
Indian Health Service

**The Federal Health Program for American Indians and Alaska Natives**

# IHS User Guide for Virtual Private Network

Version 4.3
September 2020

IHS Office of Information Technology
Albuquerque, New Mexico

# Document Information

## Audience

This manual is intended for users of the RDP/RDS Desktop-based IHS Virtual Private Network (VPN) that has been in place since 2010.

## Related Documents

IHS Support Guide for Virtual Private Network – Provides guidance for the IHS IT Service Desk, the Network Operations and Security Center (NOSC) and other agency IT support staff on how to support the RDP/RDS Desktop-based VPN Remote Access to IHS resources.

## Revision History

| VERSION | DATE | BY | DESCRIPTION OF CHANGES |
|---|---|---|---|
| Version 1.0 | 9/30/2010 | J. Berry | First published version. |
| Version 1.1 | 11/16/2010 | J. Berry | Added instructions for PhoneFactor security questions in Section 3.2. |
| Version 1.2 | 2/4/2011 | J. Berry | Added warning about not using plus sign (+) and ampersand (&) in D1 passwords. |
| Version 1.3 | 7/5/2011 | J. Berry | Added clarifications about the need to log in to the D1 domain before defining the PhoneFactor security questions in Section 3.2. |
| Version 2.0 | 10/24/2012 | J. Berry | Added section covering logging in to the VPN using a PIV Card and using the VPN to access the HHS applications. |
| Version 2.1 | 3/25/2015 | J. Berry | Performed annual review. |
| Version 3.0 | 7/6/2018 | J. Berry | Updated throughout to reflect change to NetConnect/RDP/RDS Desktop-based VPN. |
| Version 4.0 | 9/11/2019 | K. Lewis | Consolidated DITO SOP-14-01 and support guide into single document and updated for new F5 VPN appliance changes. |
| Version 4.1 | 3/30/2020 | J. Schenk | Updated various screenshots for anonymity. |
| Version 4.2 | 7/16/2020 | J. Schenk | Updated OIT Contact Information. |
| Version 4.3 | 9/23/2020 | J. Schenk | Added Section 6: Apple Device Support. |

## OIT Contact Information

If you have any questions or comments regarding this document or the installation process it describes, please contact the IHS IT Service Desk at IHS:

**Phone**: 1-888-830-728

**Web:** IHS IT Service Desk

**Self Service:** IHS IT Support

**Email:** itsupport@ihs.gov

# Table of Contents

# 1. Introduction

The Indian Health Service (IHS) Office of Information Technology (OIT) maintains and supports a secure Remote Access Virtual Private Network (VPN) solution in order to bring IHS into compliance with Federal and Departmental mandates and requirements.

VPN Access is offered for all authorized federal, contract, and tribal employees who identify a business need to access IHS resources outside of the IHSNet, either during or after regular work hours.

This document provides background on the RDP/RDS Desktop/F5-based VPN. It also walks you as the end user through the login process and the steps required to launch a Remote Desktop Protocol (RDP) application in order to access the applications and services required to support your business needs.

Additional information regarding the access policies and security surrounding the use of VPN within IHS can be found within the Indian Health Manual, Chapter 8, Part 8 and Chapter 21, Part 8.

## 1.1. Filtering Components

The VPN enables you to access your network drives and also to use the approved standard IHS applications without installing the software on your workstation. This could include (and is not limited to) the following applications:

- Microsoft Office suite
- Adobe Acrobat
- Secure Telnet Client
- Access to internal web sites and web based applications
- Access to additional RDP or RDS servers with additional site specific applications

The web-based VPN acts as a "window" to Area/Facility Remote Desktop servers. These servers host the set of common Health IT and other local applications.

### 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/multifactor authentication (MFA)**—something you know (e.g., a password) and something you have (like a phone or a smart card)—to verify that you are who you say you are. Two-factor authentication is required in order to provide the additional security mandated for the IHS VPN and network access.

IHS supports three 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

- The **PIV V-Realm** requires the use of a Personal Identity Verification (PIV) card. When you insert your PIV card into the card reader, the system automatically transmits identity verification certificates as part of the authentication process.

  PIV card access will be required for numerous internal Department of Health and Human Services (HHS) applications such as the Integrated Time and Attendance System (ITAS), GovTrip, MyPay, eOPF, HHS Learning Portal, etc. Instructions for accessing the Identity and Access Management (IAM) website via VPN can be found in Section 3.1

> **NOTE:** You can log in to the VPN using a PIV card only from a workstation or laptop equipped with the requisite card reader and software. For assistance, contact your local Service Desk.

After authentication, you are either presented with a web top access to the available list of applications or RDS/RDP locations or are provided with tunnel access based on established client requirements. See Section 2.1 for login instructions.

### 1.1.2. VPN Log In Limitations

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

- VPN logon is only authorized for valid user access accounts and not for Administrative (a_admin) accounts. Admin accounts can be used only after a valid VPN user account has completed a successful logon.
- Access to the RDS/RDP server 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. Users are discouraged from saving documents on their 'desktops' while in a 'RDS Desktop' session. If the user's profile is deleted or corrupted for any reason, they will lose any data that is saved to the desktop.
- Because the RDP/RDS server is a shared system used by several people at once, you will not be able to install any applications yourself. Only the server application admins will be able to install or modify applications.

## 1.2. Obtaining VPN Access

To obtain access to the VPN, you should discuss your business needs with your supervisor. This justification should be referenced as part of the access request to be submitted by your supervisor/COR. 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 4.2 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.
- **PIV Card** – If you choose this, you must have both a PIV card and a government-issued computer (workstation or laptop) with the requisite card reader and software.

Next, your supervisor enters the request and related information into the electronic IT Access Control (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 MFA, the physical token will be shipped to you.

## 1.3. About VPN Support

Technical Support for the IHS VPN is handled similarly to most of the IHS OIT services. 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 IHS IT Service Desk (see below).
- For after-hours support, users should call the IHS IT Service Desk phone number (see below). This number is forwarded to the Network Operations and Support Center (NOSC), which provides after-hours support.

See also the IHS OIT Service Catalog for details about the Service Level Agreements (SLAs) for the IHS VPN.

## 1.4. Contact Information

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

| | |
|---|---|
| **Phone**: | 1-888-830-728 |
| **Web:** | IHS IT Service Desk |
| **Self Service:** | IHS IT Support |
| **Email:** | itsupport@ihs.gov |

# 2. Use VPN

The following sections 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 your approved two-factor authentication device available:

- Entrust token
- Telephone that you designated for PhoneFactor authentication
- PIV Card, which should be inserted into the smart card reader

> **NOTE:** A mandatory timeout is configured for inactivity within the RDP/RDS-based VPN per IHS and HHS Security policies. Each VPN user will be logged out of the VPN when the inactivity standards are met and in alignment with HHS security policies. To reconnect, repeat the log in process outlined in Section 2.1.

