Entrust® Securing Digital Identities & Information

Securing Your Digital Life

# Technical Integration Guide for Entrust® IdentityGuard 9.3 and Microsoft Forefront Unified Access Gateway(UAG) 2010

Document issue: 1.0

January 2012

# Table of Contents

# Introduction

This technical integration guide describes how to integrate a Microsoft Forefront Unified Access Gateway and Entrust IdentityGuard 9.3. The aim of this integration is to provide strong, second-factor authentication to your Microsoft Forefront Unified Access Gateway solution using Entrust IdentityGuard 9.3.

This integration works with Entrust IdentityGuard passwords, grids, tokens, temporary PINs, out-of-band one-time passwords (OTPs), knowledge-based questions and answers and personal verification numbers. For more information on using Entrust IdentityGuard, see the *Entrust IdentityGuard Administration Guide*.

## Integration information

**Entrust product:** Entrust IdentityGuard 9.3

**Partner name:** Microsoft

**Partner product:** Forefront Unified Access Gateway

**Product version:** 2010 SP1

Check the Platform Support and Integration Center for the latest supported version information at:

https://www.entrust.com/support/psic/index.cfm

## Partner contact information

http://technet.microsoft.com/en-us/forefront/edgesecurity/bb758906.aspx#

http://www.microsoft.com/forefront/edgesecurity/iag/en/us/support-options.aspx

## Supported authentication methods

The Microsoft Forefront Unified Access Gateway software supports the Entrust IdentityGuard authentication methods and authentication protocols listed in Table 1. The capabilities may depend on the Entrust IdentityGuard configuration or setup of other third-party authentication resources, for example Active Directory.

**Note**: The Entrust IdentityGuard server supports additional authentication protocols and authentication methods. See the Entrust IdentityGuard documentation for more information if you are integrating different VPN devices.

**Table 1**: Authentication methods

| Authentication method | Notes | Supported protocols |
|---|---|---|
| Password | Password authentication is first-factor authentication with Entrust IdentityGuard's password feature. | PAP, MS-CHAPv2 |
| Radius | Radius authentication is first-factor authentication with a Radius server. | PAP, MS-CHAPv2 |
| External | External authentication is first-factor authentication with an LDAP-compliant directory or a Windows domain controller through Kerberos. | PAP, MS-CHAPv2 |
| Grid* | Two-step authentication only. | PAP, MS-CHAPv2 |
| Token* | Entrust IdentityGuard supports both response-only tokens and challenge/response tokens.<br>One-step or two-step authentication. | PAP, MS-CHAPv2 |
| Temporary PIN* | Grid or token authentication must be configured. | PAP, MS-CHAPv2 |
| Out-of-band one-time password* (OTP) | Two-step authentication only. | PAP, MS-CHAPv2 |
| Knowledge-based questions and answers | The Entrust IdentityGuard server only supports a single question and answer.<br>Two-step authentication only. | PAP, MS-CHAPv2 |
| Mutual | Serial number replay only.<br>Grid or token authentication must be configured. | PAP, MS-CHAPv2 |
| Risk Based Authentication | IPGeo only | PAP, MS-CHAPv2 |

* Can also include a personal verification number (PVN). A PVN is an additional authentication feature that can be added to other authentication methods. Grid, token, or out-of-band one-time password (OTP) authentication must be configured.

The Entrust IdentityGuard Radius proxy does not support the creation of new passwords or PVNs. Administrators must assign users their initial passwords and PVNs. Administrators can use the Entrust IdentityGuard Web interface to force users to change their PVNs. It is possible for VPN users to change their own PVNs. A new option called "Separate Challenge for PVN update" has been introduced since 9.1. See Using a PVN with your second-factor authentication response for more information.

**Note**: The Entrust IdentityGuard server supports additional authentication methods and features that are not supported in this integration due to limitations of the RADIUS protocol. The unsupported authentication methods and features include:

- Multiple question and answer pairs for knowledge-based authentication.
- Risk-based authentication based on machine authentication and IP address geo-location.
- Mutual authentication using user-selected images.

## VPN capabilities

The Microsoft Forefront Unified Access Gateway VPN allows for an easy integration of Entrust IdentityGuard authentication using the RADIUS protocol.

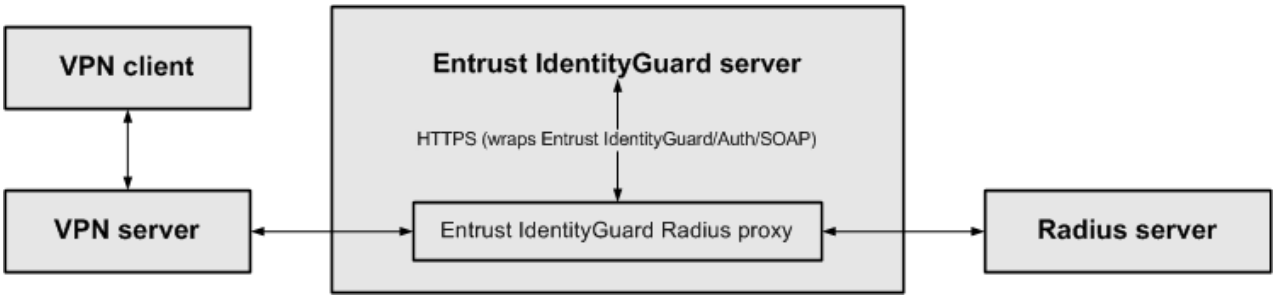
# Integration overview

When you install Entrust IdentityGuard, you also install the Entrust IdentityGuard Radius proxy. The Radius proxy allows your remote access gateway (IPsec or SSL) to communicate with Entrust IdentityGuard and (optionally) a Radius server or external first-factor authentication resource.

## Integration with Entrust IdentityGuard and a Radius server

When you install Entrust IdentityGuard, you can integrate it into an environment with a Radius server. In this environment, the Entrust IdentityGuard Radius proxy intercepts messages between the VPN server and the Radius server (see Figure 1).

**Figure 1:** Overview of Entrust IdentityGuard integrated with a VPN and Radius server




### VPN authentication with Entrust IdentityGuard and a first-factor authentication resource

The following steps outline the process of VPN authentication with Entrust IdentityGuard and a first-factor authentication resource.

A user enters first-factor credentials (user name and password) into the VPN client.

**1)** The VPN client sends the credentials to the VPN server, which forwards them to the Entrust IdentityGuard Radius proxy.

**2)** The Radius proxy forwards the credentials to the Radius server.

The Radius server generates either an accept message (the user passed first-factor authentication) or a reject message (the user failed first-factor authentication).

**3)** The Radius server sends the message to the Radius proxy.

If the message is a reject message, the Radius proxy sends the message unchanged to the VPN server.

**4)** If the message is an accept message, the Radius proxy requests a second-factor challenge from Entrust IdentityGuard.

**5)** Entrust IdentityGuard generates a second-factor challenge and sends it to the Radius proxy. The Radius proxy sends the challenge to the VPN server, which forwards it to the VPN client.

**6)** The user enters a response to the second-factor challenge into the VPN client.

**7)** The VPN client sends the response to the VPN server, which forwards it to the Radius proxy. The Radius proxy forwards the response to Entrust IdentityGuard for authentication.

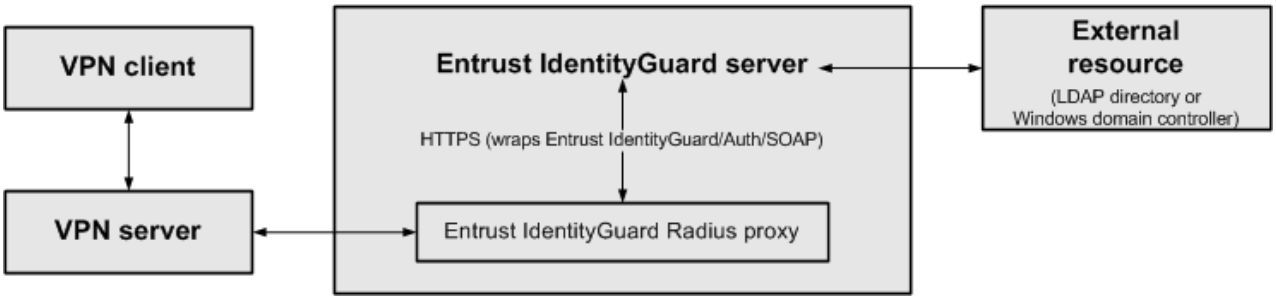
**8)** Entrust IdentityGuard either accepts or rejects the response and then sends a message to the Radius proxy. The Radius proxy forwards the message to the VPN server.

If the message is a reject message, then the user failed second-factor authentication. If the message is an accept message, then the user passed second-factor authentication.

# Integration with Entrust IdentityGuard and an external resource

When you install Entrust IdentityGuard, you can integrate it into an environment with an external first-factor authentication resource. That external resource can be an LDAP-compliant directory or a Windows domain controller through Kerberos. In this environment, the Entrust IdentityGuard Radius proxy intercepts messages from the VPN server, and the Entrust IdentityGuard server communicates with the external resource (see Figure 2).

**Figure 2:** Overview of Entrust IdentityGuard integrated with a VPN and first-factor authentication resource




## VPN authentication with Entrust IdentityGuard and a first-factor authentication resource

The following steps outline the process of VPN authentication with Entrust IdentityGuard and a first-factor authentication resource.

**1)** A user enters first-factor credentials (user name and password) into the VPN client.

**2)** The VPN client sends the credentials to the VPN server, which forwards them to the Entrust IdentityGuard Radius proxy.

**3)** The Radius proxy forwards the credentials to Entrust IdentityGuard, which forwards them to the external resource.

**4)** The external resource generates either a success message (the user passed first-factor authentication) or a fail message (the user failed first-factor authentication).

**5)** The external resource sends the message to Entrust IdentityGuard.

If the message is a fail message, the Radius proxy sends a reject message to the VPN server.

**6)** If the message is a success message, Entrust IdentityGuard generates a second-factor challenge and sends it to the Radius proxy.

**7)** The Radius proxy sends the challenge to the VPN server, which forwards it to the VPN client.

**8)** The user enters a response to the second-factor challenge into the VPN client.

**9)** The VPN client sends the response to the VPN server, which forwards it to the Radius proxy. The Radius proxy forwards the response to Entrust IdentityGuard for authentication.

**10)** Entrust IdentityGuard either accepts or rejects the response and then sends a message to the Radius proxy.

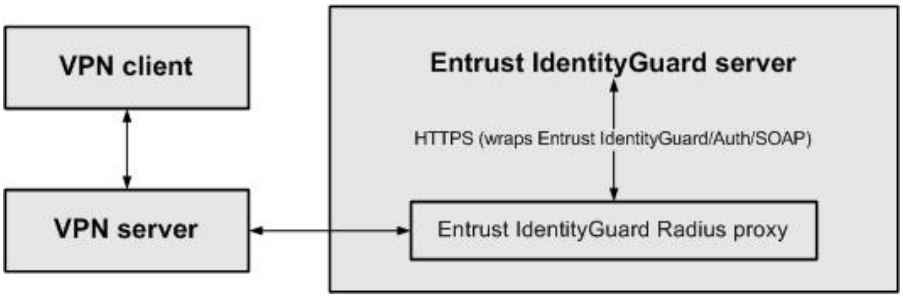
**11)** The Radius proxy forwards the message to the VPN server.

If the message is a reject message, then the user failed second-factor authentication. If the message is an accept message, then the user passed second-factor authentication.

# Integration with Entrust IdentityGuard only

When you install Entrust IdentityGuard, you can configure it to handle both first-factor authentication and second-factor authentication. In this environment, the Entrust IdentityGuard Radius proxy intercepts messages between the VPN server and Entrust IdentityGuard (see Figure 3).

**Figure 3** Overview of Entrust IdentityGuard integrated with a VPN




## VPN authentication with Entrust IdentityGuard

The following steps outline the process for VPN authentication with Entrust IdentityGuard.

**1)** A user enters first-factor credentials (user name and password) into the VPN client.

**2)** The VPN client sends the credentials to the VPN server, which forwards them to the Entrust IdentityGuard Radius proxy.

