User Guide
Remote Access to VDI/Workplace Using PIV

Innovation & Engineering Office (IM-64)
May 2015
# Table of Contents

1 Overview .............................................................................................................................................. 3  
1.1 Web Browsers .................................................................................................................................... 3  
1.2 Operating Systems .......................................................................................................................... 3  
2 Types of Smart Card Readers and Installation .................................................................................... 4  
3 Install the External Reader on a PC ...................................................................................................... 4  
4 ![ ] Access from an EITS-provisioned Laptop .................................................................................... 5  
5 ![ ] Access from a Home Personal Computer .................................................................................. 7  
6 ![ ] Access from an EITS-provisioned Mac Laptop ......................................................................... 10  
7 ![ ] Access from a Home Personal Mac ............................................................................................ 14  
Appendix A: ![ ] Remove an Incorrect Certificate from Mac ................................................................. 20  
Appendix B: ![ ] Selecting Incorrect Certificate .................................................................................. 23  
Appendix C: Google Chrome (version 42) and Citrix Receiver .............................................................. 24  
Appendix D: ![ ] Access Denied Client SSL Certificate is Invalid ......................................................... 25
1 Overview

As mandated by the Homeland Security Presidential Directive 12 (HSPD-12), Office of Management and Budget (OMB) M 11-11, and Department of Energy (DOE) O 206.2, the Office of the Chief Information Office (OCIO) Energy IT Services (EITS) has deployed hardware, software, and configuration changes that enable EITS customers to log on to their computers with their HSPD-12 credentials.

The HSPD-12 directive also covers the implementation of virtual desktops. Personal identity verification (PIV) authentication is integrated in the virtual desktop infrastructure (VDI) design and implementation. VDI is accessible from DOE-provided trusted EITS zero-clients, laptops, and conventional desktops provisioned by EITS. VDI can also be securely accessed from external clients, such as personal computers, over the Internet, which is one of the great benefits of VDI technology.

As a remote VDI user, you must authenticate your identity with your PIV card per the HSPD-12 directive. In certain cases when you cannot use your PIV card, you can use your RSA token to log on.

The tables below list Internet browser and operating system versions tested for their functionality with remote PIV with VDI.

1.1 Web Browsers

<table>
<thead>
<tr>
<th>Browser</th>
<th>Version</th>
<th>Functions with PIV?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Internet Explorer</td>
<td>9.0.8112.16421</td>
<td>Yes</td>
</tr>
<tr>
<td>Microsoft Internet Explorer</td>
<td>11.0.9600.17358</td>
<td>Yes</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>38.0.2125.111 m</td>
<td>Yes (See Appendix C)</td>
</tr>
<tr>
<td>Safari</td>
<td>6.2.3 and above</td>
<td>Yes</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>31.1.1</td>
<td>Not supported. Reconfiguration is required to support PIV and is not recommended.</td>
</tr>
</tbody>
</table>

1.2 Operating Systems

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Version</th>
<th>Function with PIV?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>7.0 and above</td>
<td>Yes</td>
</tr>
<tr>
<td>Personal Mac</td>
<td>10.10.2 and above</td>
<td>Yes</td>
</tr>
<tr>
<td>EITS-provisioned Mac</td>
<td>10.8.5/10.9.5/10.10.2</td>
<td>Yes</td>
</tr>
</tbody>
</table>
2 Types of Smart Card Readers and Installation
The three types of smart card readers used in the DOE environment are displayed below. To learn more about card readers, see HTTPS://POWERPEDIA.ENERGY.GOV/WIKI/SMART_CARD_READER.

|------------------------|------------------------|-----------------------|

3 Install the External Reader on a PC
To install the external card reader, connect the card reader to your workstation. The card reader self-installs. To view the status of the installed card reader, go to the lower left of the Windows screen. Select Start ➔ Devices and Printers.
4. **Access from an EITS-provisioned Laptop**
   1. Once the card reader has been installed, insert your PIV card into the reader.
   2. Open web browser, type HTTPS://MYDESKTOP.DOE.GOV, and press Enter.
   3. Select **Access VDI using your PIV card**.

   ![Image of web browser with URL](image)

4. A certificate box displays.

   ![Image of certificate box](image)

5. To determine the correct certificate is being used, select **Click here to view certificate properties**. Select the **Detail** tab.

   ![Image of certificate properties](image)
a. Scroll down and select **Enhanced Key Usage** and look for Smart Card Logon as shown below.

![Certificate window showing Enhanced Key Usage and Client Authentication](image)

b. After verifying the certificate, select **OK**.

   *Note: The desktop does not ask for your PIN because it was cached after you logged onto the laptop.*

7. Type your PIN at the desktop and press **Enter**.

   *Note: If you see the username and password fields, select the Other Credentials button. Select the PIV card, type your PIN, and press Enter.*

8. You are now logged on to the VDI desktop.
5  Access from a Home Personal Computer

1. Download and install the latest receiver from HTTP://WWW.CITRIX.COM/GO/RECEIVER.HTML.
2. Insert a card reader if necessary. The card reader self-installs. To view the status of the installed card reader, go to the lower left of the Windows screen. Select Start ➔ Devices and Printers.