## 2.1. Log In to VPN

1. Open your web browser and go to the VPN Login page (https://vpn.remote.ihs.gov).

*The system displays a login warning page.*

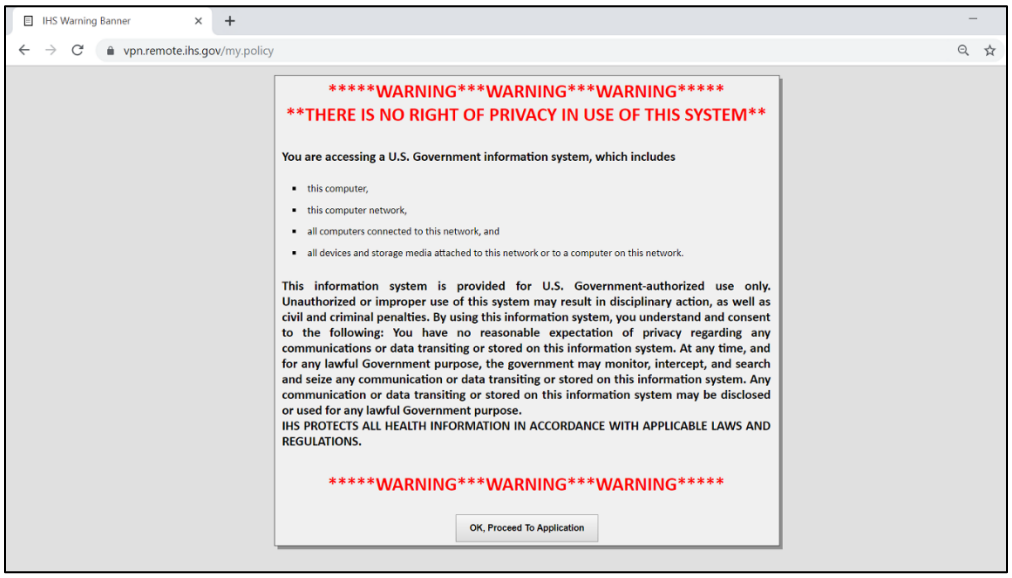


Figure 2: VPN Login page

2. Click **Ok, Proceed To Application** to accept the warning and continue to the login page.

*The system displays the VPN Login page.*

3. Enter your IHS network (D1) **Username** and **Password**.
4. From the **V-Realm** drop-down list, select the desired method of two-factor authentication:
   - If you have been assigned an Entrust token, select **Token**.

- If you are using your phone for authentication, select **Phone**.
- If you are using your PIV Card for authentication, select **PIV**.

5. Click **Next** to start the two-factor authentication process.

Proceed to the appropriate subsection below according to your authentication method.

### 2.1.1. Authenticate with Entrust

If you selected Entrust (Token) authentication, the system displays the following prompt:

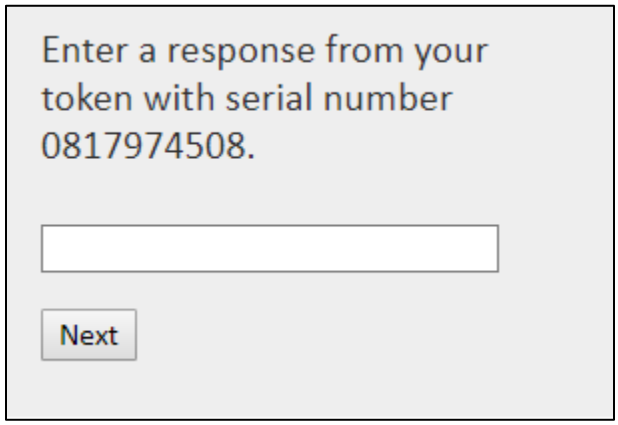


Figure 3: Entrust authentication field

Continue with the following steps to complete the login process.

1. On the Entrust token, press the button that generates the authentication number.
2. When it is displayed, type the eight-digit authentication number into the field shown in Figure 3 above.
3. Click **Next**.

*The system displays the VPN Webtop page containing the RDP/RDS Desktop applications approved for your use. Continue to Section 2.3 to set up the Remote Desktop environment.*

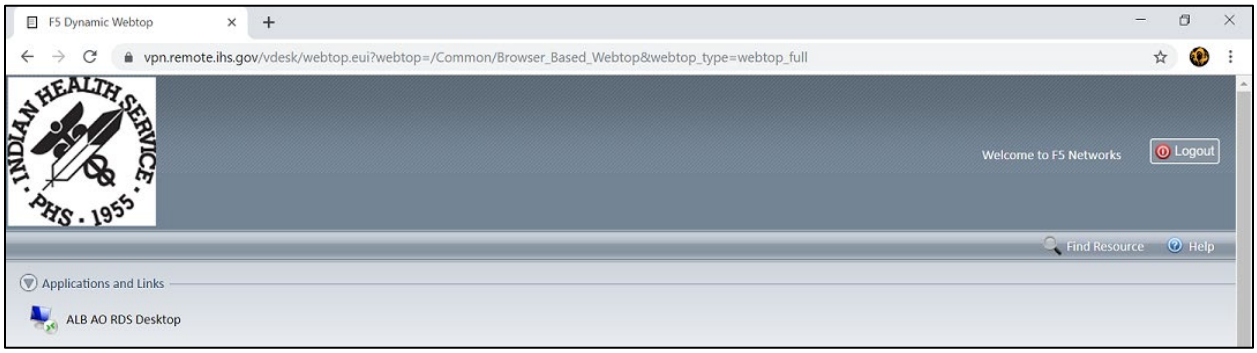


Figure 4: VPN Webtop page showing the RDP/RDS Desktop applications

### 2.1.2. Authenticate with PhoneFactor

If you selected PhoneFactor authentication, the system calls the designated phone after you click **Next** (Step 5 in Section 2.1). Continue with the following steps to complete the login process.

1. Answer the phone.
2. Press the pound key (#) on the phone when directed, and then hang up.

   *The system displays the VPN Webtop page containing the RDP/RDS Desktop applications approved for your use. Continue to Section 2.3 to set up the Remote Desktop environment.*

> **NOTE:** Be sure to log in to the PhoneFactor Portal to define your security questions. If you have not done so, the IHS IT Service Desk will not be able to validate your identity when you call them for assistance. See Section 4.2.

### 2.1.3. Authenticate with PIV Card

If you chose PIV card authentication, the system displays a list of digital certificates.

> **NOTE:** You can authenticate with an authorized user PIV card only on a government-furnished workstation or laptop that is equipped with the requisite PIV card reader and software. There are also some other technical requirements that can affect certain workstations/laptops. If you run into problems authenticating with a PIV card, contact your local Area Help Desk.

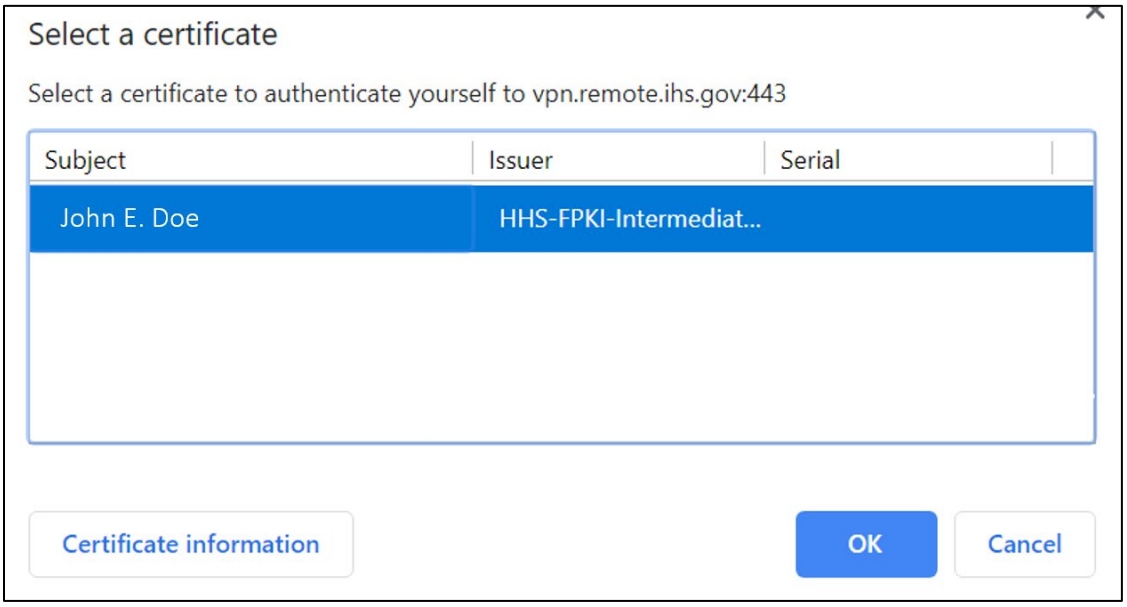


Figure 5: Select a Certificate window

Continue with the following steps to complete the login process.

