## Document History

<table>
<thead>
<tr>
<th>DATE</th>
<th>VERSION</th>
<th>DESCRIPTION OF CHANGE</th>
<th>CHANGE TYPE</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/21/13</td>
<td>1.0</td>
<td>Initial Document</td>
<td>New</td>
<td></td>
</tr>
<tr>
<td>8/2/13</td>
<td>2.0</td>
<td>SSO Plug-In</td>
<td>Addition/Update</td>
<td></td>
</tr>
<tr>
<td>10/25/13</td>
<td>5.0</td>
<td>Timeout descriptions</td>
<td>Addition/Update</td>
<td></td>
</tr>
<tr>
<td>11/25/13</td>
<td>6.0</td>
<td>Updated URL table</td>
<td>Addition/Update</td>
<td></td>
</tr>
<tr>
<td>12/13/13</td>
<td>7.0</td>
<td>Updated Citrix Client Install Info and Formatting</td>
<td>Addition/Update</td>
<td></td>
</tr>
<tr>
<td>2/12/14</td>
<td>8.0</td>
<td>Added Ft Bragg URL info to Site URL table</td>
<td>Addition/Update</td>
<td></td>
</tr>
<tr>
<td>5/5/14</td>
<td>9.0</td>
<td>Updated AVHE Site URL table</td>
<td>Addition/Update</td>
<td></td>
</tr>
<tr>
<td>6/19/14</td>
<td>10.0</td>
<td>Updated AVHE Site URL table</td>
<td>Addition/Update</td>
<td></td>
</tr>
<tr>
<td>11/13/14</td>
<td>11.0</td>
<td>Updated Steps and Screenshots</td>
<td>Addition/Update</td>
<td></td>
</tr>
<tr>
<td>1/9/15</td>
<td>12.0</td>
<td>Additional Screenshots, Grammar Changes, added Introduction</td>
<td>Addition/Update</td>
<td>Updated Template Format</td>
</tr>
<tr>
<td>9/9/15</td>
<td>13.0</td>
<td>Updated DISA link</td>
<td>Addition/Update</td>
<td>Updated DISA FBCA tool link</td>
</tr>
<tr>
<td>11/2/2015</td>
<td>14.0</td>
<td>Updated AVHE Support Citrix client download link</td>
<td>Addition/Update</td>
<td>Updated AVHE Support site Citrix client download link</td>
</tr>
<tr>
<td>2/10/2016</td>
<td>15.0</td>
<td>Updated AVHE site URLs and Remedy information</td>
<td>Addition/Update</td>
<td>Updated AVHE site URLs and Remedy information</td>
</tr>
<tr>
<td>6/15/2016</td>
<td>16.0</td>
<td>Updated for Citrix StoreFront 3.5</td>
<td>Addition/Update</td>
<td></td>
</tr>
</tbody>
</table>
# Table of Contents

1. **Introduction** .......................................................................................................................... 5  
   1.1. **Purpose**.......................................................................................................................... 5  
   1.2. **Scope** ............................................................................................................................ 5  
   1.3. **Audience** ....................................................................................................................... 5  
   1.4. **Point of Contact** .......................................................................................................... 5  

2. **System Requirements** ........................................................................................................... 6  
   2.1. **DoD Common Access Card (CAC) / VA Personal Identity Verification (PIV)** ............ 6  
   2.2. **Medical Joint Active Directory Account** ..................................................................... 6  
   2.3. **Citrix Client and End User Device Configuration Settings** ....................................... 6  
   2.4. **Additional Requirements** ........................................................................................... 6  

3. **Accessing Published Applications through a Web Browser** ............................................. 7  

4. **Printing on AVHE** ............................................................................................................... 16  

5. **Saving Files Locally When Using AVHE** .......................................................................... 18  

6. **Timeouts within AVHE** ....................................................................................................... 19  
   6.1. **StoreFront Timeout** ...................................................................................................... 19  
   6.2. **Idle Timeout for Citrix Sessions** .................................................................................. 19  
   6.3. **Disconnected Timeout for Citrix Sessions** ................................................................. 20  

7. **Accessing AVHE Apps via Citrix Receiver** ...................................................................... 21  

