Indian Health Service

The Federal Health Program for American Indians and Alaska Natives

IHS VPN User Guide

Version 1.3
July 2011

IHS Office of Information Technology
Albuquerque, New Mexico

Document Information

Audience

This manual is intended for users of the Citrix-based IHS Virtual Private Network (VPN) that was implemented and introduced in 2010.

Acknowledgements

Citrix® is a registered trademark of Citrix Systems, Inc., in the U.S. and/or other countries. All Rights Reserved.

Revision History

VERSION	DATE	DESCRIPTION OF CHANGES
1.0	9/30/2010	First published version.
1.1	11/16/2010	Added instructions for PhoneFactor security questions (Section 3.2).
1.2	2/4/2011	Added warning about not using plus sign (+) and ampersand (&) in D1 passwords.
1.3	7/5/2011	Added clarifications about the need to log in to the D1 domain before defining the PhoneFactor security questions (Section 3.2).

Table of Contents

1. Introduction

If it has not happened already, you will soon be migrated to the new Remote Access Citrix / AEP SSL VPN. (Virtual Private Network) for the Indian Health Service.

The previous implementation for providing remote access via VPN to IHS networks and data came under scrutiny by the Office of Inspector General (OIG) in October of 2008, as part of its investigation of a cyber-attack on the IHS network. The investigation identified a number of vulnerabilities and shortfalls with the previous VPN system. In response to this, IHS has implemented the ARRA-funded project, Remote Access Citrix / AEP SSL VPN solution, to bring IHS into compliance with Federal and Departmental mandates and requirements.

OIT has completed all required configuration and testing stages and is now ready to begin migrating existing VPN users to the new VPN solution.

This document provides you with some background on the new VPN. It then walks you through the login process and the process required to launch an RDP application.

1.1. How the VPN Works

The new VPN enables you to access your network drives and also to use the following common applications without installing the software on your workstation:

- Microsoft Office 2007 suite
- Adobe Acrobat Reader 9
- VanDyke SecureCRT 6.5 Telnet Client

The web-based VPN acts as a “window” to a set of centralized **Citrix servers,** shared by all VPN users. These servers host the set of common applications.

Additionally, the VPN enables you to access applications that are not part of the Citrix environment via the Remote Desktop Protocol (RDP).

1.1.1. Two-Factor Authentication

When you first log in to the system, you are prompted to enter your User Name, Password, and **V-Realm Authentication method**. The V-Realm Authentication method uses **two-factor authentication**—something you know (e.g., a password) and something you have (like a phone)—to verify that you are who you say you are. Two-factor authentication is required to establish additional security for the IHS VPN and network.

IHS supports two different V-Realm Authentication methods:

- The **Phone V-Realm** requires the use of a physical phone (landline or cell). After you log in with your username and password, a program named PhoneFactor calls the phone number you supplied when you obtained authorization for VPN access. Your response to the call is then used as part of authentication.

- The **Token V-Realm** requires the use of an Entrust Token. This physical device generates an authentication number that you enter in addition to your username and password as part of the VPN login process.

Figure 1: Entrust token

After authentication, you are presented with access to the available applications and/or desktops.

See Section 2.1 for login instructions.

1.1.2. VPN Limitations

Because of IHS Security requirements, certain functionality will not be available during a VPN session. Here are some of the differences that you can expect:

- Access to the server's local drives and CD-ROM drive is restricted.
- You will not be able to save documents to local drives or copy files to them. However, you can save documents to your network drives.
- Because this is a shared system used by several people at once, you will not be able to install any applications yourself.

  If you would like to have an additional application made available via the VPN, please send a request to your manager, who will in turn submit your request to OIT for review. However, only applications that would be useful for all IHS VPN users will be approved.
- Printing from a VPN session uses a universal driver. This driver may not support all the features of some printers.
- You will not be able to access the Citrix desktop if your D1 password contains the plus sign (+) or ampersand (&), because these are reserved characters in Citrix.

See Section 3.1 for a detailed list of modifications and limitations.

1.1.3. Access Points for Geographical Zones

The IHS VPN has been created with two geographical zones, East and West. This has been done to provide the fastest access based on your own geographical location.

- People accessing the VPN from the eastern half of the country should use the following link: https://hq2apps.ihs.gov
- People accessing the VPN from the western half of the country should use the following link: https://hq1apps.ihs.gov

These links will redirect you to your respective AEP SSL-VPN, which handles user authentication.

1.2. Obtaining VPN Access

To obtain access to the VPN, you should discuss your business needs with your supervisor. You should also determine which authentication method is best for you:

- PhoneFactor – If you choose this, you will need to supply the phone number of the phone you will use (landline or mobile); and you will need to have this phone with you each time you log in to the VPN.

  You should also define four security questions using the PhoneFactor Portal. Although these are not required to log in to the VPN, they are required to validate your identity when you call the Help Desk for assistance. (See Section 3.2 for details.)

- Entrust – If you choose this, you will be sent a token, and you must have the token with you each time you log in to the VPN.

Next, your supervisor enters the request and related information into the electronic ITAC system.

The request is then reviewed by the designated approvers. If approved, notification that access has been granted is sent to your supervisor, and for Entrust, a token is shipped to you.

1.3. About VPN Support

Technical Support for the AEP/Citrix-based VPN is handled similarly to any other part of the IHS network. Specifically:

- During normal business hours, users should report problems to their local (Tier 1) or Area (Tier 2) support staff. That staff can then escalate the issue, if necessary to Tier 3, which is handled by the OIT Help Desk (see below).
- For after-hours support, users should call the OIT Help Desk phone number (see below). This number is forwarded to the NOSC, which provides after-hours support.