1. Select the top "–A" certificate.

2. Click OK.

*The system displays the Windows Security PIN window.*

3. Type the PIN number associated with your user PIV card.

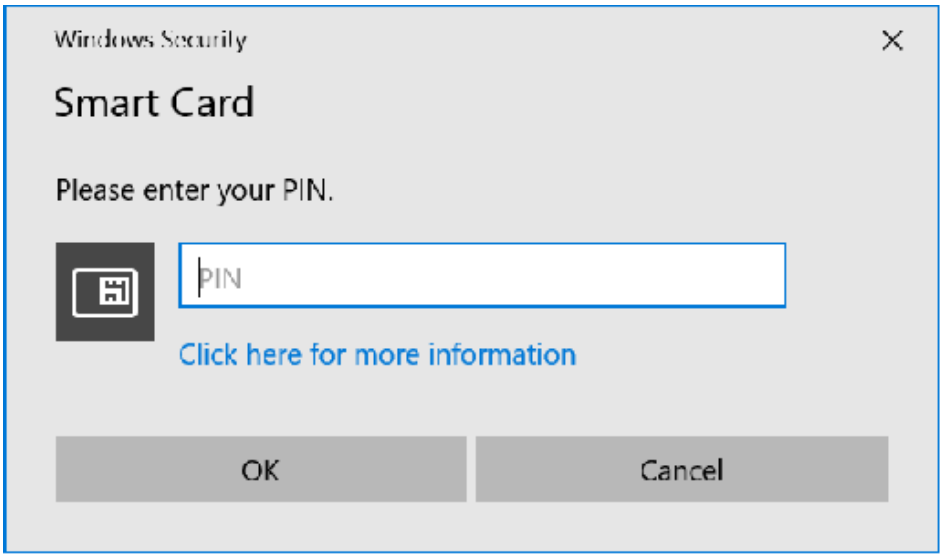


Figure 6: Windows Security login window for PIN number

4. Click **OK**.

*The system displays the VPN Webtop page containing the RDP/RDS Desktop applications approved for your use.*

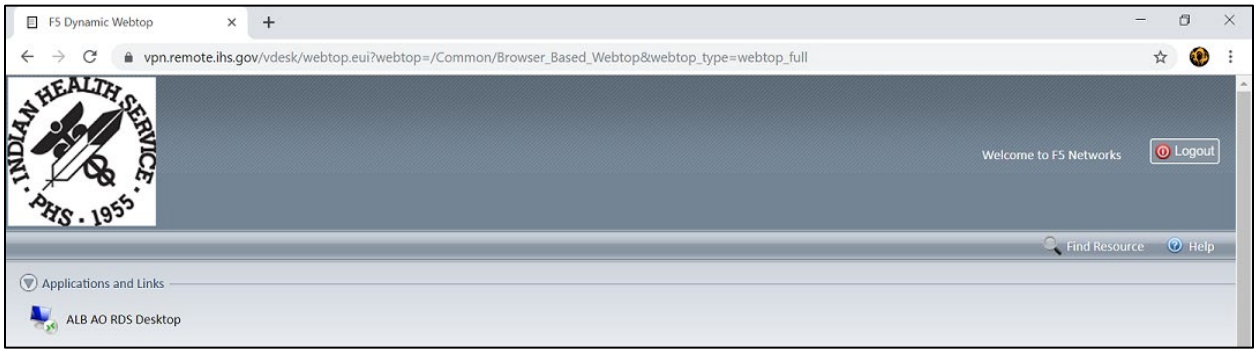


Figure 7: IHS VPN WebTop

## 2.2. Connect to the Remote Desktop Environment

The first time you connect to the Remote Desktop environment, the RDP application will be downloaded to your system. No additional setup is required.

**NOTE:** This download does not require administrative privileges.

1. Click **RDP/RDS Desktop** applications to display the Remote Desktop login page containing the standard federal government privacy warning.

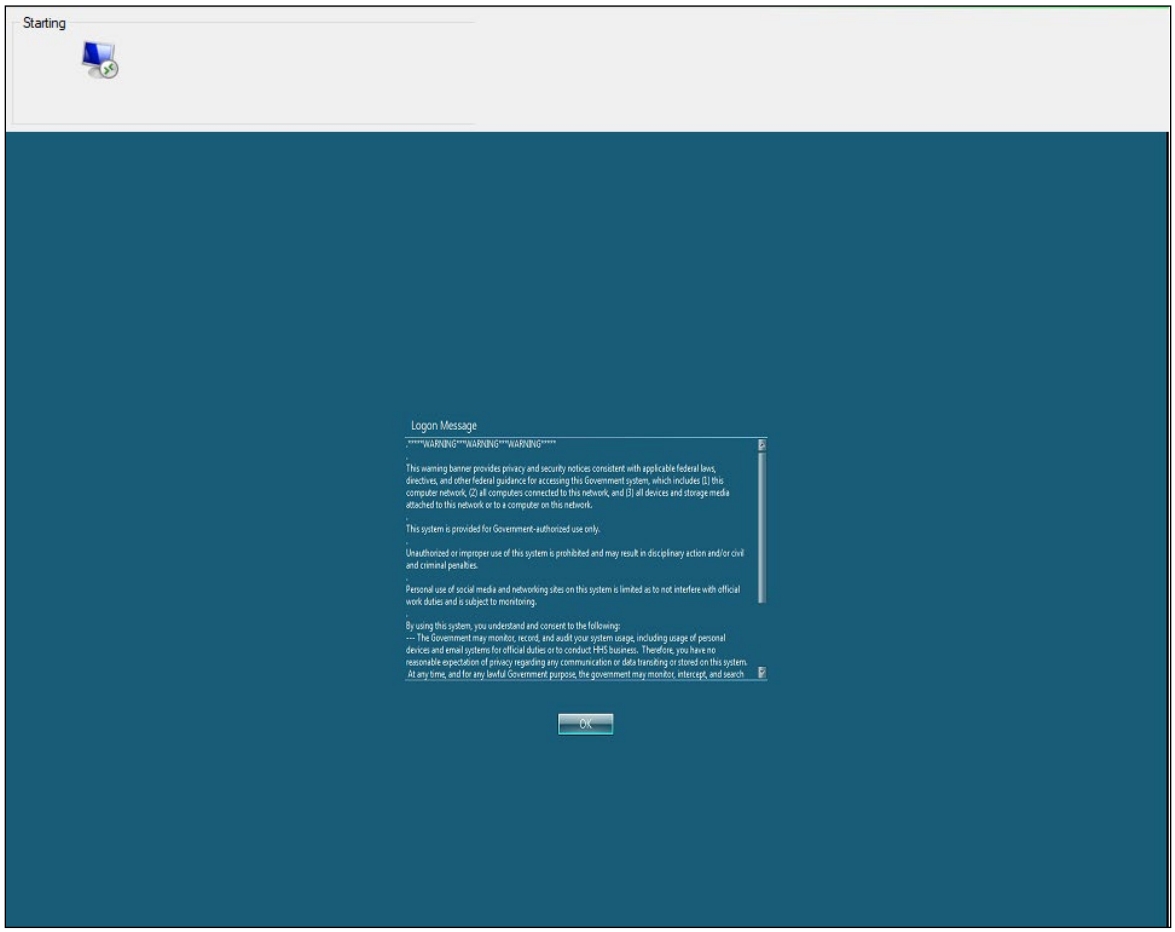


Figure 8: Federal government privacy warning

2. Click **OK** to continue to the server login window.

## 2.3. Launch a Remote Desktop Session

1. Click the Area/Facility Remote Desktop icon.

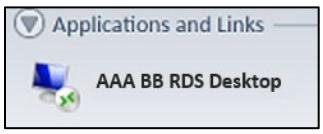


Figure 9: Remote Desktop icon

*The system displays the standard IHS privacy warning window.*

2. Click **OK**.

*The system loads your profile. In some cases, this may take 7-10 seconds or more. After your profile loads, the system displays the Remote Desktop for your Area/Facility.*


Figure 10: Remote 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** menu and select **Log off**.