**3)** The Radius proxy forwards the credentials to Entrust IdentityGuard.

**4)** Entrust IdentityGuard generates either an accept message (the user passed first-factor authentication) or a reject message (the user failed first-factor authentication).

If the message is a reject message, the Radius proxy sends the message unchanged to the VPN server.

If the message is an accept message, Entrust IdentityGuard generates a second-factor challenge and sends it to the Radius proxy. The Radius proxy sends the challenge to the VPN server, which forwards it to the VPN client.

**5)** The user enters a response to the second-factor challenge into the VPN client.

**6)** The VPN client sends the response to the VPN server, which forwards it to the Radius proxy. The Radius proxy forwards the response to Entrust IdentityGuard for authentication.

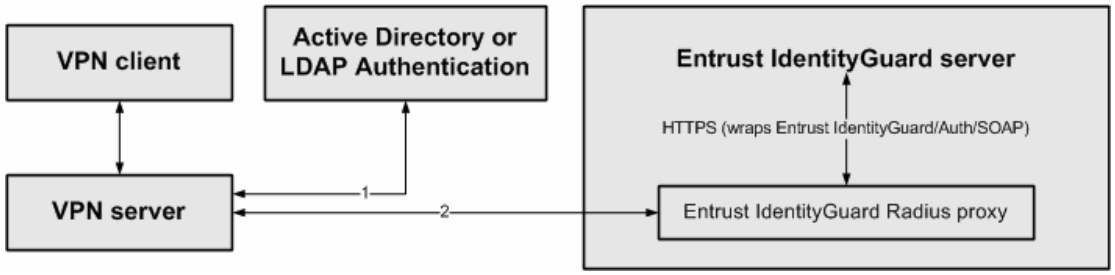
**7)** Entrust IdentityGuard either accepts or rejects the response and then sends a message to the Radius proxy. The Radius proxy forwards the message to the VPN server.

If the message is a reject message, then the user failed second-factor authentication. If the message is an accept message, then the user passed second-factor authentication.

# Integration with Active Directory or LDAP and Entrust IdentityGuard

The VPN device can be configured to chain authentication servers, so that the user has to authenticate to multiple servers. Microsoft Forefront UAG 2010 supports authentication chaining. Chaining an Active Directory authentication with Entrust IdentityGuard can be advantageous since the VPN can manage password expiry and notification of the Active Directory user account. This setup is only recommended when using one-step token with IdentityGuard (see Figure 4).

**Figure 4** Overview of Entrust IdentityGuard integrated with VPN and Active Directory




## VPN authentication with Entrust IdentityGuard and Active Directory

The following steps outline the process for VPN authentication with Entrust IdentityGuard and Active Directory.

**1)** A user enters their Active Directory user name and password into the Web browser along with the Entrust IdentityGuard token response. This is all on one login page.

**2)** The VPN server authenticates the Active Directory credentials against a defined Domain Controller.

If the user account is in need of a password change, the user is prompted to change their password.

**3)** The VPN server then sends the user name and token response to the Entrust IdentityGuard server to authenticate the token response.

**4)** Entrust IdentityGuard generates either an accept message (the user passed token authentication) or a reject message (the user failed token authentication).

# Migrating users to Entrust IdentityGuard

When integrating your VPN with Entrust IdentityGuard, your VPN users must also become Entrust IdentityGuard users to take advantage of Entrust IdentityGuard authentication. You can accomplish this migration in one of several ways:



Each migration scenario is discussed in more detail in the following sections.

## Forced migration

With forced migration, you have an existing VPN that provides access to a protected resource and you want to use the Entrust IdentityGuard Administration interface to migrate all users to Entrust IdentityGuard at a pre-announced switch-over date.

**Advantages**

- Easy to implement.
- Effective with a small number of users.

**Disadvantages**

- Administrators may experience a large number of problems on the switch-over date.
- No user feedback that a pilot would generate.
- Need an external process that maintains users between the existing system and the new Entrust IdentityGuard system.

### To perform a forced migration

**1)** Inform your VPN users that you plan to add second-factor authentication on a specified date.

**2)** Provide your users with their grid cards, tokens, or temporary PINs for Entrust IdentityGuard authentication.

**3)** On the switch-over date, have an Entrust IdentityGuard administrator use the bulk operations mechanism of Entrust IdentityGuard to load all your VPN users into the Entrust IdentityGuard repository. (See the *Entrust IdentityGuard Administration Guide* for information about bulk operations.)

**4)** Integrate your VPN and Entrust IdentityGuard.

## Phased migration with a parallel authentication resource

With phased migration you have an existing VPN that provides access to a protected resource, and you use another authentication resource to authenticate users with Entrust IdentityGuard. An authentication resource may be another VPN device, or it may be a parallel configuration on your current VPN. For example with an SSL VPN, Entrust IdentityGuard users might use another URL to login, or choose a different authentication realm or group to authenticate to. The exact form of the parallel authentication resource depends on your VPN. Create the alternate login mechanism on the VPN and migrate users to Entrust IdentityGuard in phases using the Administration

interface. Migrated users are forced to authenticate with Entrust IdentityGuard authentication. Users that have not yet migrated bypass Entrust IdentityGuard authentication.

**Advantages**

- Allows for a pilot and user feedback.
- Any users not yet migrated to the new system do not see any changes.

**Disadvantages**

- Need an external process that maintains users between the existing system and the new Entrust IdentityGuard system.
- May require another VPN
- Users can by bypass the second-factor login by using the old authentication mechanism

### To perform a phased migration with a parallel authentication resource

**1)** Integrate Entrust IdentityGuard with your existing VPN or a new dedicated VPN.

**2)** Have an Entrust IdentityGuard administrator use the bulk operations mechanism of Entrust IdentityGuard to load all your VPN users into the Entrust IdentityGuard repository. (See the *Entrust IdentityGuard Administration Guide* for information about bulk operations.)

**3)** Inform your users that they should now use second-factor authentication and provide them with their grid cards, tokens, or temporary PINs for Entrust IdentityGuard authentication.

**4)** Direct your users to the new authentication resource integrated with Entrust IdentityGuard.

**5)** After all your users have migrated, disable the old access method not integrated with Entrust IdentityGuard.

## Co-deployment or phased migration with a Radius server

If you have an existing VPN that provides access to a protected resource and an existing Radius server that provides authentication, you can choose to keep the Radius server for first-factor authentication, and add Entrust IdentityGuard for second-factor authentication. In this scenario, users are migrated to Entrust IdentityGuard in phases, with non-migrated users authenticating against the Radius server only, and migrated users authenticating against the Radius server and Entrust IdentityGuard.

Another option is to displace the Radius server altogether after all users have migrated to Entrust IdentityGuard. In this scenario, non-migrated users continue to authenticate to the Radius server only, while migrated users authenticate against Entrust IdentityGuard but not the Radius server. After all users are migrated, you can decommission your Radius server.

**Advantages**

- Any users not yet migrated to the new system are not inconvenienced.
- Any users migrated to the new system cannot bypass it and use the old system.
- Gradually adding users to the new system means administrators experience fewer problems.
- Starting with a small group of users allows for a pilot that generates user feedback.

**Disadvantages**

- Need an external process that maintains users between the existing system and the new Entrust IdentityGuard system.
- Requires a Radius server

- Need to inform users in a staged manner.

### To perform a phased migration or co-deployment with a Radius server

See the *Entrust IdentityGuard 9.3 Co-deployment with RSA ACE/Server or a Radius Server* for instructions.

## Phased migration with an external resource

With phased migration with an external resource, you have an existing VPN that provides access to a protected resource and an external resource (an LDAP-compliant directory or Windows domain controller through Kerberos) that provides first-factor authentication. You use the Entrust IdentityGuard Administration interface to migrate users to Entrust IdentityGuard in phases. Migrated users are forced to authenticate with Entrust IdentityGuard authentication. Non-migrated users bypass Entrust IdentityGuard authentication.

**Advantages**

- Any users not yet migrated to the new system are not inconvenienced.
- Any users migrated to the new system cannot bypass it and use the old system.
- Gradually adding users to the new system means administrators experience fewer problems.
- Starting with a small group of users allows for a pilot that generates user feedback.

**Disadvantages**

- Need an external process that maintains users between the existing system and the new Entrust IdentityGuard system.
- Need to inform users in a staged manner.

### To perform a phased migration with an external resource

**1)** Have an Entrust IdentityGuard Administrator use the bulk operations mechanism of Entrust IdentityGuard to load all your VPN users into the Entrust IdentityGuard repository. See the *Entrust IdentityGuard Administration Guide* for information on bulk operations.

**2)** Integrate your VPN and Entrust IdentityGuard. When setting Entrust IdentityGuard properties for your VPN, set the **Skip Second-Factor Authentication for Users Unable to Respond** property to **True**. For more information about this property, see the *Entrust IdentityGuard Administration Guide*.

**3)** Provide a portion of users with grid cards, tokens, or temporary PINs for Entrust IdentityGuard authentication.

**4)** After these users have successfully migrated, provide another portion of users with grid cards, tokens, or temporary PINs.

**5)** Continue this process until all users have migrated.

# Prerequisites

Complete the following steps before integrating your authentication system with Entrust IdentityGuard:

- Install and configure your first-factor authentication resource, using the documentation provided by the vendor. The first-factor authentication resource can be a Radius server or an external authentication resource (either an LDAP-compliant directory or Windows domain controller through Kerberos).
- Install and configure the Microsoft Forefront Unified Access Gateway using the documentation provided by Microsoft. The device must be able to route traffic before integrating it with Entrust IdentityGuard.
- Install and configure Entrust IdentityGuard and the Entrust IdentityGuard Radius proxy with the latest patches (see the *Entrust IdentityGuard Installation Guide*). Take note of the shared secrets, IP addresses, and ports you use. You need this information to configure the Microsoft Forefront Unified Access Gateway and first-factor authentication resource.
- If you want to configure your Microsoft Forefront Unified Access Gateway and first-factor authentication resource to recognize Entrust IdentityGuard user groups, you must define the Entrust IdentityGuard user groups first (see the *Entrust IdentityGuard Administration Guide*).

# Integrating the Microsoft Forefront Unified Access Gateway with Entrust IdentityGuard

This section contains the following topics:



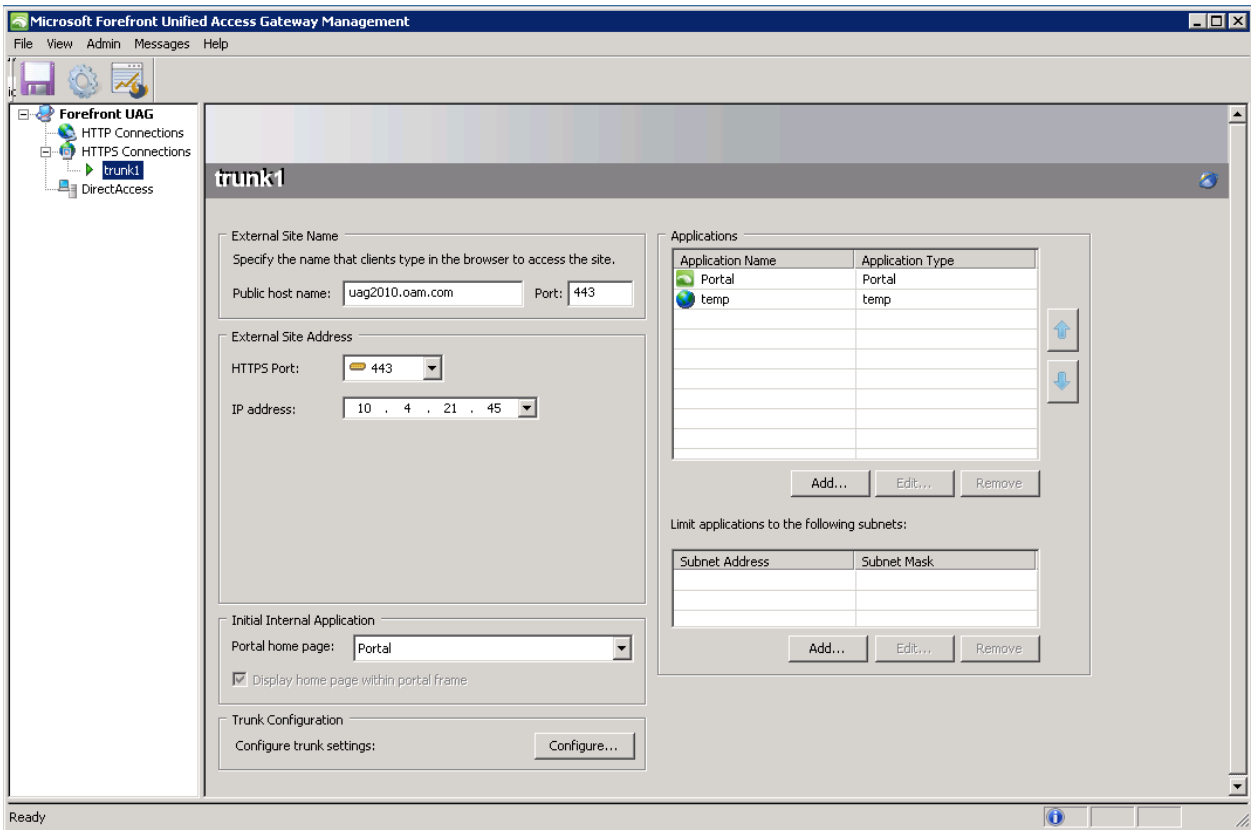
## Configuring the Microsoft Forefront Unified Access Gateway VPN

The following procedures describe how to configure the Microsoft Forefront Unified Access Gateway to use the Entrust IdentityGuard server. It is assumed that you are familiar with the Microsoft Forefront Unified Access Gateway administration interface.