See also the *OIT Customer Service Handbook* for details about the Service Level Agreements (SLAs) for the AEP/Citrix-based VPN.

1.4. Contact Information

If you have any questions or comments regarding the VPN or this document, please contact the OIT Help Desk at IHS:

Phone:	505.248.4371 or 888.830.7280
Fax:	505.248.4363
Web:	http://www.ihs.gov/GeneralWeb/HelpCenter/Helpdesk/index.cfm
E-Mail:	support@ihs.gov

2. How to Use the New VPN

The following sections will take you through the login process, show you how to access the applications, and show you where your data is kept.

Before you begin, be sure that you have either your Entrust token or the telephone that you designated for PhoneFactor authentication.

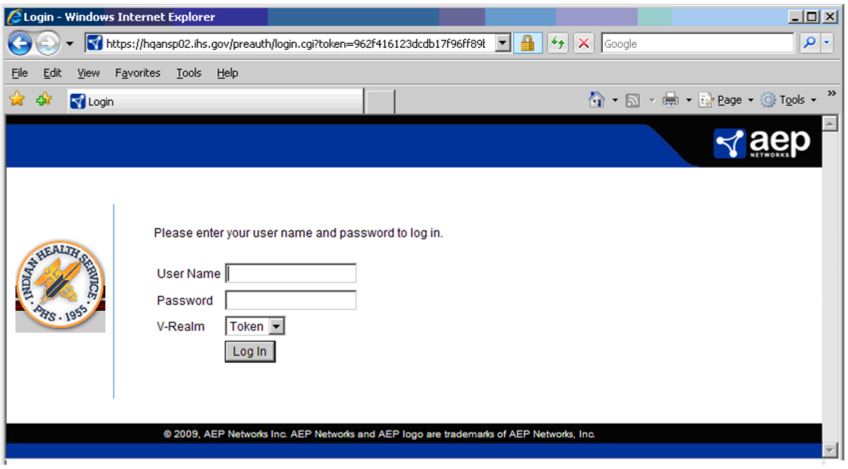
2.1. Logging In

1. Open your web browser and go to the URL appropriate for your location:

   East: https://hq2apps.ihs.gov

   West: https://hq1apps.ihs.gov

   The system displays a login page like the following:


Login - Windows Internet Explorer
https://hqansp02.ihs.gov/preauth/login.cgi?token=962f416123dcdb17f96ff89t
Google
File Edit View Favorites Tools Help
Login
Page Tools
aep NETWORKS
INDIAN HEALTH SERVICE · PHS · 1955
Log In

Please enter your user name and password to log in.

User Name

Password

V-Realm Token

© 2009, AEP Networks Inc. AEP Networks and AEP logo are trademarks of AEP Networks, Inc.

Figure 2: VPN Login page

2. Enter your IHS network (D1) user name and password in their respective fields.

> **WARNING**: If your D1 password contains a plus sign (**+**) or an ampersand (**&**), you will not be able to log in to the Citrix desktop. (These are reserved characters for Citrix.)

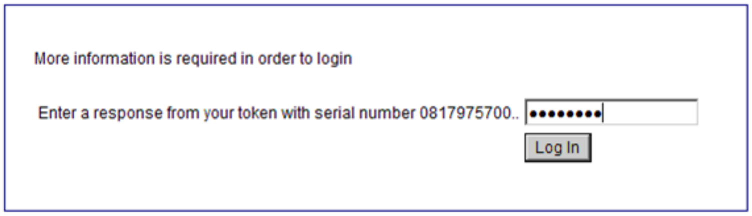
3. Make a selection from the **V-Realm** drop-down list, as follows:
   - If you have been assigned an Entrust token, select **Token**.
   - If you are using your phone for authentication, select **Phone**.

> **NOTE**: The **Local** option is available only for VPN Administrators.

4. Click the **Log In** button, to start the two-factor authentication process.

2.1.1. Authenticate with Entrust

If you chose Entrust authentication, the system displays the following prompts after you click **Log In**:



More information is required in order to login

Enter a response from your token with serial number 0817975700.. ••••••••

Figure 3: Entrust Authentication field

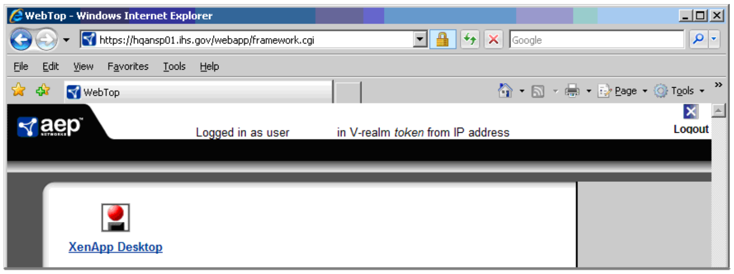
Continue with the following steps to complete the login process.

5. On the token, press the button that generates the authentication number.

6. When it is displayed, type the 8-digit authentication number into the field shown in Figure 3 above, **Enter a response from your token ....**

7. Click **Log In**.

At this point, the system displays the AEP NSP page containing the **XenApp** icon, and you can continue with the steps in Section 2.2 to set up the XenApp environment.



WebTop - Windows Internet Explorer

https://hqansp01.ihs.gov/webapp/framework.cgi

Logged in as user in V-realm *token* from IP address

Figure 4: AEP NSP page showing the XenApp Desktop icon

2.1.2. Authenticate with PhoneFactor

If you chose PhoneFactor authentication, the system calls the designated phone after you click the **Log In** button (Step 4 in Section 3.1). At this point, do the following:

1. Answer the phone.

2. Press the pound key (#) on the phone, and hang up.

The system then displays the AEP NSP page containing the **XenApp** icon, and you can continue with the steps in Section 2.2 to set up the XenApp environment.