**NOTE:** 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. Locate Your 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 local System Administrator.) Here's how to locate your files and access your network drives:

1. Open the **Start** menu, and then select **Computer**.

*The system presents an Explorer window similar to the one below.*

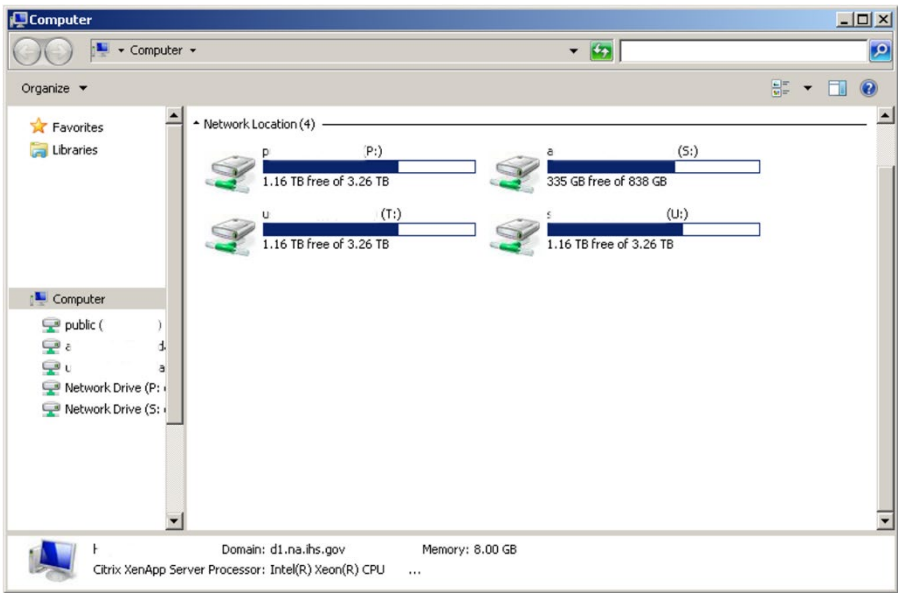


Figure 11: Explorer window showing network drives

2. Navigate to the desired network drive.

## 2.4. Launch an RDP Session

Before you can use an RDP application, you must 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. Click on the RDP application.


Figure 12: RDP Application icon

2. Type the name of the machine to which you want to connect.

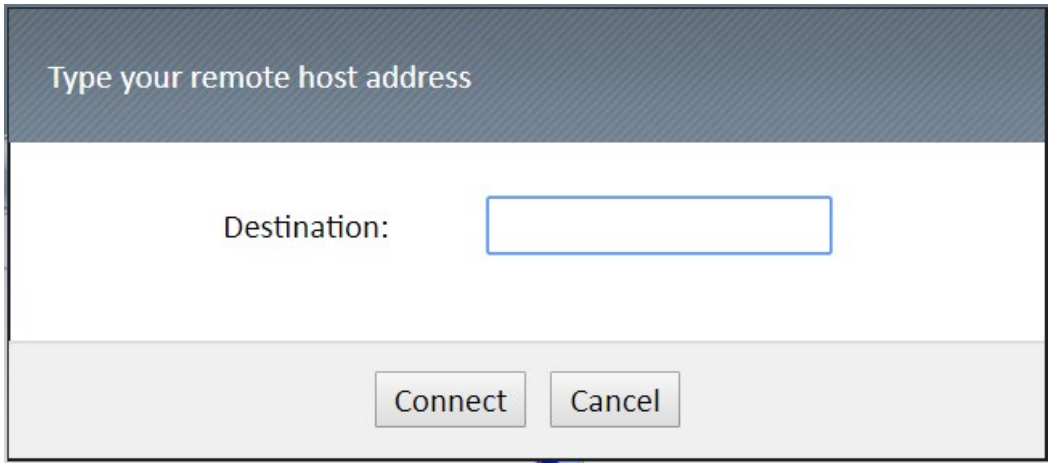


Figure 13: Remote Desktop Connection window

3. Click **Connect.**

*The system displays the Remote Desktop Connection Publisher Verification window.*