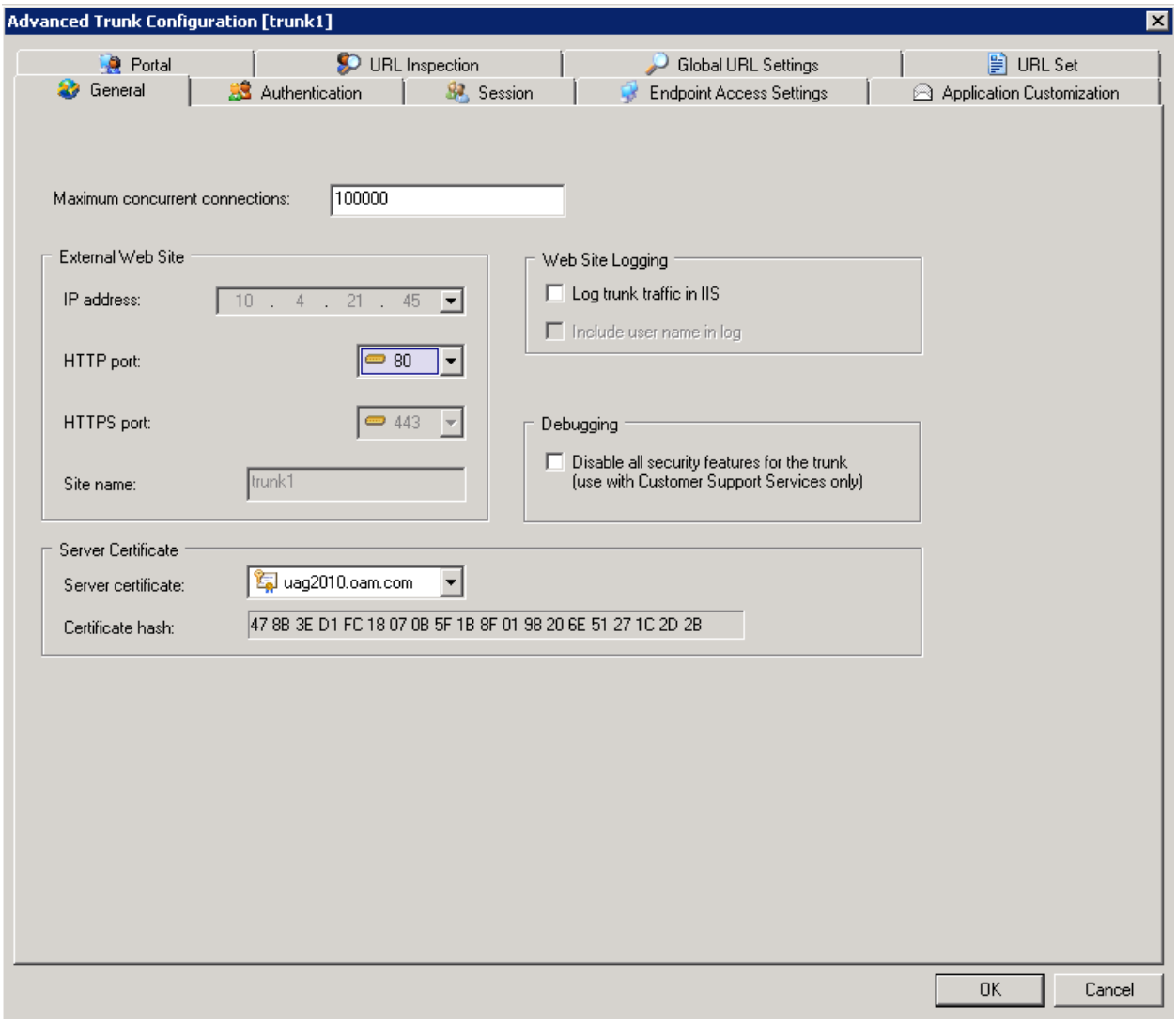
### To configure the Microsoft Forefront Unified Access Gateway VPN

**1)** Log in to the Forefront Unified Access Gateway Configuration Console.

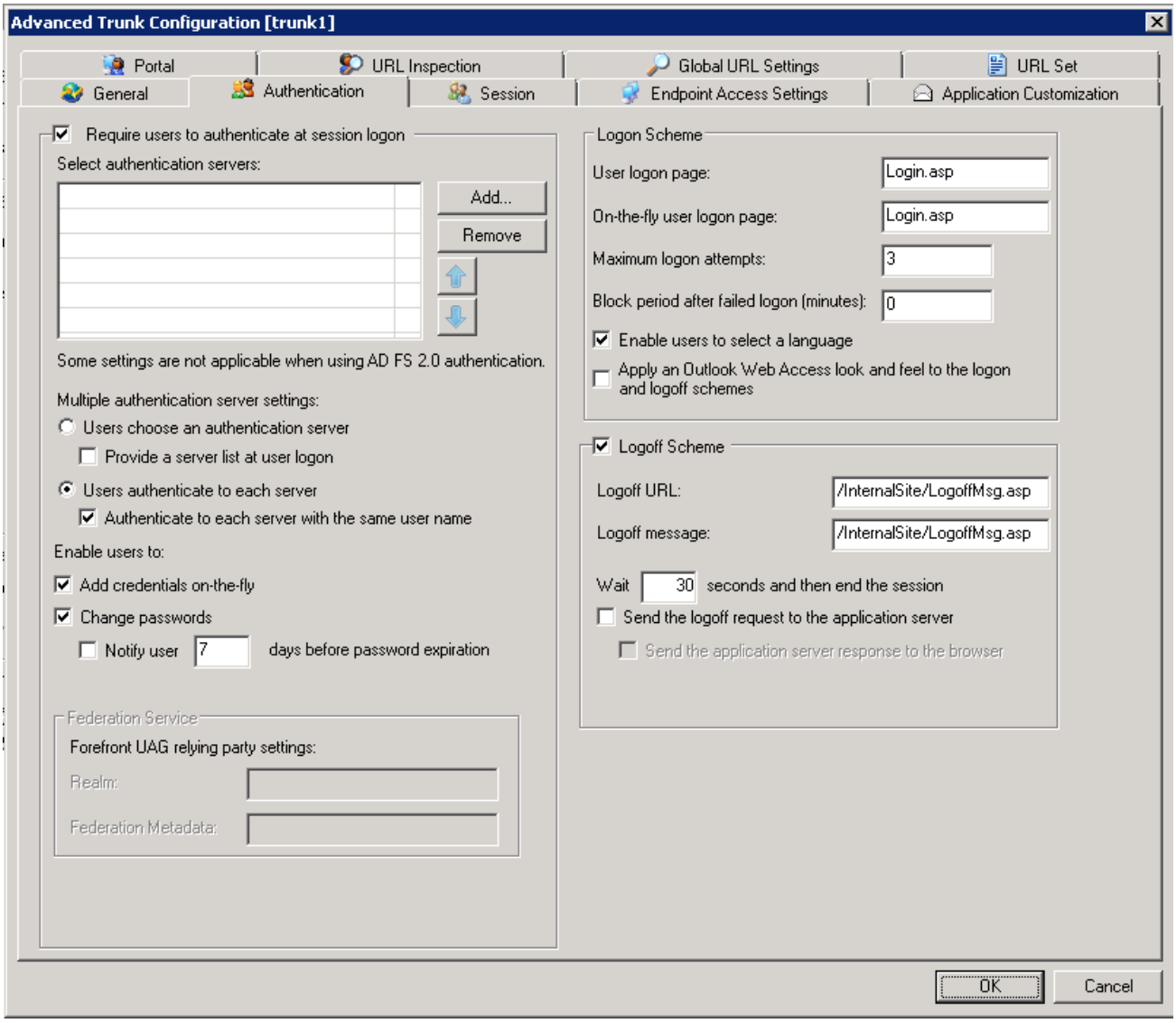
**2)** In the left-hand menu, under **Forefront UAG**, select the Trunk you would like to configure.



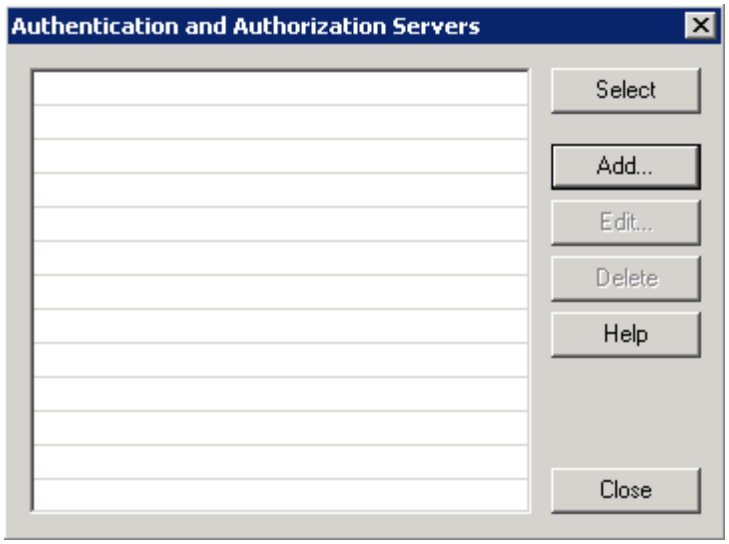

**3)** Once the Trunk settings are displayed, select the **Configure** button next to Configure trunk settings. **Advanced Trunk Configuration** dialog appears