3. Once the card reader has been installed, insert your PIV card into the reader.
4. Open web browser, type in HTTPS://MYDESKTOP.DOE.GOV, and press Enter.
5. Select **Access VDI/Workplace using your PIV card.**

6. A certificate box displays.

7. To determine the correct certificate is being used, select **Click here to view certificate properties.** Select the **Detail** tab.
a. Select **Enhanced Key Usage** and look for Smart Card Logon as shown below.

![Certificate window](image)

b. After verifying the certificate, select **OK**.

a. The PIN prompt box displays.

![PIN prompt box](image)

8. Type your PIN and select **OK**. If you do not see the PIN prompt box, check to make sure it did not pop up behind another window.


10. Type your PIN at the desktop prompt and press **Enter**.

    **Note:** If you see the username and password fields, select the **Other Credentials** button. Select the PIV card and type your PIN.

11. You are now logged on to the VDI desktop.
6 Access from an EITS-provisioned Mac Laptop

1. Insert a card reader and your PIV card.
2. Log on to your Mac using your PIV credential.
3. Open Safari or Chrome.
4. Go to HTTPS://MYDESKTOP.DOE.GOV.

5. Select Access VDI using your PIV card.
6. You are prompted to select a certificate. Select the Show Certificate button and scroll down to Purpose #2 Smartcard Logon.
7. After verifying the certificate, select **Continue**.
8. You are not required to enter your PIN because it was cached during logon to your Mac.
9. At the prompt **Do you want to trust the website “mydesktop-piv.vdi.doe.gov” to use “Citrix Receiver Plug-in?”**, select **Trust** to unblock the Citrix plug-in.
10. Your desktop displays.
   a. If you have a single desktop, it auto-launches.
   b. If you have more than one desktop, select the preferred desktop to launch.
11. After the desktop has launched, the DOE Security Banner screen appears. Select **OK** to continue.
12. The desktop displays the message **Reading smart card...**
13. At the prompt, type your PIN and press **Enter**.
14. You are now logged on to the desktop.
Access from a Home Personal Mac

If you are a Mac user and want to access VDI using your PIV card, you must have the operating system, X Yosemite 10.10.2 or higher and Centrify Express for Smartcard installed.

1. Download and install the latest Mac receiver from [HTTP://WWW.CITRIX.COM/GO/RECEIVER.HTML](http://WWW.CITRIX.COM/GO/RECEIVER.HTML).
2. Complete the form at [HTTP://WWW.CENTRIFY.COM/EXPRESS/SMART-CARD-FORM](http://WWW.CENTRIFY.COM/EXPRESS/SMART-CARD-FORM) and accept the End User License Agreement. Select **Download Now** to see Centrify Express for Smartcard.
3. Select **Download for Mac OS 10.7, 10.8, 10.9, 10.10**.

![Centrify Express for Smartcard](image)

4. **Install** Centrify Express for Smartcard.

5. To verify that Centrify Express for Smartcard is installed, select the **Launchpad**. Find the **Smart Card Assistant**.

![Launchpad](image)

6. Open Safari and type **HTTPS://MYDESKTOP.DOE.GOV**.

7. Insert the card reader.
8. Insert your PIV card.
9. Select **Access VDI using your PIV card**.

10. You are prompted to select a certificate. Select **Show Certificate** and scroll down to Purpose #2 Smartcard Logon.
11. After verifying the certificate, select **Continue**.
   a. Centrify Express for Smartcard stores this option in the keychain, and you are not prompted to select the certificate again.
   b. If you accidentally select the wrong certificate, see appendix A for the steps to remove the certificate from the Centrify Express for Smartcard keychain.
12. At the next prompt, type your PIV card PIN, which is your keychain password. Select **OK**.
13. At the prompt **Do you want to trust the website “mydesktop-piv.vdi.doe.gov” to use “Citrix Receiver Plug-in?”**, select **Trust** to unblock the Citrix plug-in.
14. Your desktop displays.
   a. If you have a single desktop, it auto-launches.
   b. If you have more than one desktop, select the preferred desktop to launch.

15. After the desktop has launched, the DOE Security Banner screen appears. Select **OK** to continue.
16. The desktop displays the message **Reading smart card...**
17. At the prompt, type your PIN and press **Enter**.
18. You are now logged on to the desktop.
Appendix A:  🍎 Remove an Incorrect Certificate from Mac
If you select the wrong certificate in Safari, you must remove it from the Centrify Express for Smartcard keychain to be prompted to select a certificate again.

