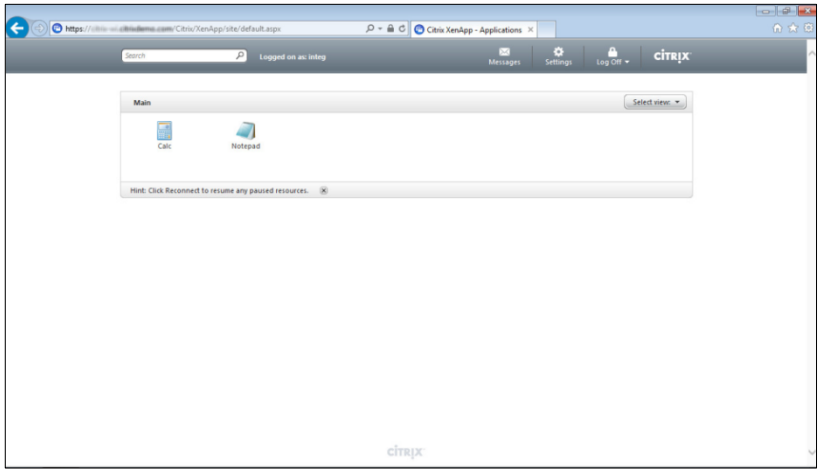
4. Retrieve the token code sent via text message to your mobile device, as shown in the example below.



5. On the **Two-Factor Authentication** window, enter your token code in the text box, and then click **OK**.



The **Citrix XenApp Main** window is displayed.



(The screen image above is from Citrix® Systems, Inc. software. Trademarks are the property of their respective owners.)

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Table 1: Support Contacts

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	