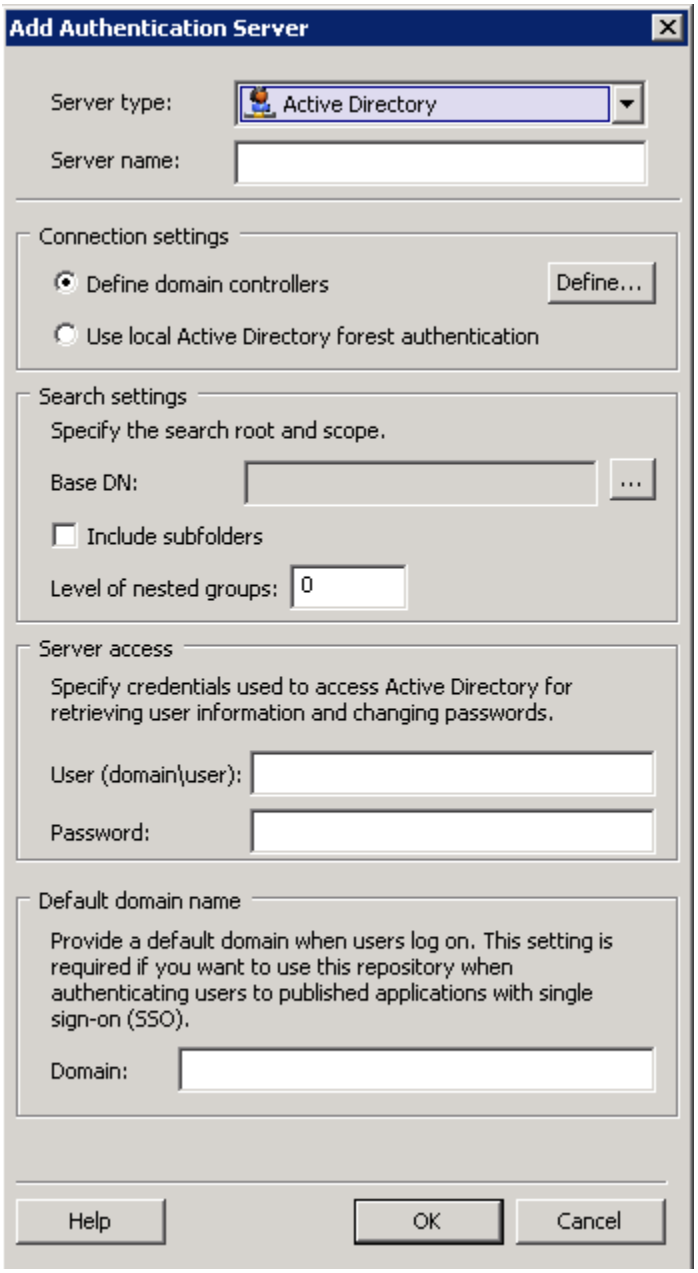

**4)** Select the **Authentication** tab
Make sure that **Require users to authenticate at session login** checkbox, is selected




**5)** Next to the **Select Authentication Servers** box, click **Add**…
**Authentication and Authorization Servers** list is displayed

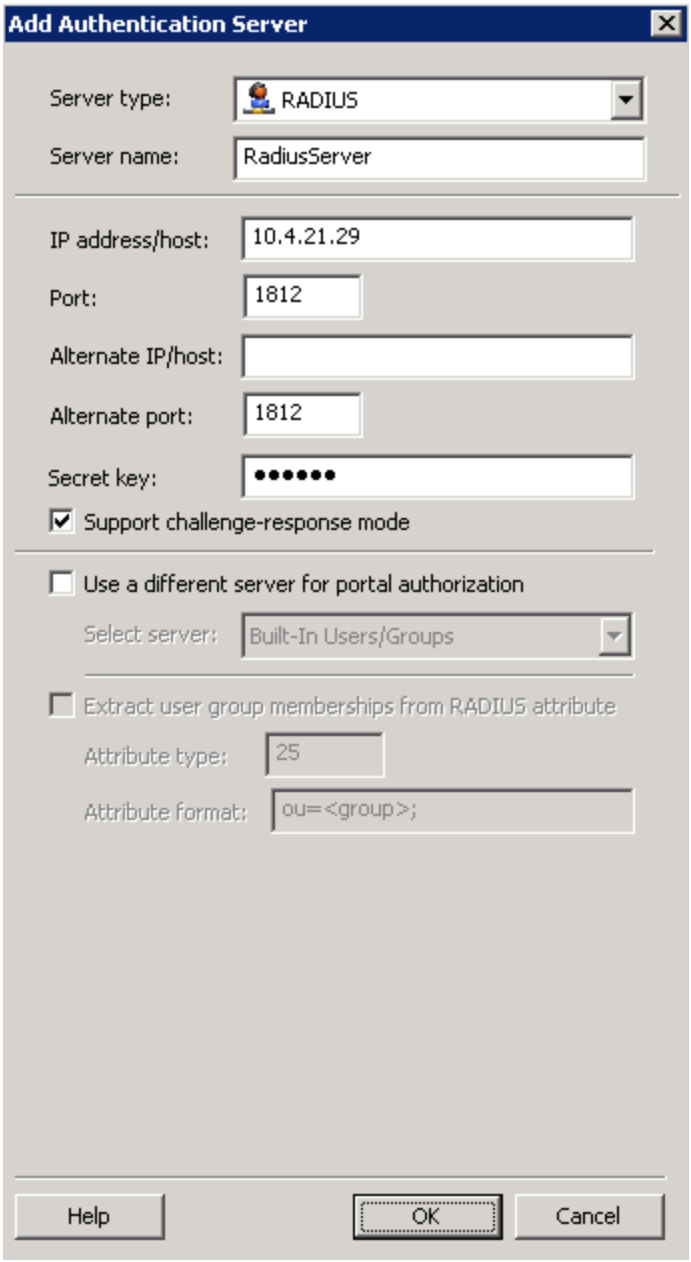



**6)** In the **Authentication and Authorization Servers** dialog click **Add…**
**Add Authentication Server** dialog appears

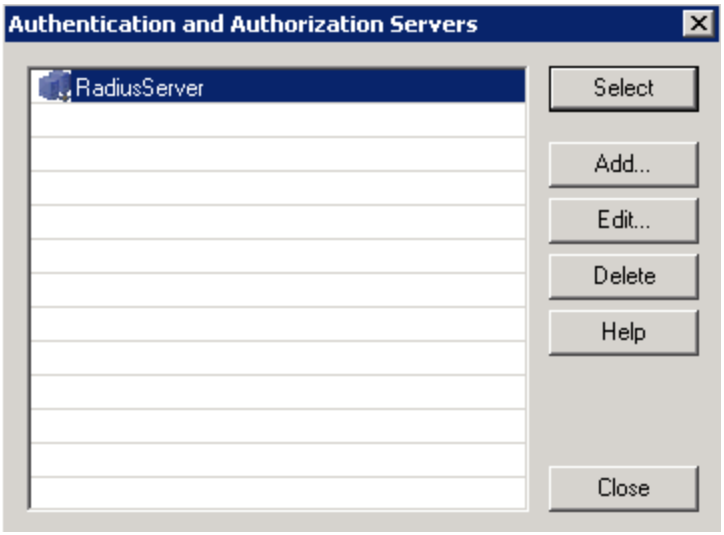



**7)** Enter following information to add **RADIUS** server

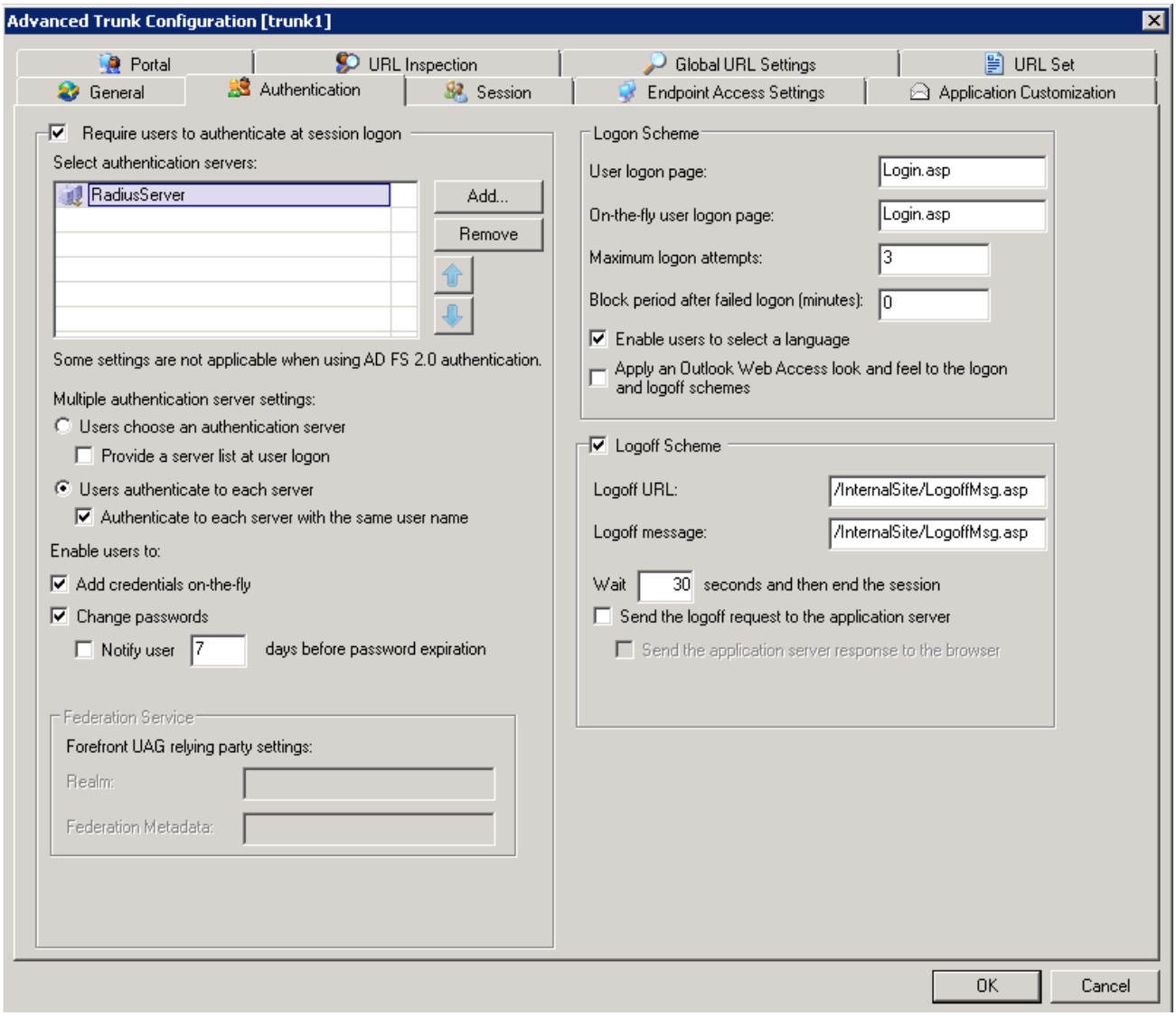
- Select RADIUS in Server type: drop-down
- In the Server name: field, enter a value, for example RadiusServer.
- Enter the IP address/hostname of the IdentityGuard Server in the IP/Host: field.
- In the Port: field, enter the port number your RADIUS server will use.
  **Note:** To enable IG failover at the VPN level, you could enter a backup or replica IG server in the Alternate IP/Host: entry.
- For Secret Key: enter the same value as entered for the VPN definition on the IdentityGuard server.
- Select the **Support challenge-response mode** check box.




**8)** Click **OK**
Newly created **RadiusServer** will appear in the **Authentication and Authorization Servers** list




**9)** Highlight the newly created **RadiusServer**, and click **Select**
The selected server should appear in the **Authentication servers** list




**10)** Ensure that **Users authenticate to each server** is selected and **Authenticate to each server with the same user name** is checked.
**11)** Click **OK** and save your new configuration.