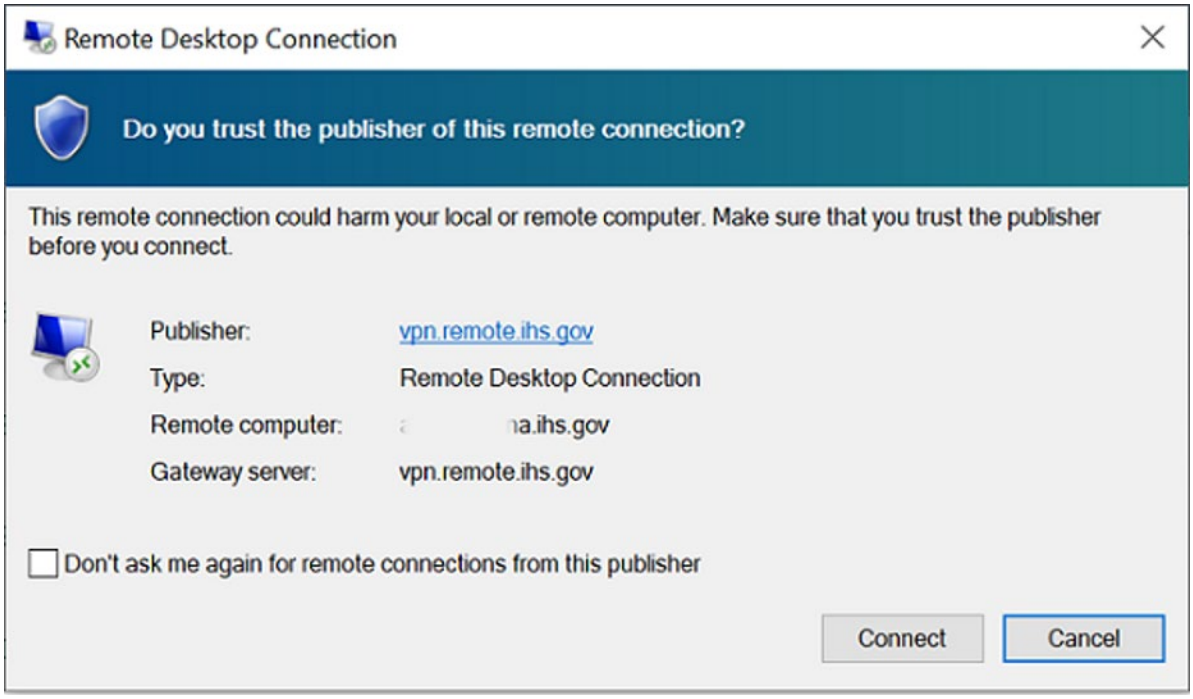


Figure 14: Remote Desktop Connection Publisher Verification window

4. Click **Connect.**

*The system displays the Remote Desktop Connection status indicator window.*

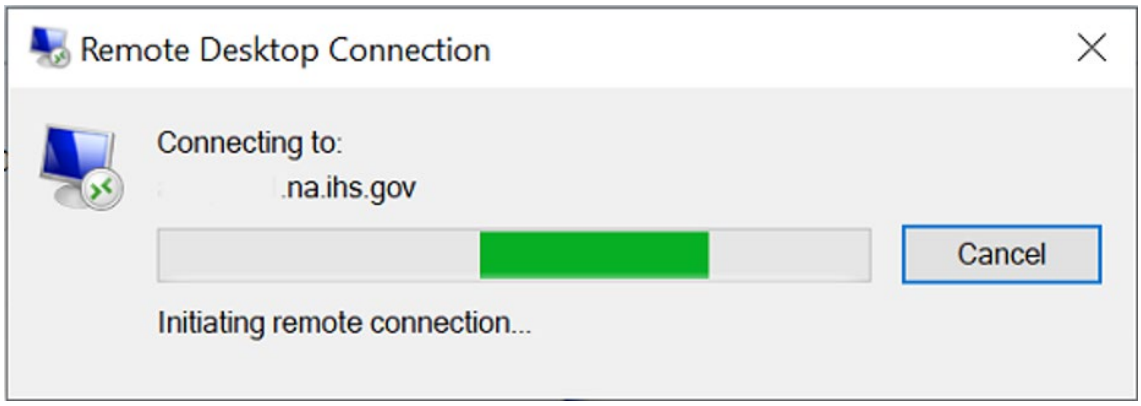


Figure 15: Remote Desktop Connection status indicator window

*The system displays the Windows Security credentials window.*

5. Enter your d1 user name and password using the following format: d1\<*username*>.

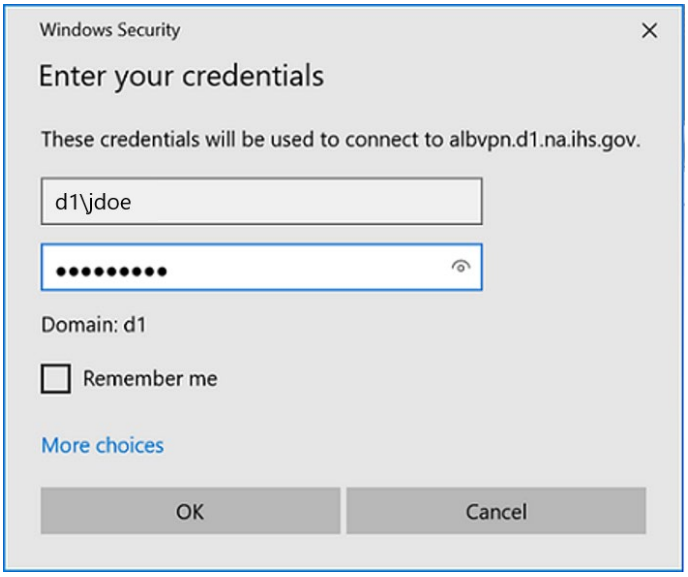


Figure 16: Windows Security credentials window

6. Click **OK**.

*The system displays the Remote Desktop Connection certificate warning window.*

7. Click **Yes**.


Figure 17: Remote Desktop Connection certificate warning window

## 2.5. Log Out and Disconnect from VPN

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

> **NOTE:** A mandatory timeout is configured for inactivity within the RDP/RDS-based VPN per IHS and HHS Security policies. Each VPN user will be logged out of the VPN when the inactivity standards are met and in alignment with HHS security policies. To reconnect, repeat the log in process outlined in Section 2.1