1. If the certificate did not show **Purpose #2 Smartcard Logon**, you have selected the wrong certificate.

2. Open **Launchpad** and open **Smart Card Assistant**.
3. Select **Diagnostics**, then press the **Open Keychain** button.
4. On the left, select login under **Keychains**, then select **All Items** under **Category**.

5. On the right, select the identity preference entry and select **Delete**.

6. Go back to section 6, *Access from a Home Personal Mac*. Go to step 6 to log on again. The system prompts you for the correct certificate.
Appendix B: Selecting Incorrect Certificate

If you select the wrong certificate after entering your PIN, an error message states the page cannot be displayed. Follow these troubleshooting steps to select the correct certificate.

1. Close the browser.
2. Remove your PIV card from the reader, then re-insert it.
3. Open the browser again.
4. Go back to the logon instructions to select the correct certificate.

If the wrong certificate was chosen in Safari, first follow the steps in Appendix A, Remove an Incorrect Certificate, then follow the instructions.
Appendix C: Google Chrome (version 42) and Citrix Receiver

In April 2015, Google disabled Netscape Plugin Application Programming Interface (NPAPI) plug-in support in Chrome version 42 to improve security and stability. The NPAPI plug-in for Windows and Mac enables users to launch applications by selecting them. The removal of NPAPI support impacts those who access Citrix Receiver for Web using the Chrome browser on Windows and Mac.

In September 2015, Google will remove the override and NPAPI support will be permanently removed from Chrome version 45. Installed extensions requiring NPAPI plugins will no longer be able to load those plugins. Citrix is working on a non-NPAPI plugin in upcoming Receiver releases.
Appendix D: Access Denied Client SSL Certificate is Invalid
EITS has discovered that recent security updates by Microsoft that have caused some corruption in the SystemCertificates registry key within the user profile that was used to install the updates. This does not affect any other user profile on the user’s system and connections from those profiles will continue to work. We are working with Microsoft on this issue, but in the mean time there is a workaround to get your system working properly. Follow the instructions below.

- Option A—Requires creation of new user profile.
- Option B—Requires changes to the Windows key registry.

Option A
Create a New User Account

1. At the Windows screen, select Start→Control Panel.
2. Under User Accounts and Family Safety, select Add or remove user accounts.
3. Select Create new account.
4. Type a new account name, such as User 2, and leave as Standard user.
5. Select the Create Account button.
6. The new account is created.

**Switch User to New Account**

1. Select **Start**.
2. Hover over the arrow next to **Shut down** and select **Switch user**.

3. Windows creates the new profile and logon.
4. Ensure your card reader is attached and your PIV card is inserted.
5. Open your browser and go to **https://mydesktop.doe.gov**.
6. You can now logon.
Switch Back to Another Account
1. Select Start.
2. Hover over the arrow next to Shut down and select Switch user.
3. Select another account.

Log Off New Account
1. Select Start.
2. Hover over the arrow next to Shut down and select Log off.

Option B

Warning: Changes made to the Windows registry happen immediately and no backup is automatically made. Do not edit the Windows registry unless you are confident about doing so. Microsoft has issued the following warning with respect to the Registry Editor.

Using Registry Editor incorrectly can cause serious, system-wide problems that may require you to re-install Windows to correct them. Microsoft cannot guarantee that any problems resulting from the use of Registry Editor can be solved. Use this tool at your own risk.

How to Open the Registry Editor
1. At the taskbar, select Start ➔ Search Programs and File.
2. Type regedit.exe and press Enter.
3. A pop-up for User Access Control displays and select Yes.
4. The registry editor opens
How to Back Up the Registry

Before editing the registry, make a backup of the current settings.

1. Open the Registry editor
2. From the Registry drop-down menu, select Export Registry File.
3. In the Export range panel, select All, then save the registry as the backup.

Instructions

1. At the taskbar, select Start.
2. In the upper-right corner of the Start menu, the profile name displays (see figure 1 below). Remember your profile name for the next steps.

Figure 1

3. In Search Programs and Files, type cmd and select Enter.
4. A command prompt opens. Type wmic useraccount get name,sid and select Enter.
5. A list of profile names and security identifiers (SID) display. Match the username from earlier with this SID (see figure 2 below). Remember your SID for the next steps.
6. At the taskbar, select **Start** ➔ **Search Programs and Files**. Type `regedit.exe` and select **Enter**.
8. Expand `HKEY_USERS | <SID> | Software | Microsoft | SystemCertificates` (see figure 3 below).
   The `<SID>` is the identifier you were asked to remember in the previous steps.
9. Right-click **SystemCertificates** and select **Delete** (see figure 4 below).
10. Select on 50F68CB28F9A9B7FBB06AC452A827A31CA9BC55E.
11. In the right pane, right-click on the REG_BINARY key called Blob (see figure 5).
12. Select Delete.
13. Select Yes to Confirm Value Delete.
15. Open the browser and try to authenticate using your PIV card. You can now connect without receiving the error.