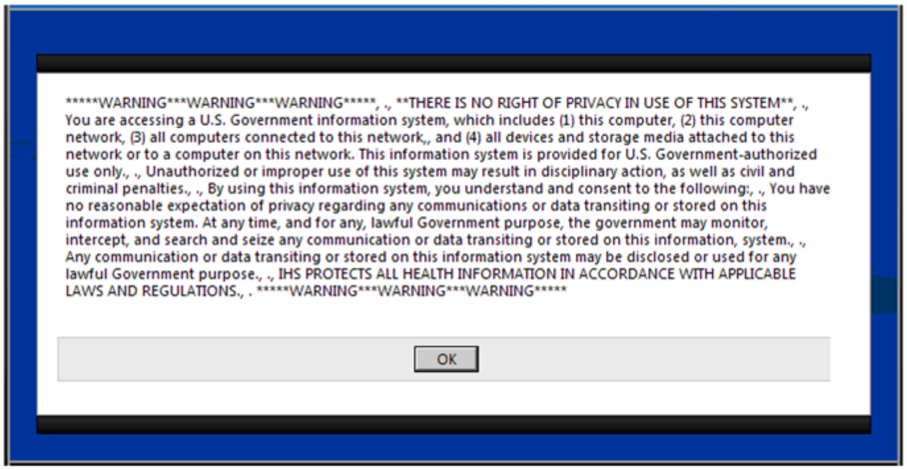
> **NOTE**: Be sure to log in to the PhoneFactor Portal to define your security questions. If you have not done so, the Help Desk will not be able to validate your identity when you call them for assistance. See Section 3.2.

2.2. Setting Up the XenApp Environment

The first time you connect to the Citrix environment, you will need to download and install the Citrix XenApp plug-in. Use the steps below to do this.

NOTE: This installation does not require administrative privileges.

1. Click the **XenApp** icon to display a Citrix XenApp page, containing the standard federal government privacy warning.



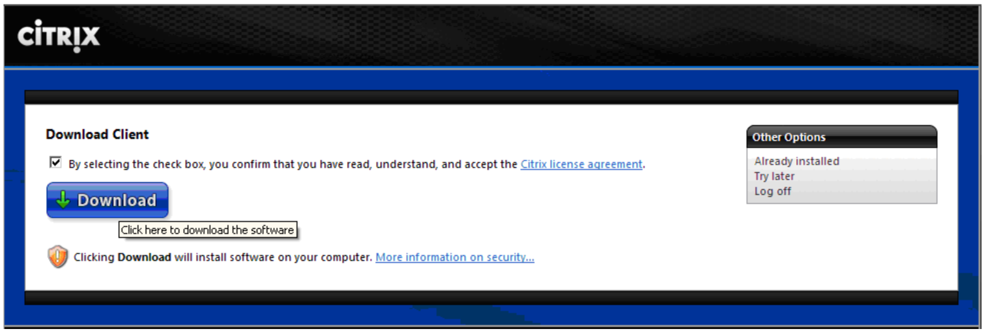
*****WARNING***WARNING***WARNING*****, ., **THERE IS NO RIGHT OF PRIVACY IN USE OF THIS SYSTEM**, ., You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network,, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only., ., Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties., ., By using this information system, you understand and consent to the following:, ., You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, and for any, lawful Government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information, system., ., Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose., ., IHS PROTECTS ALL HEALTH INFORMATION IN ACCORDANCE WITH APPLICABLE LAWS AND REGULATIONS., . *****WARNING***WARNING***WARNING*****

Figure 5: Federal government privacy warning

NOTE: If instead of this page, the system displays a **Logging in ...** message, the problem may be that your D1 password contains a Citrix reserved character (**+** or **&**). If so, you need to change your password to one without those characters before you can proceed.

2. Click **OK** to display the download screen.

3. Click in the checkbox to confirm that you accept the license agreement.



Download Client

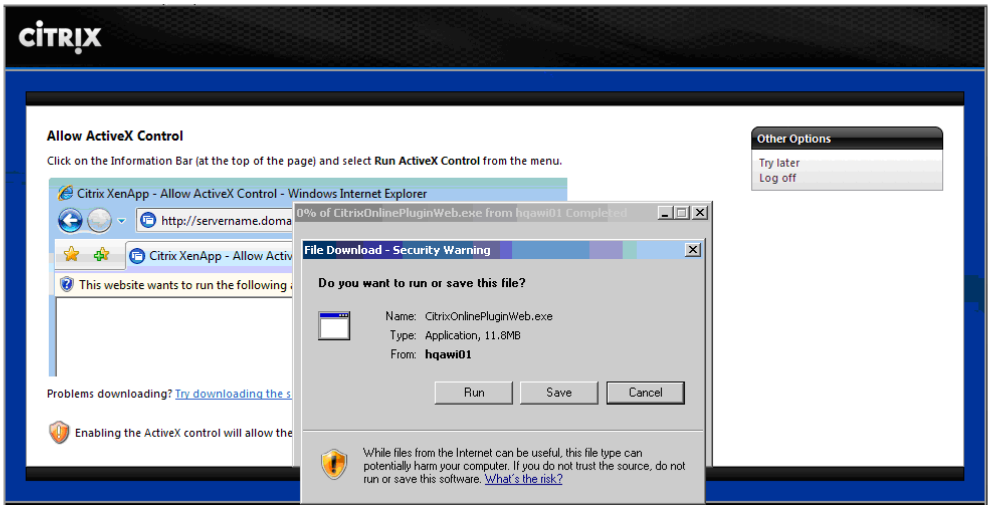
☑ By selecting the check box, you confirm that you have read, understand, and accept the Citrix license agreement.