1. On your Remote Desktop, open the **Start** menu, and then click **Log Off**.

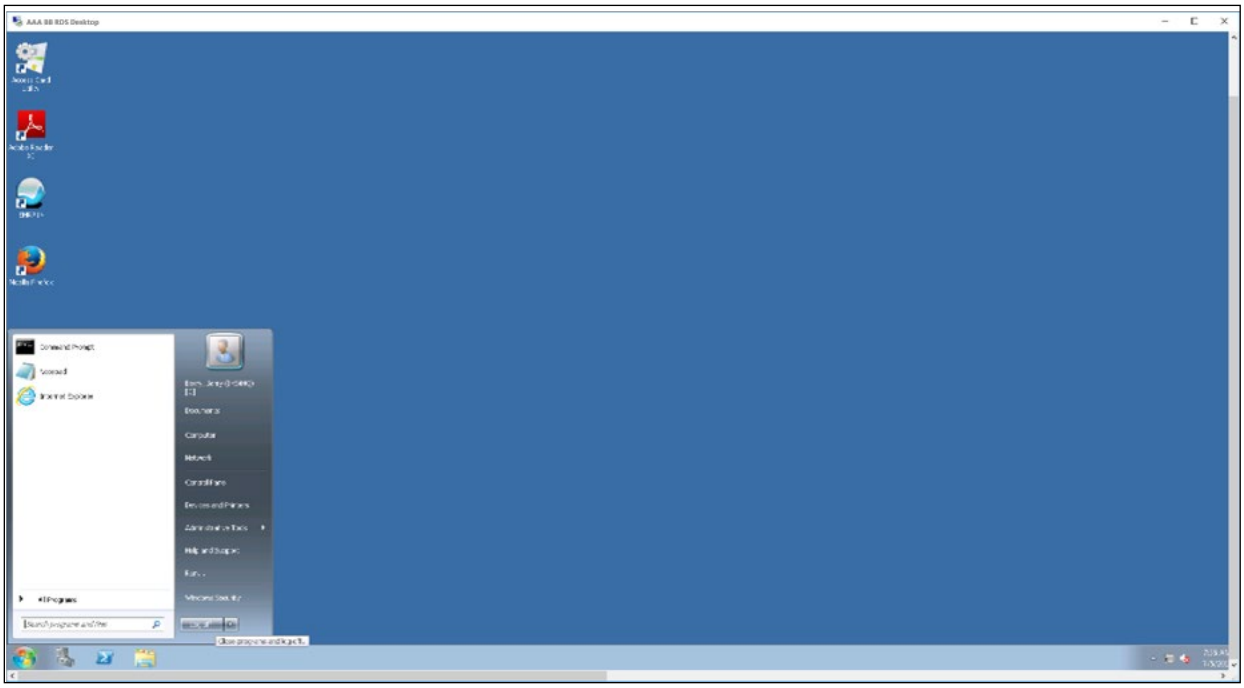

Figure 18: Start menu showing Log Off button

*The system will log you off of the Remote Desktop session.*

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

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

3. On the VPN Webtop page, click **Logout** on the upper-right corner of the page.

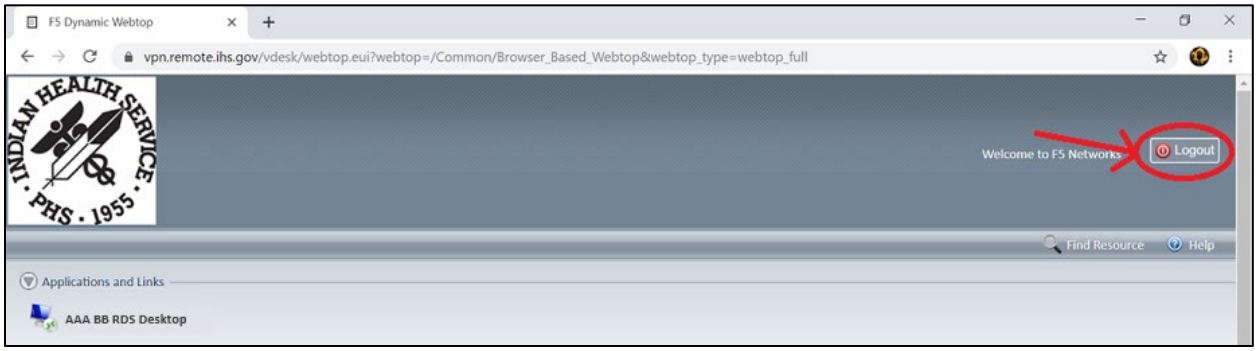


Figure 19: VPN Webtop page with Logout button

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

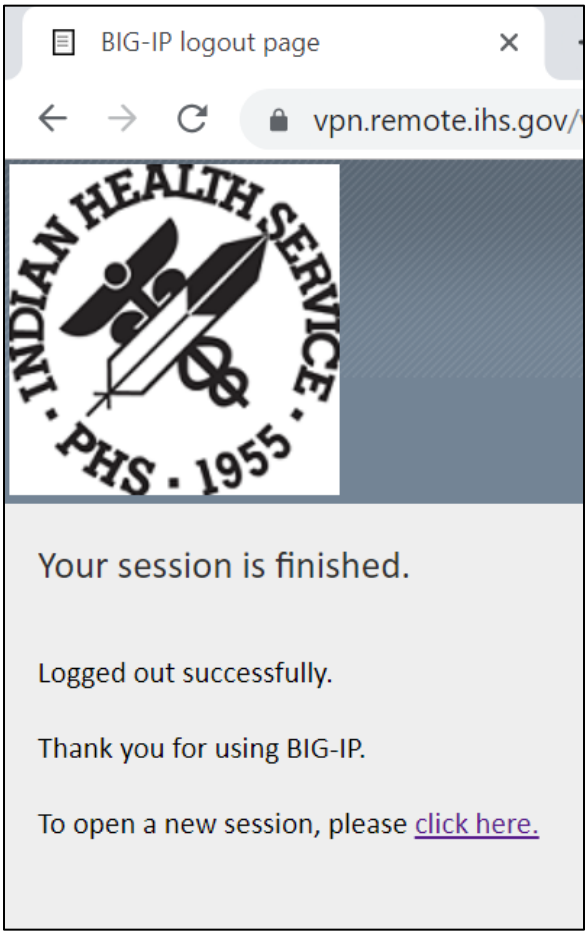


Figure 20: Login screen showing logout confirmation

# 3. Use VPN to Access PIV-Enabled HHS Applications

Many HHS applications now require the use of a PIV card to access and request information. These include ITAS, myPay, eOPF, HHS Learning Portal, GovTrip, etc. When using the IHS VPN to access these websites, you must meet the following requirements:

- Use government-furnished equipment (GFE) with a working PIV-card reader and current ActivClient software.
- Use a PIV card with current (not expired) certificates.
- Use a PIV card that work within the IHS network on the current GFE.

> **NOTE:** You do not need to use the PIV V-Realm for logging into VPN in order to access HHS applications that require the PIV card for access. Any other approved two-factor authentication can be used. However, your PIV card must be inserted into the card reader prior to accessing the websites for HHS.

## 3.1. Access IAM@HHS.GOV

1. Open a web browser and navigate to the IAM@HHS website (https://iam.hhs.gov/opensso/SimpleLogin.jsp).

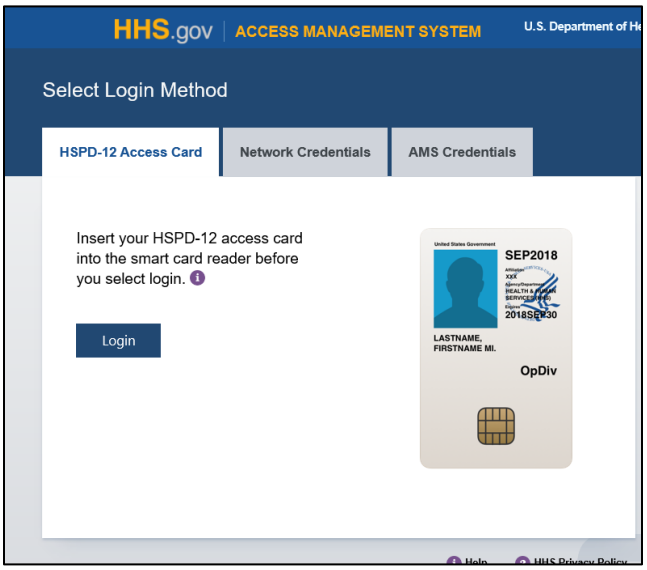


Figure 21: Login page for Identity and Access Management

2. Click **Login**.

*The system displays the Government Warning window.*

3. Click **Agree**.

*The system displays the Select a Certificate window.*

4. Select the top certificate in the list, and then click **OK**.

*The system displays the Smart Card PIN window.*

5. Type your PIV-card PIN number.
6. Click **OK**.

*The system displays the AMS Home Page with a list of options, based on your access rights.*

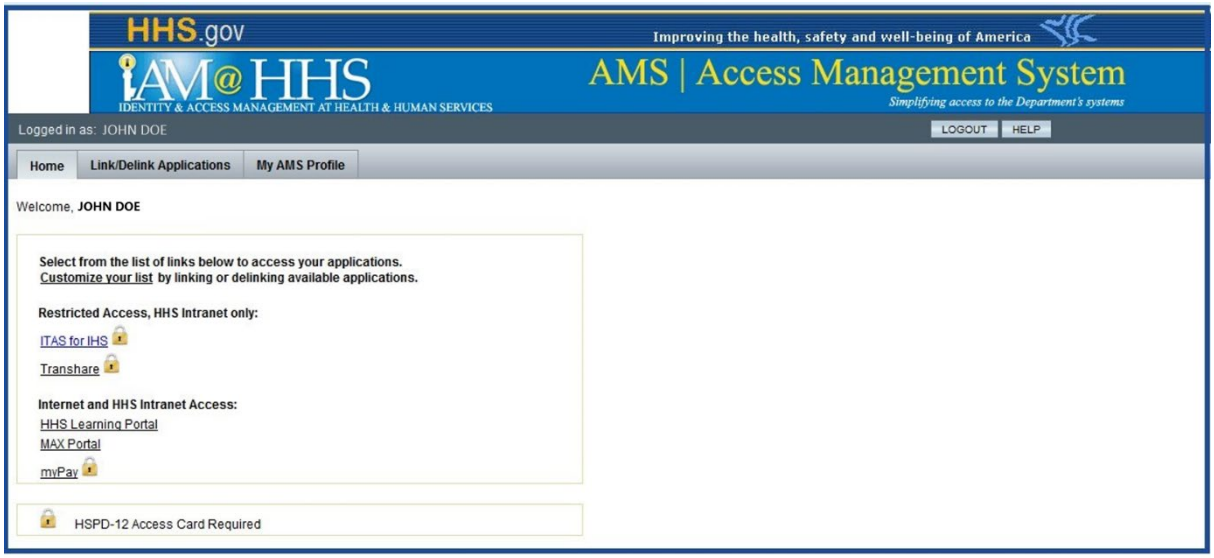


Figure 22: AMS Home Page

Other applications not listed will also prompt you for your PIV card login information as needed.

# 4. Reset VPN Password

Users are required to change their VPN password prior to password expiration. (Email notifications are sent out within two weeks of expiration.) This is accomplished using the Remote Desktop environment.