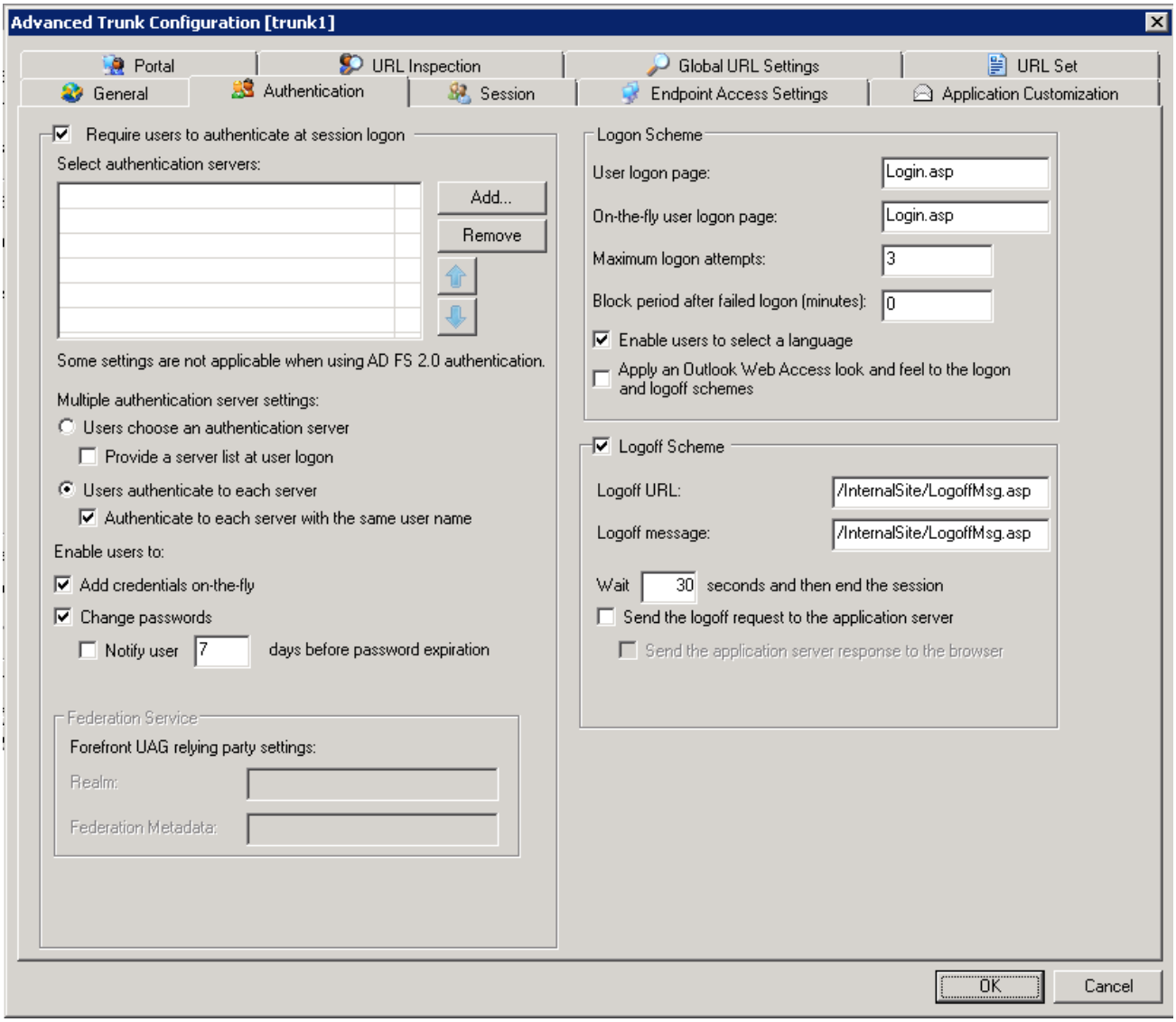
## Chaining Entrust IdentityGuard and Active Directory authentication

The Microsoft Forefront Unified Access Gateway VPN has a configuration option that allows you to display all authentication server prompts on one login page. This implementation works when using native VPN Active Directory (or LDAP) authentication as first factor and Entrust IdentityGuard one-step token (see To configure Entrust IdentityGuard One-Step Token and Active Directory Authentication) or another Entrust IdentityGuard authentication method for second-factor authentication (see To configure Entrust IdentityGuard second-factor and Active Directory authentication).

## To configure Entrust IdentityGuard One-Step Token and Active Directory Authentication

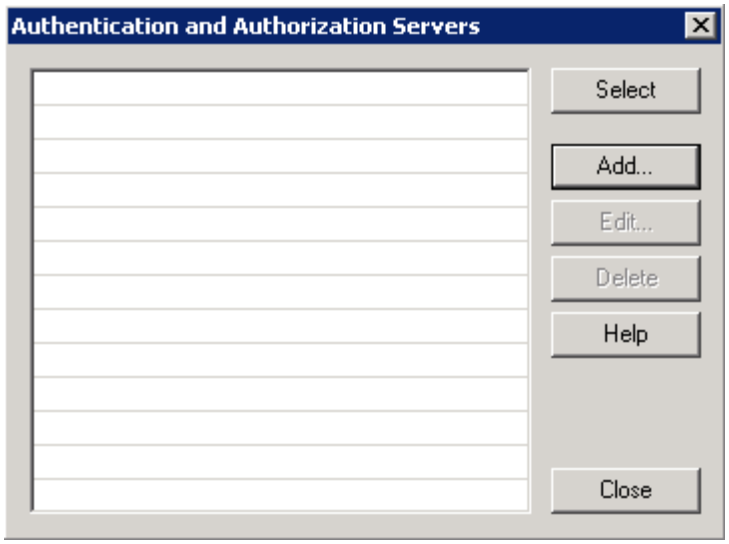
**1)** Follow steps 1 to 3 from section, "Configuring the Microsoft Forefront Unified Access Gateway VPN" on page 15

**2)** Select the **Authentication** tab.




**3)** Next to the **Select Authentication Servers** box, click **Add…**

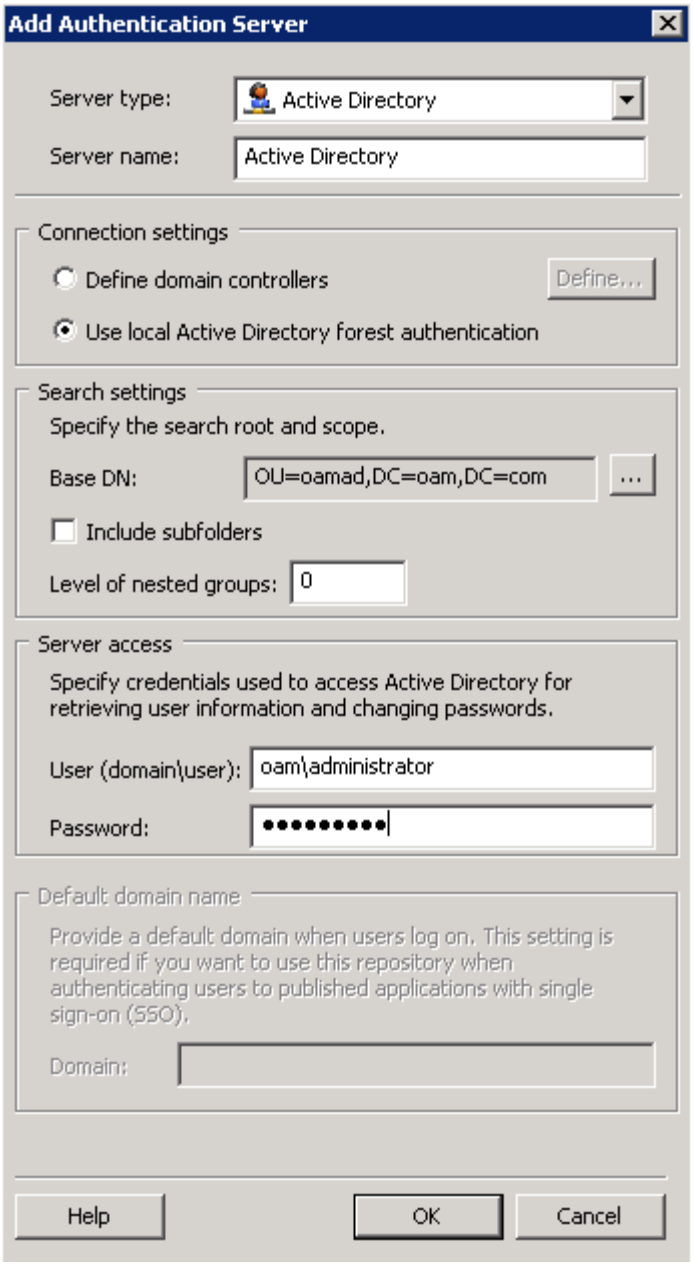
**Authentication and Authorization Servers** list is displayed




**4)** In the **Authentication and Authorization Servers** window click **Add…**

**Note:** If you have an existing Active Directory Authentication server entry that you would like to use as the first-factor authentication, skip the next step and move on to Step 6.

**5)** Enter the following information to add Active Directory server for authentication.




a) Select **Active Directory** in the **Server type:** drop-down.

b) In the **Server name:** enter the name of the server or repository (ex: Active Directory).

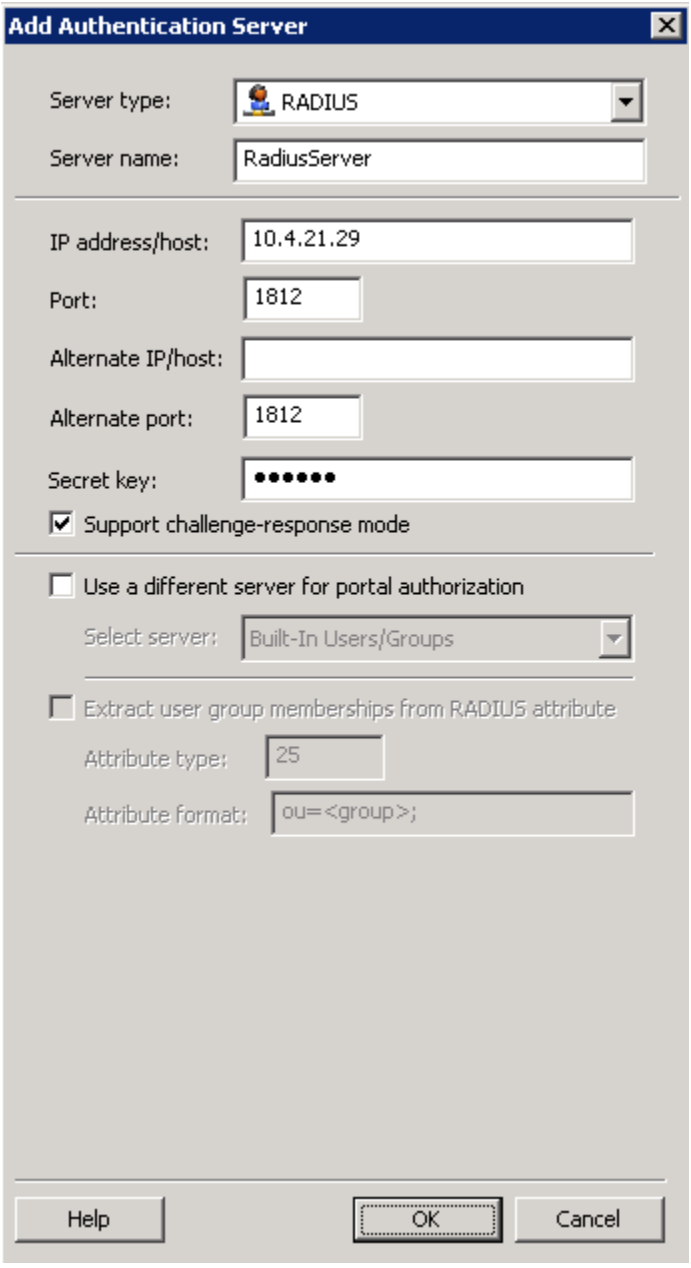
c) In the **Base DN field:** enter the root and scope to search for users (ex: OU=serverad,DC=example,DC=com).

d) Enter credentials to access the Active Directory server.

e) Click **OK.**

**6)** Create an additional RADIUS authentication server for Entrust IdentityGuard by clicking **Add…** in the **Authentication and Authorization Servers** window.

Enter the following information to add a RADIUS server.




a) Select **RADIUS** in the **Server type:** drop-down.

b) In the **Server name:** enter the name of server (ex: RadiusServer).

c) In the **Port:** enter the port number your RADIUS server be using.