Clicking **Download** will install software on your computer. More information on security...

Figure 6: Citrix plug-in download screen

4. Click the **Download** button to start the process.

5. On the Security Warning window, click **Run**.


CITRIX
Other Options
Try later
Log off
Citrix XenApp - Allow ActiveX Control - Windows Internet Explorer
http://servername.doma
Citrix XenApp - Allow Activ
0% of CitrixOnlinePluginWeb.exe from hqawi01 Completed
Run
Save
Cancel

Allow ActiveX Control

Click on the Information Bar (at the top of the page) and select **Run ActiveX Control** from the menu.

This website wants to run the following

Problems downloading? Try downloading the s

Enabling the ActiveX control will allow the

File Download - Security Warning

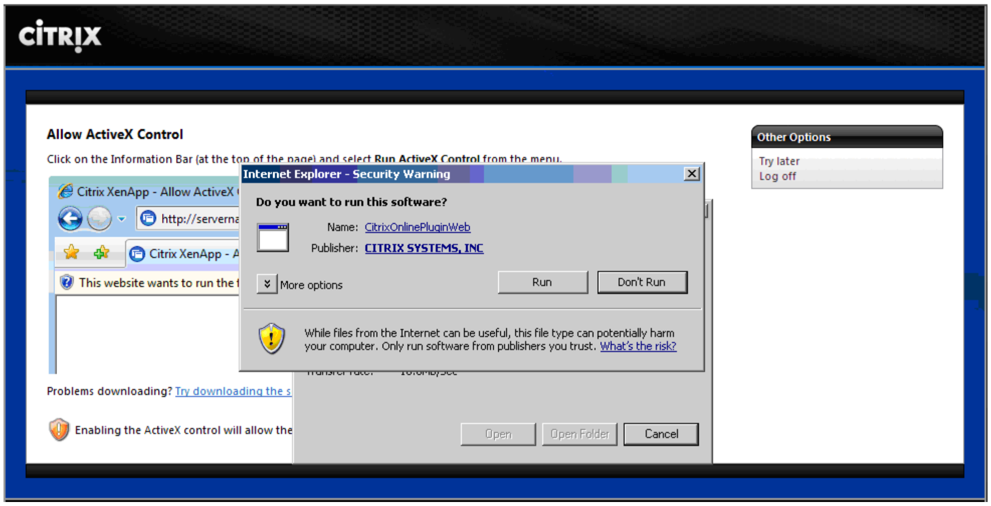
Do you want to run or save this file?

Name: CitrixOnlinePluginWeb.exe
Type: Application, 11.8MB
From: **hqawi01**

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

Figure 5: Security Warning window for download

When the download completes, the system displays a second Security Warning window.



Allow ActiveX Control

Click on the Information Bar (at the top of the page) and select **Run ActiveX Control** from the menu.

This website wants to run the

Problems downloading? Try downloading the s

Enabling the ActiveX control will allow the

Internet Explorer - Security Warning

Do you want to run this software?

Name: CitrixOnlinePluginWeb
Publisher: **CITRIX SYSTEMS, INC**

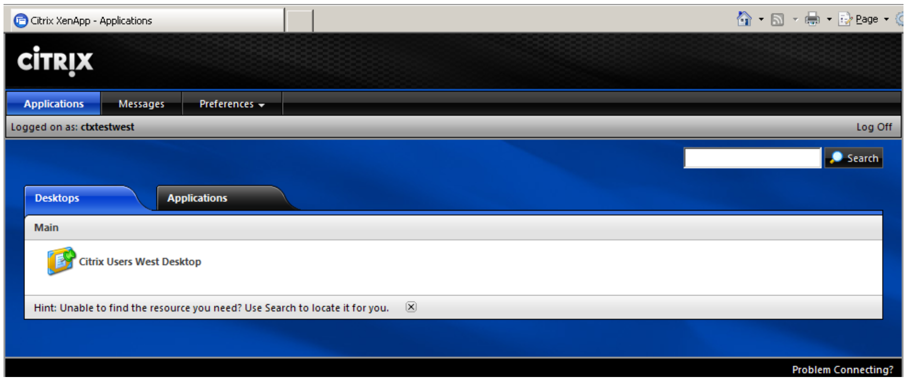
While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

Figure 7: Security Warning window for install

6. Click **Run**.

7. When the system notifies you that the installation completed successfully, click **OK**.

   The system then displays the Desktop tab on the Applications window, and an icon for the Citrix Users Desktop, either East or West.



Logged on as: ctxtestwest

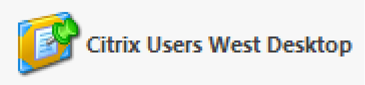
Hint: Unable to find the resource you need? Use Search to locate it for you.

Figure 8: Desktops tab on the Citrix Applications window

At this point, you can continue with the steps in the next section to launch a desktop session.

2.3. Launching a Desktop Session

1. Click the Citrix Users Desktop icon (East or West, as appropriate).



The system displays the standard IHS privacy warning.

> **NOTE**: If instead of the privacy warning, the system displays a **Logging in …** message, the problem may be that your D1 password contains a Citrix reserved character (**+** or **&**). If so, you need to change your password to one without those characters before you can proceed.

2. Click **OK**.

The system now loads your profile. In some cases this can take 7–10 seconds or more.

It then displays the Citrix Users Desktop for your geographical zone (i.e., East or West).