1. From within the remote desktop, press the following key combo: Ctrl+Alt+End.
2. Click **Change a password.**

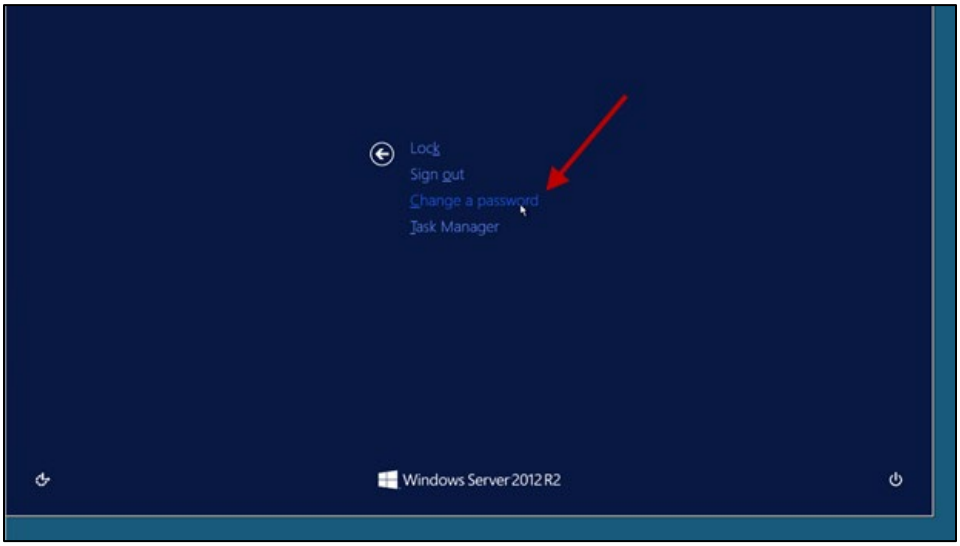


Figure 23: Click on Change a password.

3. Type the **Old password.**
4. Type a **New password.**
5. Retype your new password to **Confirm password.** .

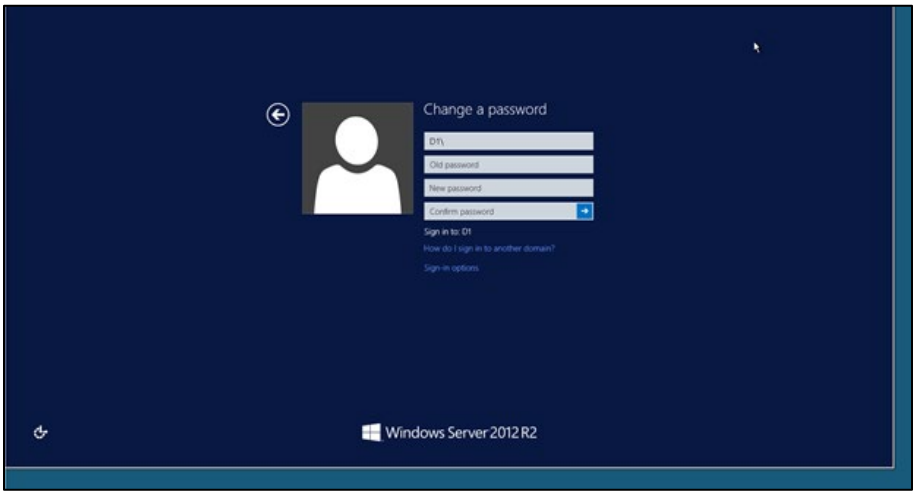


Figure 24: Apply password change.

6. Click the arrow to apply the change

# 5. Use the F5 VPN Big IP Edge (Tunnel) Client

Various users (by request only with valid justification) have access to the IHS network via the F5 VPN Big IP Edge Client. This is a standalone client installed on the user's GFE laptop that creates a connection to the internal IHS network. This type of access is reserved for government furnished equipment, or GFE, only. GFE must also meet minimum security requirements to include the following:

- System must be joined to the D1 domain
- System must be encrypted using Bitlocker
- System must have the IHS Enterprise AV client (Symantec Endpoint Protection 14.2) installed
- System must have the IHS Enterprise Patch Management agent installed (Symantec Management Agent)

## 5.1. Log On to the IHS Network via the F5 VPN Big IP Edge Client

Once a user has requested (and received approval for) tunnel access, the F5 VPN Big IP Edge client must be installed by OIT/ETS VPN Support if it is not already present on the system.

1. Log into the laptop using your IHS username and password as you would if you were on the IHS network.
2. Locate the pop-up message in the lower-right corner of your screen and click the **Attention Required, Click Here** message:

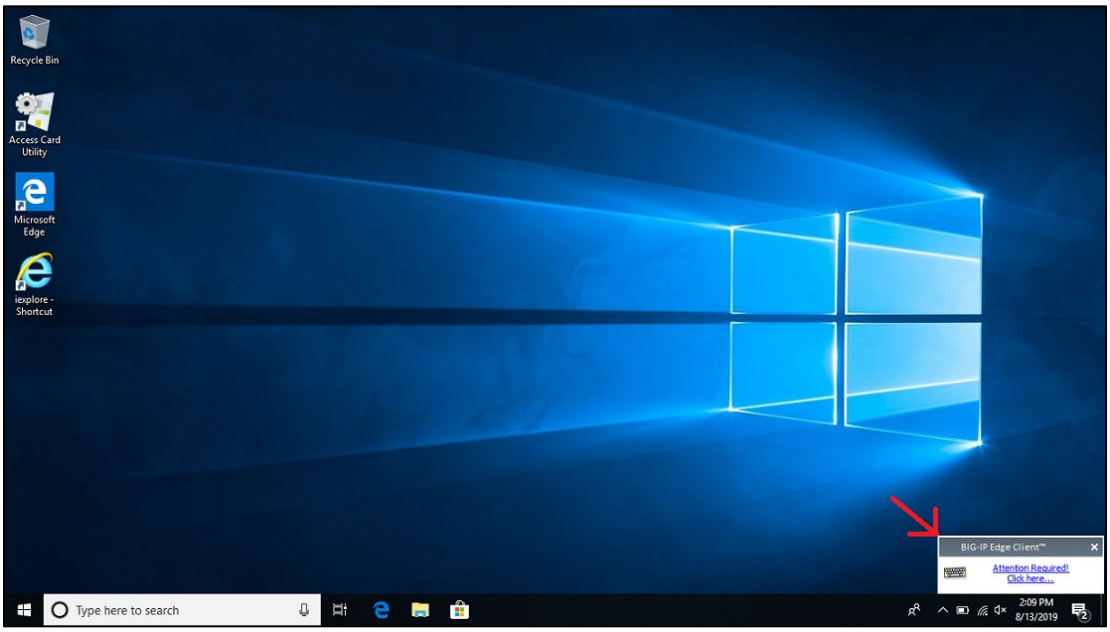


Figure 25: Attention Required, Click Here message displayed on desktop

*The system displays the VPN BIG IP Edge Client login window.*

3. Type your IHS username and password and select the V-Realm that matches your two-factor authentication method (Token, Phone, or PIV).

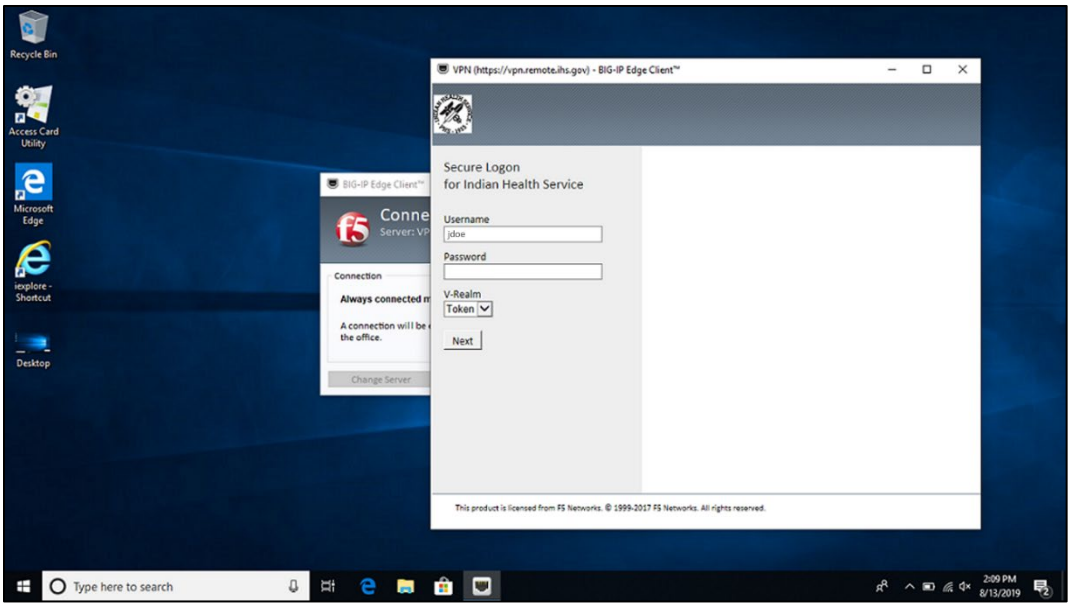


Figure 26: VPN BIG IP Edge Client login window

4. Click **Next**.

*Once you've successfully authenticated, the system displays the status of the client integrity checks being performed on the system. This process takes anywhere from 10 to 30 seconds to complete.*