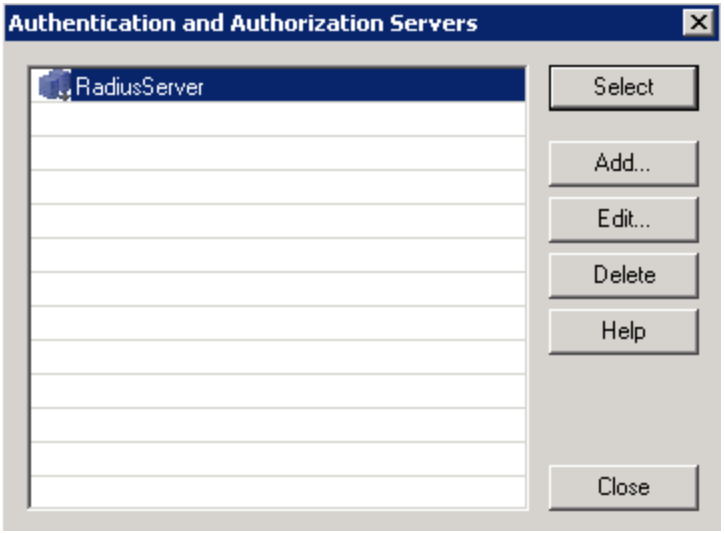
**Note:** To enable IG failover at the VPN level, you can enter a backup or replica IG server in the **Alternate IP/Host:** entry.

d) In the **Secret Key:** enter the same value as entered for the VPN definition on the IdentityGuard server.

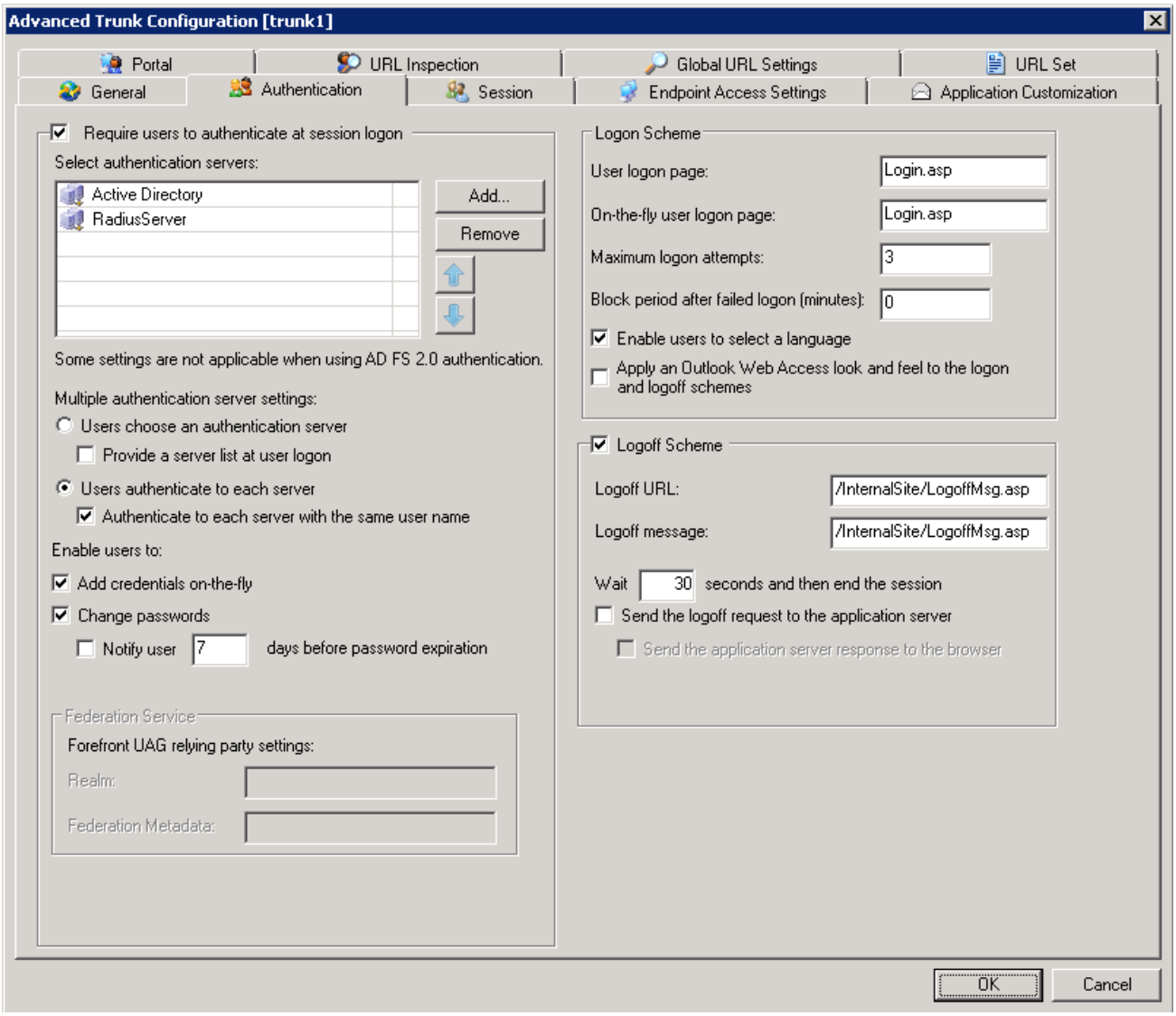
e) Select the **Support Challenge Response** check box

f) Click **OK.**

**7)** In the **Authentication and Authorization Servers** window highlight the newly created IdentityGuard entry and click **Select**. Repeat the same step for the Active Directory server entry. Both IdentityGuard and Active Directory entries should be visible in the **Select authentication servers** list.




**8)** Ensure that the **Active Directory** server entry is first on the list, ahead of the IdentityGuard server entry.




**9)** Select **Users authenticate to each server** option. **Authenticate to each server with the same user name** must also be selected.

**10)** Click **OK** and save your configuration.

**11)** In Entrust IdentityGuard, you need to ensure that the VPN server definition for Microsoft Forefront Unified Access Gateway has the First-Factor Authentication Method set to “Entrust IdentityGuard Token”.

## To configure Entrust IdentityGuard second-factor and Active Directory authentication

This configuration is similar to the last setup but in this setup IdentityGuard challenge is shown to the user after they enter their Active Directory credentials. As part of the Forefront Unified Access Gateway configuration both Active Directory and IdentityGuard servers are added to the authentication servers list, therefore the login page then shows multiple password fields, one for each of the authentication servers. Even though a password entry is not required for the IdentityGuard server in this setup, the user is forced to enter a value in the password field. The workaround is to edit the login page file (`Login.asp`) to hide the IdentityGuard password field. The instructions below will show the steps needed to do this. If these steps are not followed then the users will be required to enter at least one character into the field to continue.

Complete steps **1** to **13** (inclusively) from the previous procedure before moving on to the instructions shown below. We highly recommend that you make a copy of `Login.asp`, rename it and point to the new renamed file in your Forefront Unified Access Gateway configuration.

**1)** Make a copy of the file **`<Forefront Unified Access Gateway install dir>\Microsoft Forefront Unified Access Gateway\von\InternalSite\Login.asp`** and rename the copied file, for example **`Entrust_Login.asp`**.

**2)** Open the renamed file, `Entrust_Login.asp`, and locate the first occurrence of the line that starts with "**for each repository_name**".

**3)** Replace the following lines:

```
for each repository_name in repositories.NameVec
            if not use_the_same_user_name then%>
            <TR>
             <TD class="paramText"><%=repository_name%> <%=GetString(108,
"User Name:")%></TD>
             <TD><INPUT class="paramTextbox" TYPE="text" ID="user_name"
NAME="user_name" maxLength="<%=UserNameLimit%>" size="11"></TD>
            </TR>
            <%end if%>
           <TR>
            <TD class="paramText"><%=repository_name%> <%=GetString(109,
"Password:")%></TD>
            <TD><INPUT class="paramTextbox" TYPE="password" ID="password"
NAME="password" maxLength="<%=PasswordLimit%>"
onkeypress="capsDetect(arguments[0]);" size="11"></TD>
           </TR>
```

with these lines:

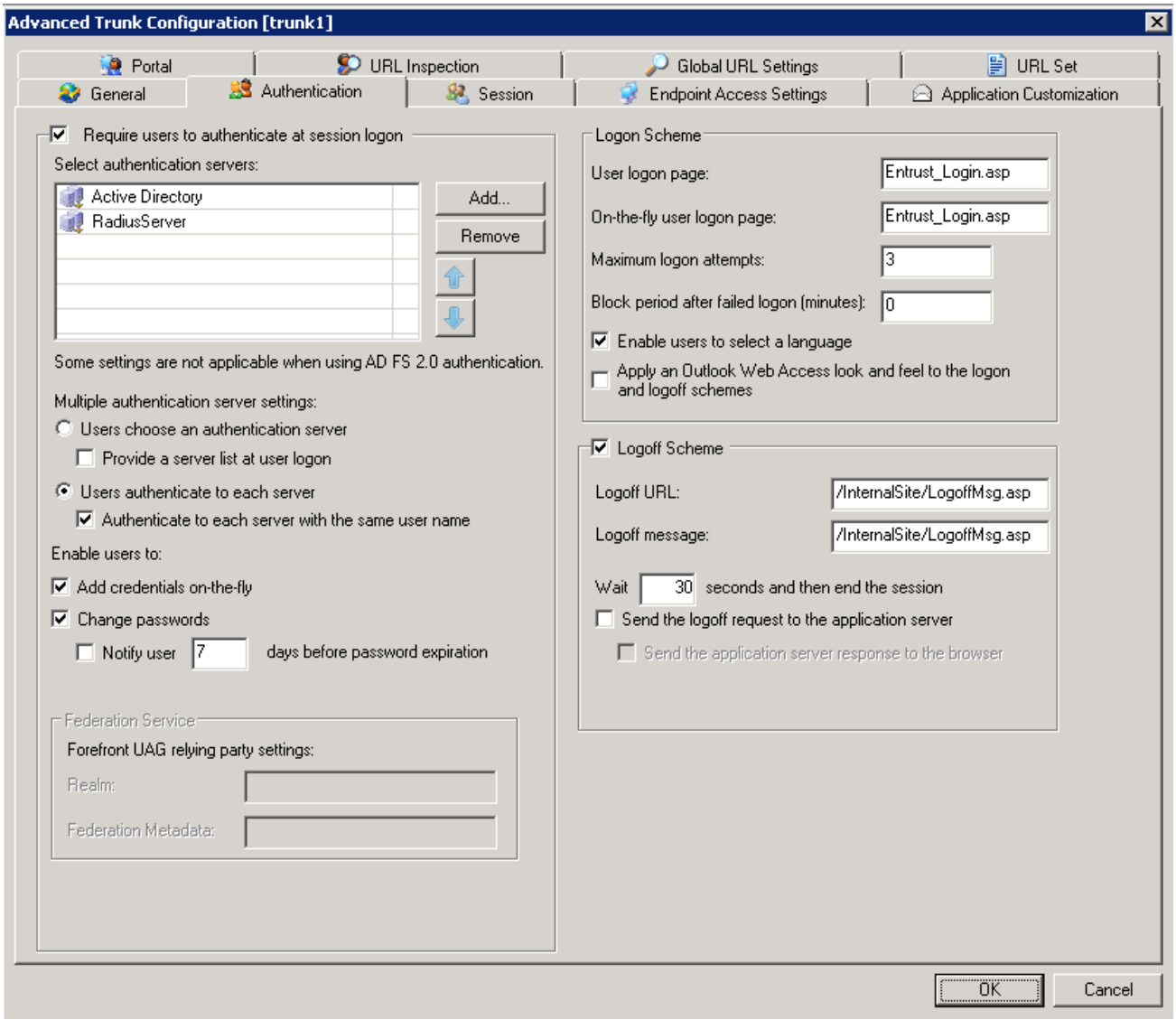
```
for each repository_name in repositories.NameVec
            if not use_the_same_user_name then%>
            <TR>
             <TD class="paramText"><%=repository_name%> <%=GetString(108,
"User Name:")%></TD>
             <TD><INPUT class="paramTextbox" TYPE="text" ID="user_name"
NAME="user_name" maxLength="<%=UserNameLimit%>" size="11"></TD>
            </TR>
            <%end if%>
            <%if repository_name = "RadiusServer" then%>
             <INPUT TYPE="hidden" ID="password" NAME="password" VALUE="abc">
            <%else%>
            <TR>
             <TD class="paramText"><%=repository_name%> <%=GetString(109,
```

```
"Password:")%></TD>
             <TD><INPUT class="paramTextbox" TYPE="password" ID="password"
NAME="password" maxLength="<%=PasswordLimit%>"
onkeypress="capsDetect(arguments[0]);" size="11"></TD>
            </TR>
            <%end if%>
```

**4)** Ensure that the name of the **IdentityGuard server** defined in your Forefront Unified Access Gateway configuration is the same name used in the line **`<%if repository_name = "RadiusServer" then%>`**.