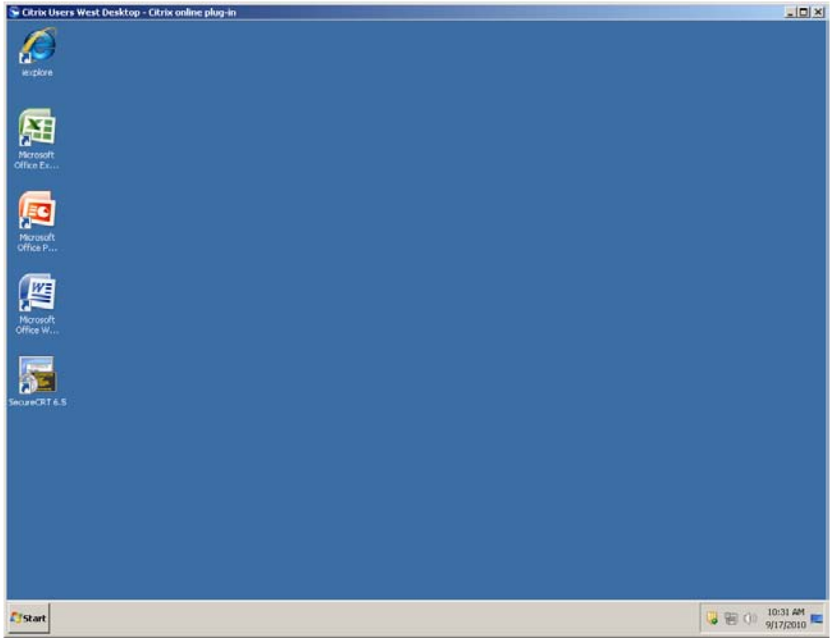


Figure 9: Citrix Users Desktop with application icons

3. At this point, you can do the following:

a. To open an application, double-click its icon.

> **NOTE**: Applications not on the desktop may be available from the **Start** menu.

b. To access your network drives, open the **Start** menu and select **Computer**. Then navigate to the desired drive.

c. To log off and end the VPN session, open the **Start** men and select **Log off**.

> **IMPORTANT**: Be sure to perform the Log Off step before closing the browser window. If you do not, the session may persist in a “hung” state, and you will not be able to establish a new VPN session. For assistance, contact your local Help Desk.

2.3.1. Where Are My Files?

All of your files are located on the network share and network drives assigned to you as part of your network account and profile. (For assistance, contact your System Administrator.)

To locate your files, access your network drives, open the **Start** menu and select **Computer**. Then navigate to the desired network drive.

You will be presented with an Explorer window similar to the one below.

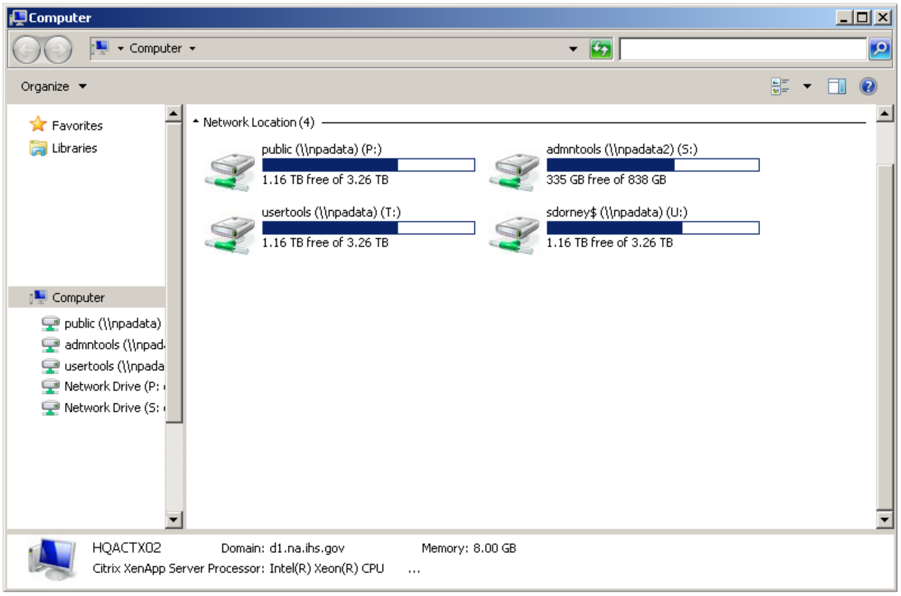


Figure 10: Explorer window showing network drives

2.4. Launching an RDP Session

To be able to launch a Remote Desktop Protocol (RDP) session, you must first work with your local Area/facility IT staff to identify the servers and workstations you need to access via RDP.

Then, you can use these steps to launch an RDP session within the VPN after you have completed the VPN login and authentication steps.

1. Access the Desktops tab of the Citrix XenApp – Applications screen.

   This is the screen that displays the Citrix Users Desktop icon (either East or West.)