Figure 27: System client integrity check progress

*Once the client integrity checks complete successfully, the systems displays the connection status of 'initializing' then it will minimize to the system tray once connected.*

5. Click the **F5** shortcut in the system tray to verify the connection status.

*The system displays the BIG-IP Edge Client connection status window.*

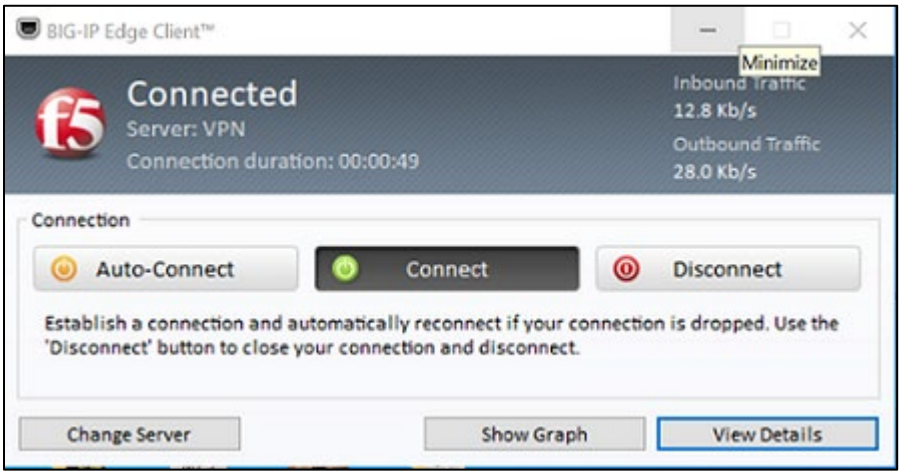


Figure 28: BIG-IP Edge Client VPN connection status window

**NOTE:** A mandatory timeout is configured for inactivity within the F5 VPN per IHS and HHS Security policies. Each VPN user will be logged out of the VPN when the inactivity standards are met and in alignment with HHS security policies. To reconnect, select **Connect** in the F5 VPN connection status window (Figure 28), and repeat the log on process outlined in Section 5.1.

## 5.2. Log Out and Disconnect from the F5 VPN Big IP Edge Client

1. Click the **F5** shortcut in the system tray.

*The system displays the F5 BIG-IP Edge Client connection status window.*

2. Click **Disconnect**.

*The system logs off the F5 VPN Big IP Edge client and terminates your connection.*

# 6. Apple Device Support

The use of Apple Devices for F5 Edge (Tunnel) Client is not supported due to client domain and validation requirements. However, Apple devices can use the Web-Portal RDP solution to connect to the IHS network. The Apple Devices supported for use with the F5 Web-Portal RDS solution are as follows: iPad, iMac, and MacBook.

To use the Web-Portal RDP solution on a supported Apple device, complete the following steps:

1. Open the App Store on your Apple Device and search for the Remote Desktop Mobile app.

   **NOTE:** This application is developed by Microsoft Corporation.

2. Install the app on your mobile device.
3. Once the Remote Desktop Mobile app is successfully installed, open the Safari Web Browser and navigate to the following web address: http://vpn.remote.ihs.gov.
4. Login with your D1 credentials and respective form of multi-factor authentication (Token, Phone or PIV).
5. Connect to your respective RDP Session using the icon(s) in the VPN Web-Portal.

# 7. Appendix A: VPN RDS Support Restrictions

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

Access to the following functions may be 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 may not be available:

- 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

# 8. Appendix B: 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 navigate to the PhoneFactor User Portal.

*The system displays the PhoneFactor User Log In page.*

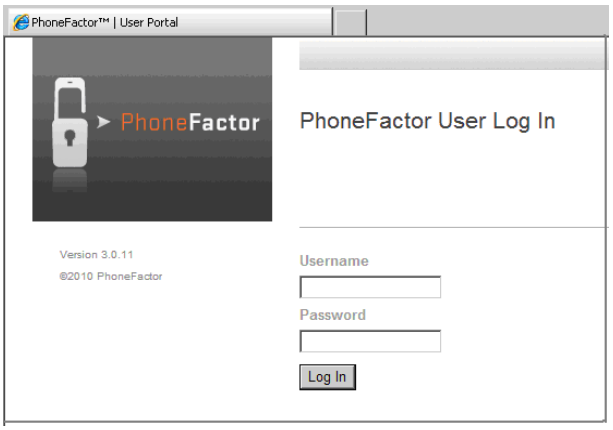


Figure 29: PhoneFactor User Log In page

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.

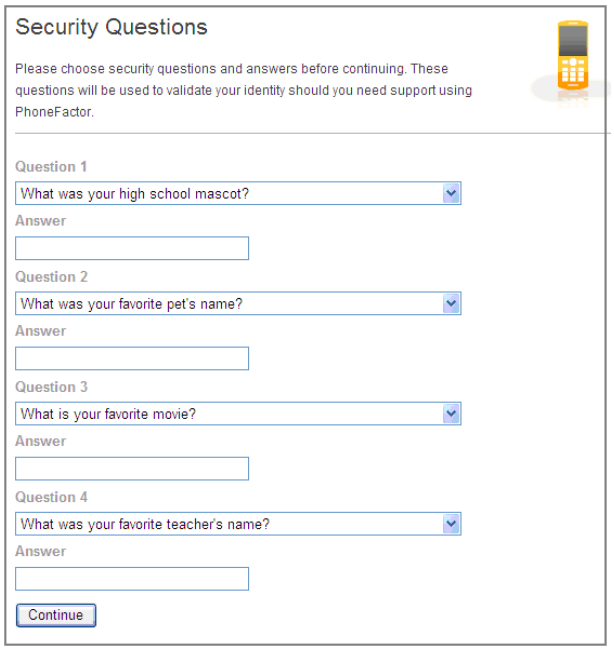


Figure 30: Security Questions page

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.

# 9. Appendix C: Acronym List

| ACRONYM | DESCRIPTION |
|---|---|
| CD-ROM | Compact Disc – Read-Only Memory |
| DIS | Division of Information Security |
| DVD | Digital Versatile Disc |
| GFE | Government-Furnished Equipment |
| HHS | Department of Health and Human Services |
| IAM | Identity and Access Management |
| IHS | Indian Health Service |
| IT | Information Technology |
| ITAC | Information Technology Access Control |
| ITAS | Integrated Time and Attendance System |
| NOSC | Network Operations and Security Center |
| NSP | Netilla Security Platform |
| OIT | Office of Information Technology |
| PIV | Personal Identity Verification |
| RDP | Remote Desktop Protocol |
| SLA | Service Level Agreement |
| SSL | Secure Sockets Layer |
| VPN | Virtual Private Network |