**5)** Save and close `Entrust_Login.asp`.

**6)** In your **Authentication** window, point your **User logon page** and **On-the-fly user logon page** to the modified file.



**7)** Click **OK** and save your configuration.

**8)** In Entrust IdentityGuard, ensure that the VPN server definition for Microsoft Forefront Unified Access Gateway has the First-Factor Authentication Method set to “No First-Factor Authentication”.

# Testing the integration

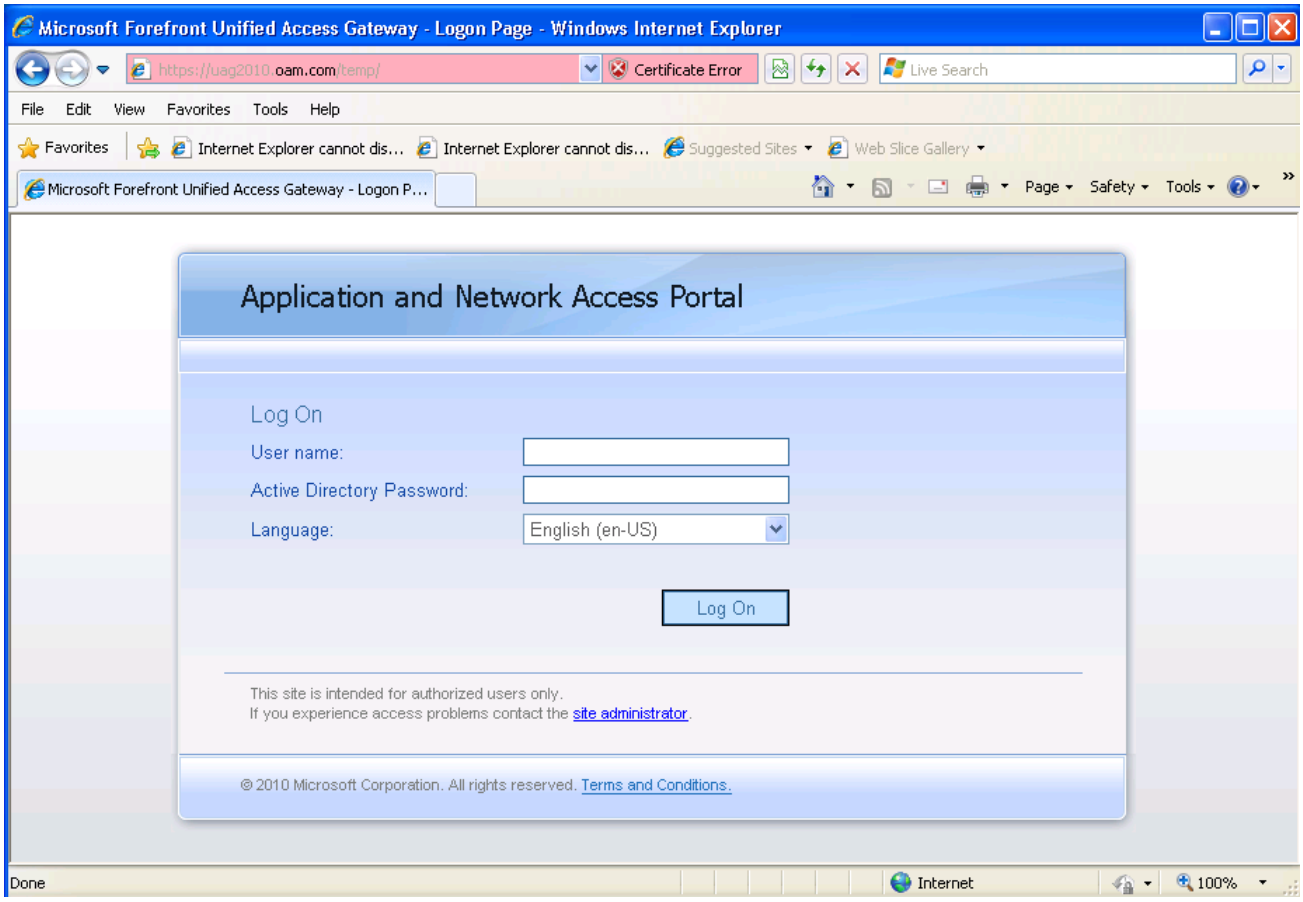
After configuring your Microsoft Forefront Unified Access Gateway and Entrust IdentityGuard, use a standard Web browser to test the integration to ensure you configured everything correctly.



## Testing one-step or two-step Entrust IdentityGuard authentication

This test scenario can be used if you set up an Entrust IdentityGuard server as a second-factor authentication resource, using authentication methods like GRID, TOKEN, 'Knowledge-based questions and answers' or One-time password. This test can also be used to test one-step token response authentication.

**1)** Open a Web browser and enter the URL for your site.




**2)** Enter the IdentityGuard user name in the **User Name** field.

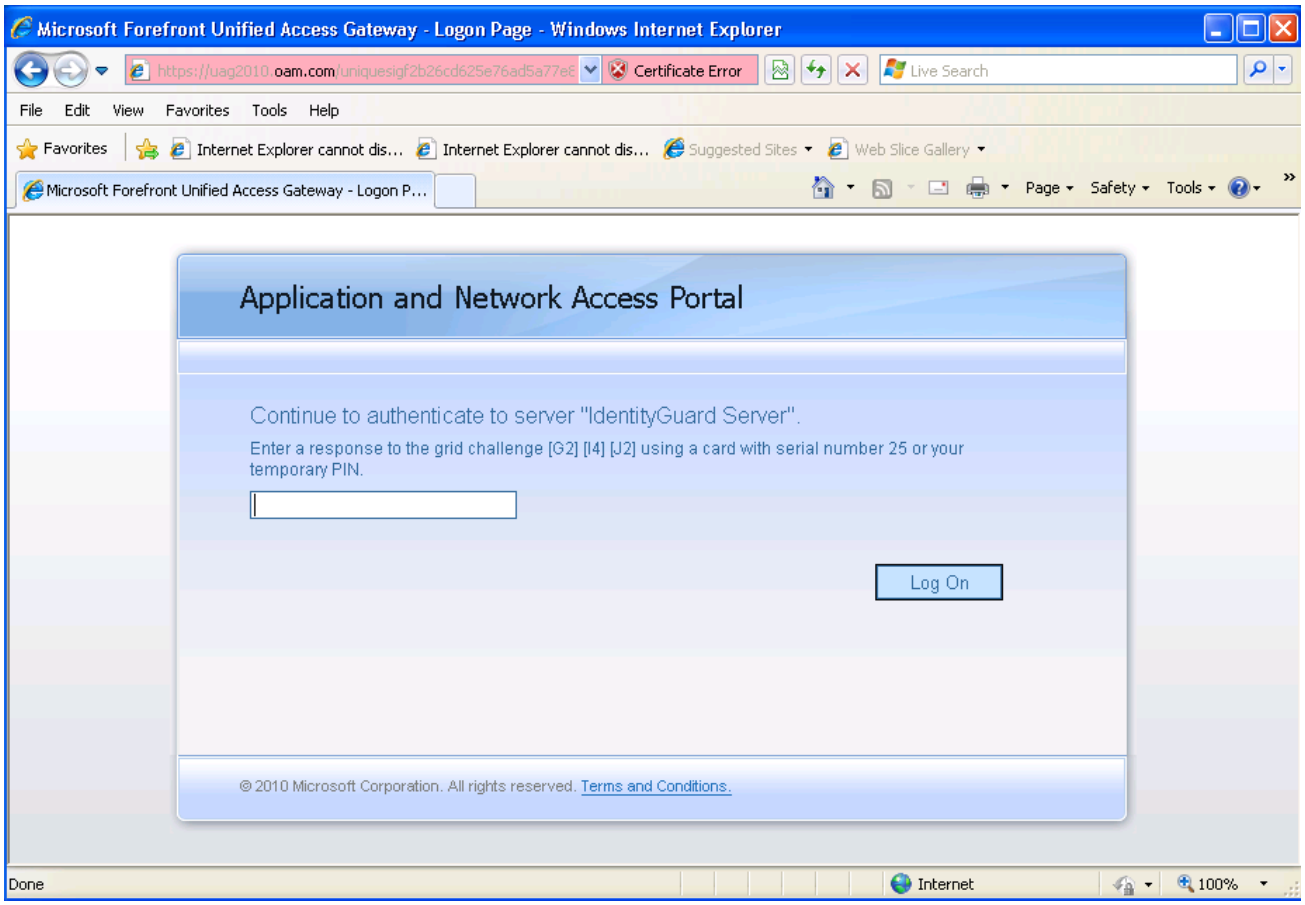
**3)** In the **Password** field, do one of the following:

- If you are using one-step token authentication, enter the token response.

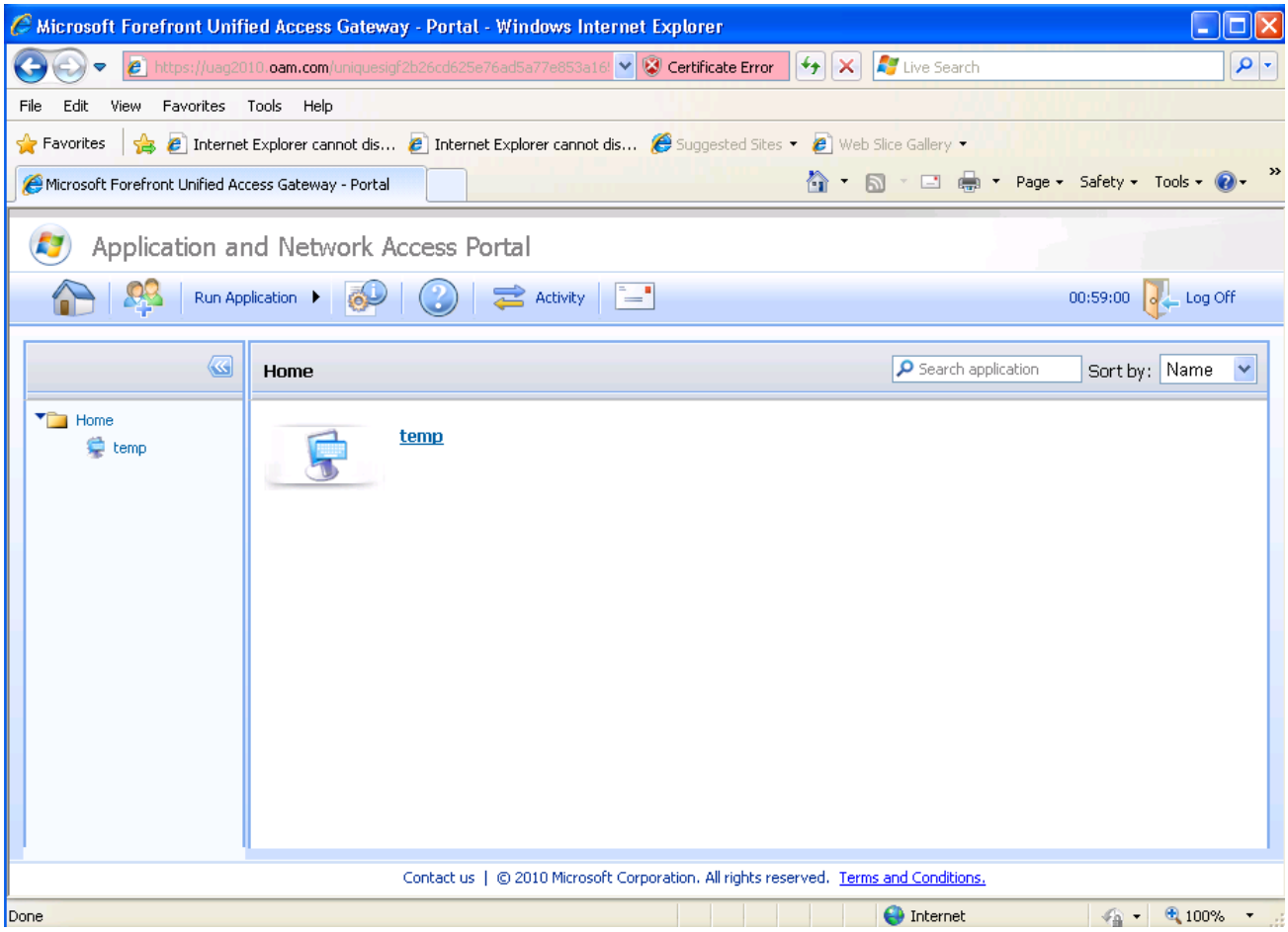
- If you are using two-step authentication, enter the password for your first-factor authentication resource, such as Active Directory password, Entrust IdentityGuard Password and so on.