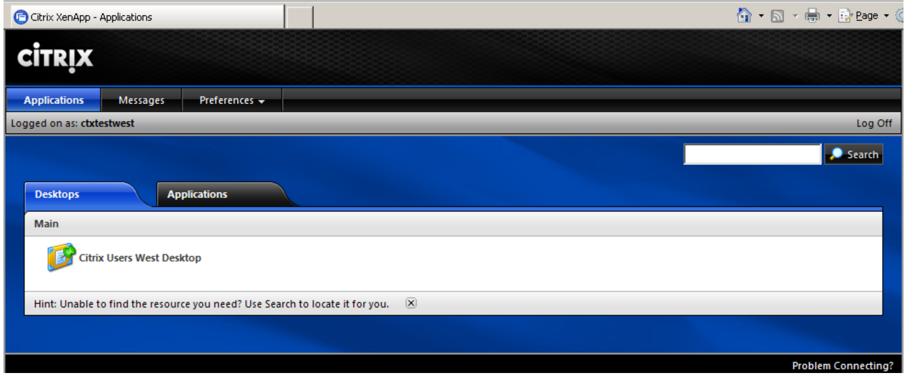
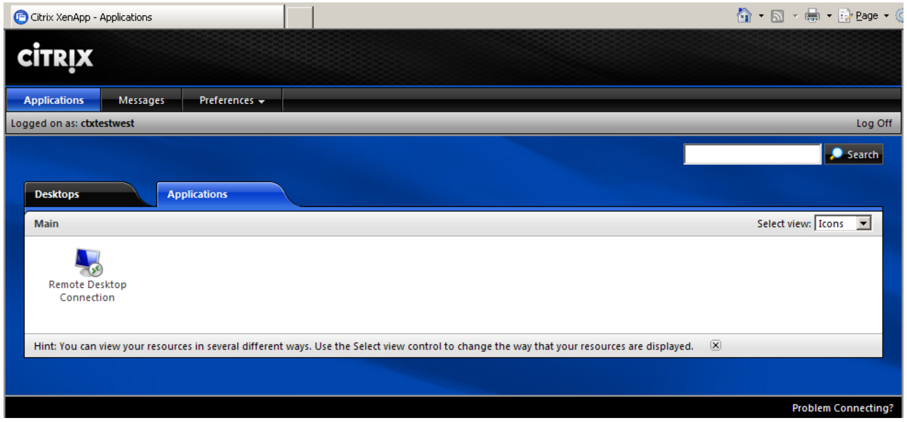

Citrix XenApp - Applications
Page
CITRIX
Applications
Messages
Preferences
Logged on as: ctxtestwest
Log Off
Search
Desktops
Applications
Main
Citrix Users West Desktop
Hint: Unable to find the resource you need? Use Search to locate it for you.
Problem Connecting?

Figure 11: Citrix XenApp – Desktops tab

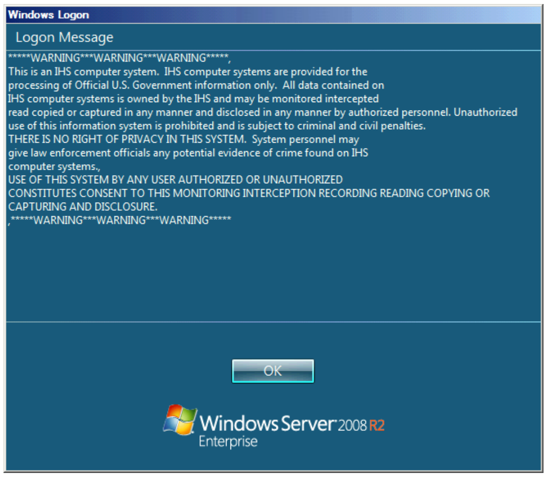
2. Switch from the Desktops tab to the Applications tab.



Hint: You can view your resources in several different ways. Use the Select view control to change the way that your resources are displayed.

Figure 12: Applications tab showing Remote Desktop Connection icon

3. Click the **Remote Desktop Connection** icon to display the Windows Logon screen..

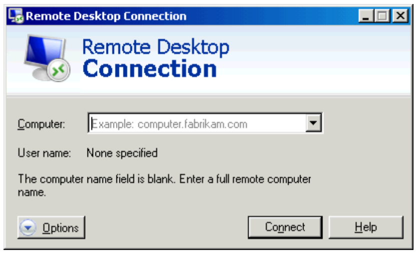


Logon Message

*****WARNING***WARNING***WARNING*****,
This is an IHS computer system. IHS computer systems are provided for the
processing of Official U.S. Government information only. All data contained on
IHS computer systems is owned by the IHS and may be monitored intercepted
read copied or captured in any manner and disclosed in any manner by authorized personnel. Unauthorized
use of this information system is prohibited and is subject to criminal and civil penalties.
THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may
give law enforcement officials any potential evidence of crime found on IHS
computer systems.,
USE OF THIS SYSTEM BY ANY USER AUTHORIZED OR UNAUTHORIZED
CONSTITUTES CONSENT TO THIS MONITORING INTERCEPTION RECORDING READING COPYING OR
CAPTURING AND DISCLOSURE.
,*****WARNING***WARNING***WARNING*****

Figure 13: Windows Logon screen

4. Click **OK** to display the Remote Desktop Connection window.



Computer: Example: computer.fabrikam.com

User name: None specified

The computer name field is blank. Enter a full remote computer name.

Figure 14: Remote Desktop Connection window

5. Enter the name of the machine you want to connect to, and click **Connect**.

The system then displays the desktop of the remote machine you specified above.

2.5. Logging Off and Disconnecting

Logging off is very similar to the way you would log out of a PC. Use the following steps to log off and disconnect from the VPN.