**4)** Click **Submit**.

**5)** For two-step authentication you will now be challenged to enter your second-factor credentials.

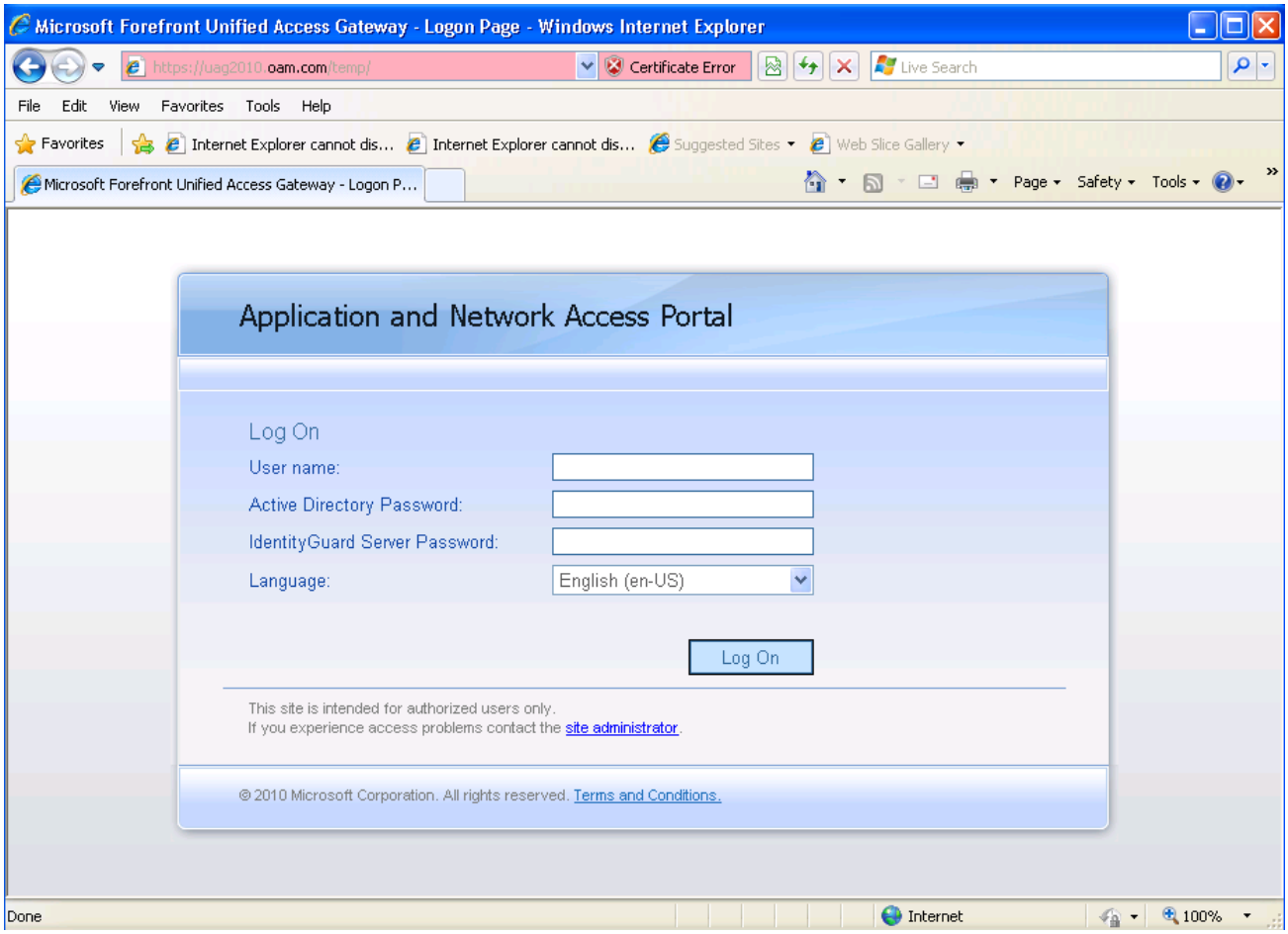



**6)** Once authenticated, you will be logged in to the site.




## Testing Entrust IdentityGuard One-Step Token chained with Active Directory authentication

**1)** Open a Web browser and enter the URL for your site.



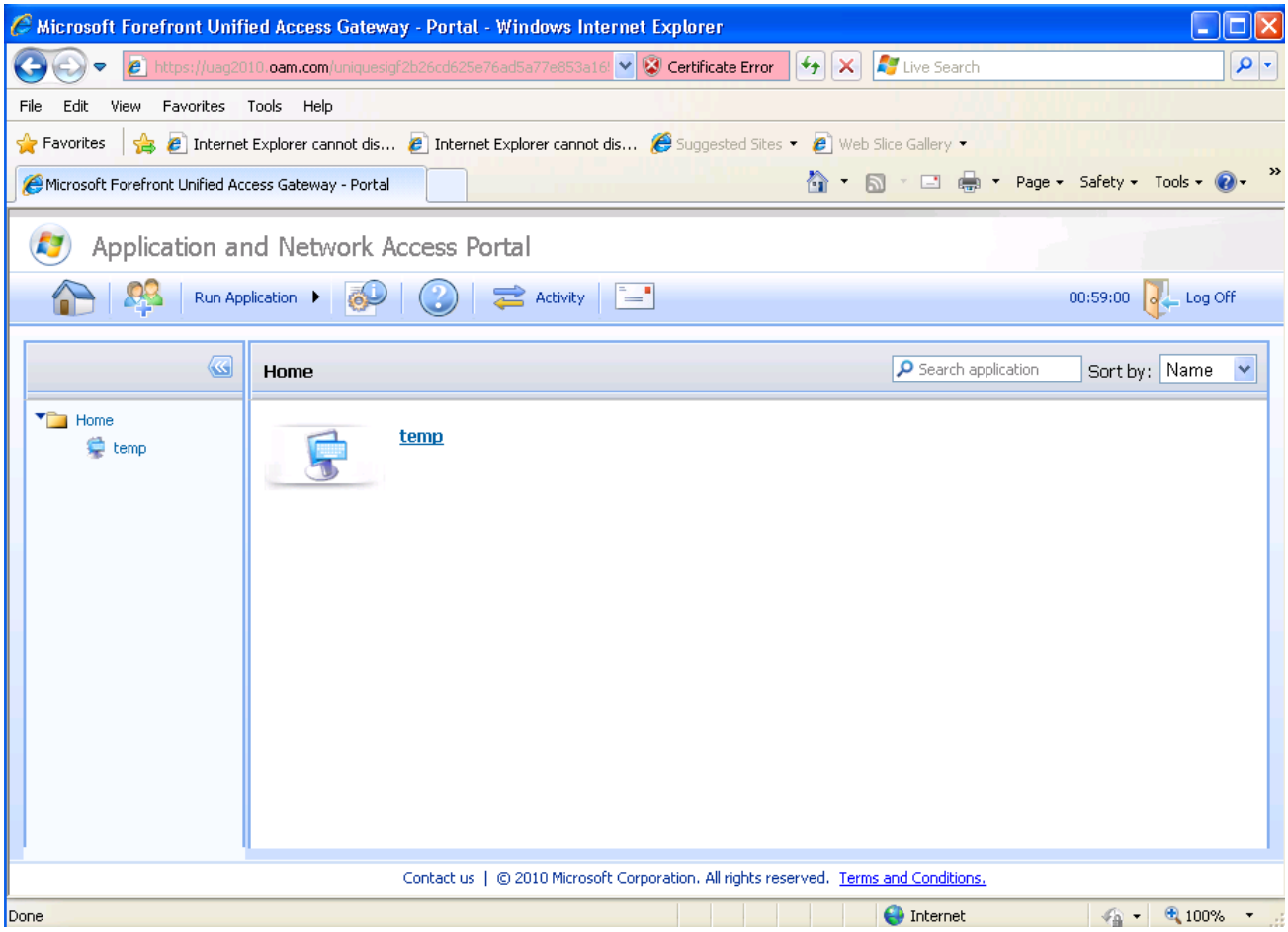

a) Enter your Active Directory/Entrust IdentityGuard user name in the **User Name** field.

b) Enter the Active Directory password in the **Active Directory Password** field.

c) Enter the Entrust IdentityGuard server password in the **IdentityGuard Server Password** field.

d) Click **Submit**.

**2)** If successfully authenticated, you will be logged in to the site.




## Using a PVN with your second-factor authentication response

When using tokens with a PVN, see the information about using a token in the *Entrust IdentityGuard Administration Guide*. When using the Radius proxy, PVNs are specified as part of the token or grid response.

For example, if your PVN is 1234, and the token response is 94167505, the combined Radius password is entered as: 123494167505 (PVN first, followed by token response). The PVN and grid response are combined similarly.

It is also possible for users to change PVNs using the VPN client interface. In addition to the default method, a new option called “Separate Challenge for PVN update” had been introduced since IdentityGuard 9.1.

In the default behavior, Entrust IdentityGuard displays one prompt, at which the user must enter the old PVN, the challenge response, the new PVN, and confirmation of the new PVN all on one line, in the following format:

```
old pvn + challenge response + new pvn + new pvn
```

With the Separate Challenge option enabled, Entrust IdentityGuard displays three prompts, allowing the user to enter the information separately, in the following format:

```
old pvn + challenge response
```

```
new pvn
```

```
new pvn
```

For details of how to enable "Separate Challenge for PVN update" and other related information, see the *Entrust IdentityGuard Administrators Guide*.

# Troubleshooting

If you encounter problems during the integration of your Microsoft Forefront Unified Access Gateway with Entrust IdentityGuard, see the log files. For information about Entrust IdentityGuard log files, see the *Entrust IdentityGuard Administration Guide.*

# Known Issues

**Problem:** When Entrust IdentityGuard responds to Forefront Unified Access Gateway with an Access-Reject message, the VPN displays the login page requesting the user name and password. An Access-Reject message can be returned by Entrust IdentityGuard when the user is locked out due to too many incorrect login attempts. Without the error message the user has no idea why they can't log in using their first-factor credentials.

**Cause:** We are unclear at this point why the VPN behaves like this, as it should show the error message similar to when a user enters a wrong respond to the Entrust IdentityGuard challenge.

**Solution:** There is currently no solution to this problem. This issue has been raised with Microsoft.

**Problem:** IP Geo RBA does not work with UAG 2010.

**Cause:** UAG 2010 sends the client-IP as an attribute NAS-IP-ATTRIBUTE, which Entrust IdentityGuard cannot process. It expects the IP address to be in string format, whereas it comes as hex address of actual ip address.

**Solution:** ~~There is currently no solution to this problem. In the future release of Entrust IdentityGuard this attribute NAS-IP-ADDRESS may be supported.~~. This problem is addressed in Entrust IdentityGuard 10.1 patch release.