1. On your Citrix Users Desktop, open the **Start** menu, and then click **Log off**.

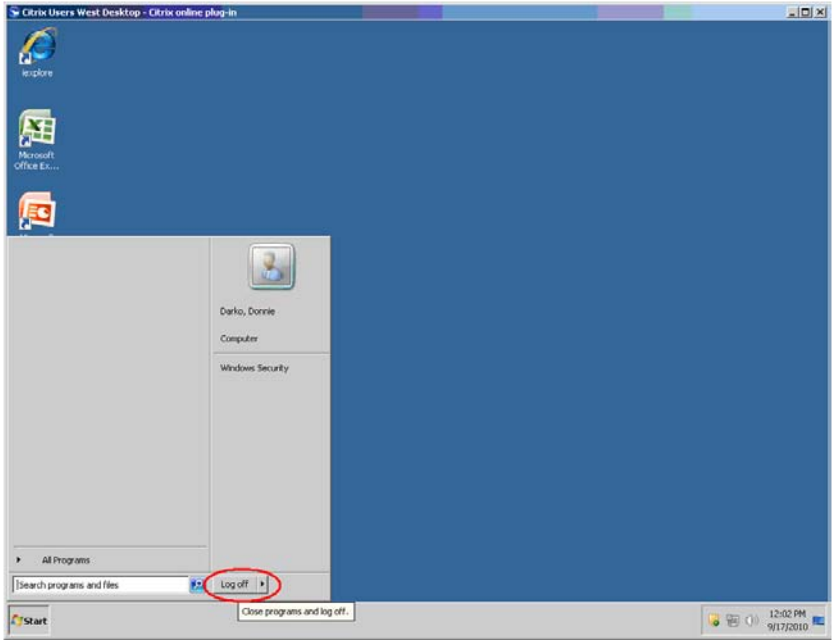
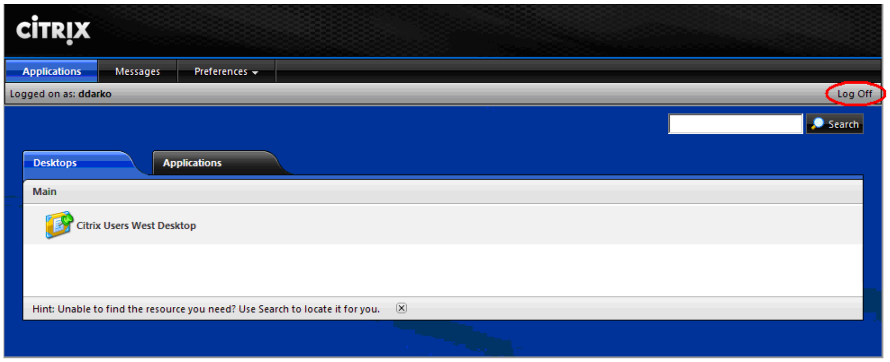


Figure 15: Start menu showing Log Off button.

The system will log you off of the Citrix session, and redirect you to the Desktops tab of the Citrix Web Interface screen.

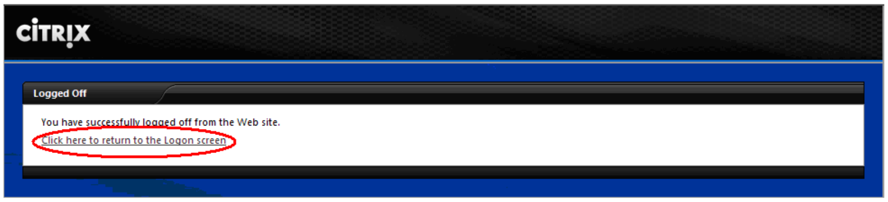


Logged on as: ddarko

Hint: Unable to find the resource you need? Use Search to locate it for you.

Figure 16: Citrix Desktops tab with Log Off button

2. Click **Log Off** in the upper right hand corner to log off.



Logged Off

You have successfully logged off from the Web site.

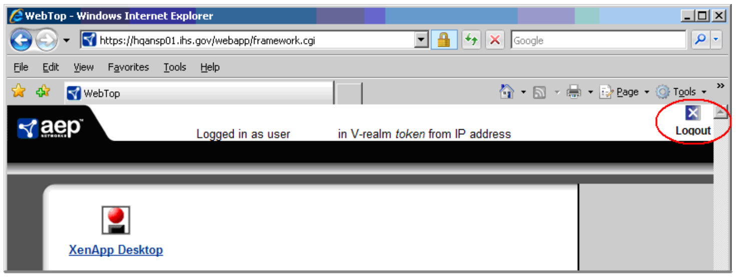
Click here to return to the Logon screen

Figure 17: Prompt confirming logoff

3. To continue exiting your VPN session, close this Internet Explorer window.

> **NOTE**: You can also log back in by clicking the link, **Click here to return to the Logon screen**.

4. On the AEP NSP page, click **Logout**.



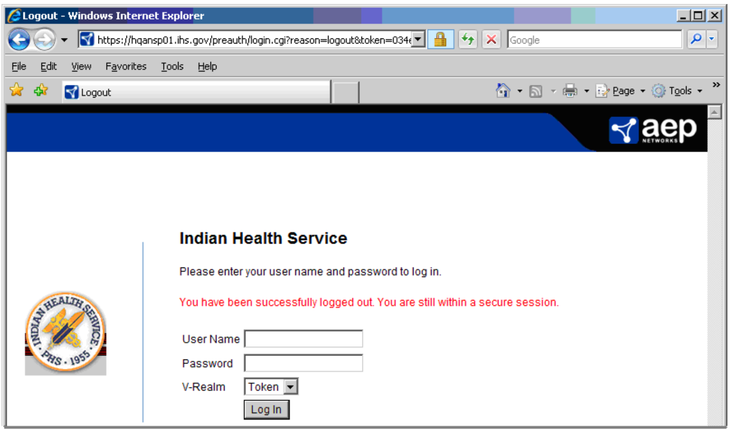
https://hqansp01.ihs.gov/webapp/framework.cgi

Logged in as user in V-realm *token* from IP address

WebTop - Windows Internet Explorer
File Edit View Favorites Tools Help
WebTop
Page Tools
aep
Logout
XenApp Desktop

Figure 18: AEP NSP page with Logout button

The system will automatically redirect you to the login screen with a status message showing that you have successfully logged out.



https://hqansp01.ihs.gov/preauth/login.cgi?reason=logout&token=034

Indian Health Service

Please enter your user name and password to log in.

You have been successfully logged out. You are still within a secure session.

User Name

Password

V-Realm Token

Log In

Logout - Windows Internet Explorer
File Edit View Favorites Tools Help
Logout
Page Tools
aep
INDIAN HEALTH SERVICE · PHS · 1955

Figure 19: Login screen with logout confirmation

5. Close the Internet Explorer window to disconnect fully.

3. Appendixes

3.1. VPN Limitations

Computer management tools and various Control Panel utilities that are typically available on a PC will not be available from within your VPN session. Because any administrative modification to the Citrix server would affect everyone else on that server, OIT has secured the system so that only system administrators have access to these tools.

Access to the following has been disabled:

- Modifying Desktop wallpaper
- CD and DVD Media Information Retrieval
- CD Burning features
- Context menus on the taskbar
- Music File Media Information Retrieval
- Network Connections from Start menu
- Registry editing tools
- Shutdown, Restart, Sleep, Hibernate settings
- Task Manger
- Taskbar and Start Menu settings
- Command prompt
- The following tabs: Hardware, Network, Privacy, Security
- Music icon from the Start Menu
- My Documents icon
- Network icon from Start Menu
- Pictures icon from Start Menu
- Use of all Windows Update features
- Adjustment of desktop toolbars
- Auto connect client drives
- Balloon Tips on Start Menu items
- Client drive redirection
- Client fixed drives
- Client floppy drives
- Client LPT port redirection
- Client microphone redirection
- Client optical drives
- Client removable drives

- Client USB device redirection
- Client USB Plug and Play device redirection

Additionally, the following Control Panel items have been hidden:

- Add hardware
- Add or Remove Programs
- Administrative Tools
- Automatic Updates
- Date and Time
- Game Controllers
- Java Plug-In
- Licensing
- Network Connections
- Phone and Modem options
- Power options
- Printers and Faxes
- Scanners and Cameras
- Scheduled Tasks
- Speech
- Stored User Names and Passwords
- Symantec Live Update
- System

3.2. PhoneFactor Security Questions

Before an OIT technician can assist you when you have problems accessing the IHS VPN, he or she must validate your identity. For PhoneFactor, OIT uses a set of four user-defined questions for this purpose, much like many other secure sites on the Web.

> **NOTE**: If you have not defined your security questions, you will still be able to log in to the VPN. However, the OIT Help Desk will not be able to assist you if you encounter a problem.

Use these steps to define your PhoneFactor security questions.

1. Log in to the IHS network (either directly or through the VPN) using your D1 username and password. (See Section 2.1.)

> **NOTE**: You must be logged in to the D1 domain before you can access the PhoneFactor Portal.

2. Open a web browser and go to the following site: https://npad1step/phonefactor

   The system displays the PhoneFactor User Log In page.

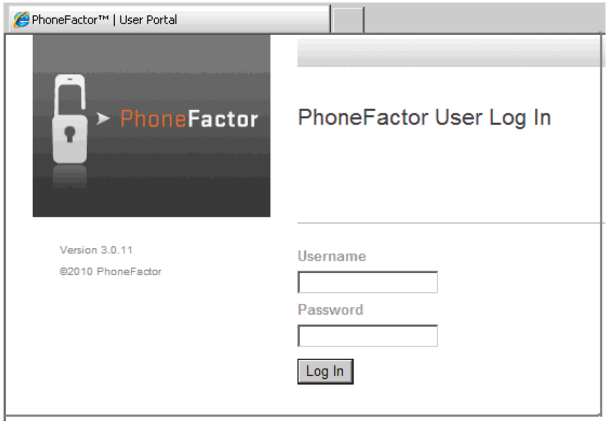


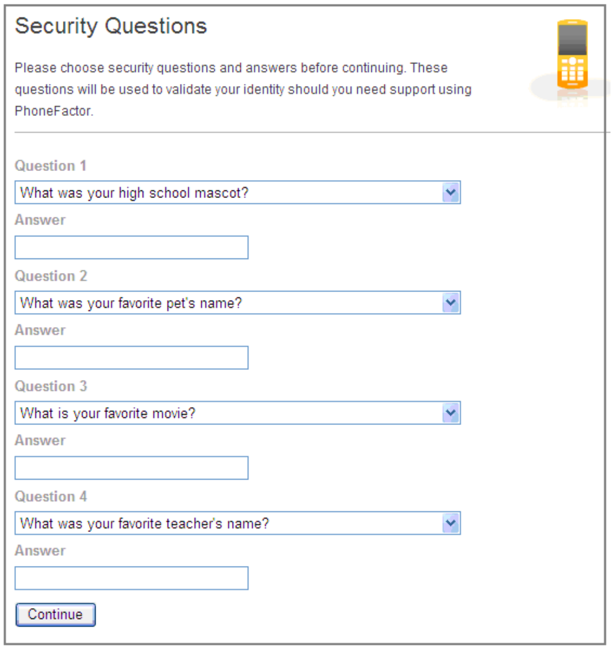
Figure 20: PhoneFactor User Log In page

3. Enter your D1 **Username** and **Password** in the respective fields and click **Log In**.

   At this point, PhoneFactor calls your designated phone number.

4. Answer your phone and verify that it is PhoneFactor; then press the **#** key on the phone.

   The system displays the Security Questions page.



Security Questions

Please choose security questions and answers before continuing. These questions will be used to validate your identity should you need support using PhoneFactor.

Question 1

What was your high school mascot?

Answer

Question 2

What was your favorite pet's name?

Answer

Question 3

What is your favorite movie?

Answer

Question 4

What was your favorite teacher's name?

Answer

Figure 21: Security Questions page

5. For each question, select a question from the drop-down list and type an answer.

   Be sure you define answers you can easily remember!

6. Click **Continue** to open the PhoneFactor Welcome page.

7. Click **Log Out** to exit.

If you ever want to change your questions and/or answers, you can repeat these steps. Remember, however, that you must be working within the IHS network to be able to access the Portal.