# Index of Figures

- **Figure 1**: AVHE URL in Web Browser .................................................................................. 7  
- **Figure 2**: Select DOD EMAIL Cert from CAC ................................................................. 7  
- **Figure 3**: Enter CAC/PIV Pin .............................................................................................. 8  
- **Figure 4**: “You are not allowed to login” Error Message .................................................... 8  
- **Figure 5**: Info Page if you did not select your DOD EMAIL cert from your CAC ............... 8  
- **Figure 6**: DOD Warning Banner from AVHE StoreFront .................................................. 9  
- **Figure 7**: Default Applications on Favorites tab ............................................................... 9  
- **Figure 8**: AVHE StoreFront Desktops tab ........................................................................ 10  
- **Figure 9**: AVHE StoreFront Apps tab .............................................................................. 10  
- **Figure 10**: A typical application icon .................................................................................. 11  
- **Figure 11**: AHLTA Published Application icon ............................................................... 11  
- **Figure 12**: DOD Warning Banner from AVHE Citrix Server .......................................... 11  
- **Figure 13**: Citrix Client File Security Prompt ..................................................................... 11  
- **Figure 14**: Published Application Security Banner (AHLTA) ............................................ 12  
- **Figure 15**: Published Application Logon Screen (AHLTA) ............................................... 12  
- **Figure 16**: Citrix Single Sign On (SSO) Prompt ................................................................. 13
Figure 17: New Logon Form for Citrix SSO to Store Application Credentials (AHLTA) ........................................ 13
Figure 18: Citrix Password Manager (SSO) Published Application icon on AVHE StoreFront Page .................. 14
Figure 19: Citrix SSO Logon Manager ........................................................................................................ 14
Figure 20: Citrix SSO Stored Application Credentials (AHLTA) .................................................................. 15
Figure 21: Selecting a Printer in an AVHE Published Application Session .................................................. 16
Figure 22: Printers Published Application icon on AVHE StoreFront Page ................................................ 16
Figure 23: Setting Printing Preferences for an AVHE Published Application Session ................................. 17
Figure 24: Setting Print Layout Preferences for an AVHE Published Application Session ........................... 17
Figure 25: Selecting a Printer from a Published Application (SNPMIS) ........................................................ 17
Figure 26: Saving a File to Your Local Workstation Drive .......................................................................... 18
Figure 27: Copying and Pasting Between Local and Published Applications Using Your Clipboard .......... 18
Figure 28: AVHE StoreFront Timeout Warning ....................................................................................... 19
Figure 29: Health.mil Re-Direct After Timeout ......................................................................................... 19
Figure 30: The Citrix Receiver Add Account Wizard .............................................................................. 21
Figure 31: Select the Email Certificate ..................................................................................................... 22
Figure 32: Enter the CAC PIN ................................................................................................................. 22
1. Introduction

The Military Health System (MHS) Virtualization (MHSV) program serves as a foundational and transitional infrastructure component for future Medical Community of Interest (Med-COI) capabilities and requirements within the Department of Defense (DoD). The MHSV program and associated MHS Application Access Gateway (MAAG) sites represent a key enabler to the MHS Enterprise Architecture goal of evolving the distributed architecture and processes to enable rapid, secure delivery and life cycle support of Information Technology (IT) products and services. This is directly aligned with the Defense Health Agency (DHA) Quadruple Aim: achieve medical readiness, improve the health of our people, enhance the experience of care, and lower our healthcare costs.

MHSV is designed to provide a uniform and universal platform on which MHS applications will be hosted and delivered. Comprised of both a Server Virtualization Hosting Environment (SVHE) and Application Virtualization Hosting Environment (AVHE), combined with standardized hardware and modern blade technologies, the MHSV platform will provide the vehicle for health care providers and other authorized users to attain secure and stable access to current and future clinical and business applications. MHSV capabilities are hosted across 20 worldwide, geographically-dispersed MHS Application Access Gateway (MAAG) sites. Each MAAG site represents a centrally-managed, standard, integrated, robust and scalable computing infrastructure to support the regional delivery of applications and services to the entire MHS community. Med-COI will provide the network transport, protection and inspection for all services residing within a MAAG site.

AVHE is the framework for providing DoD-medical user's access to a growing list of client applications and delivering these applications, in most cases, through a web browser. AVHE is a Citrix-based capability that is hosted worldwide at each regional MAAG site. AVHE enables capabilities and benefits such as roaming, mobility and session persistence across multiple end-user devices and delivers access to applications “anytime, anywhere”.

1.1. Purpose

The purpose of this document is to provide IT support personnel and end-users access to resources and information for leveraging AVHE to access published applications. It includes technical requirements, key links, instructions and information pertaining to common questions when using AVHE to access applications. Additionally, it outlines support procedures for getting help.

Additional information may be found at: https://avhe-support.health.mil.

1.2. Scope

AVHE supports the delivery of a wide-variety of clinical and business applications in support of the MHS. The scope of this document is focused on gaining access to these applications as well as understanding features, such as printing and saving files, when using AVHE. User Guides for hosted applications are out of scope of this document.

1.3. Audience

The intended audience for this document are IT support personnel and end-users to help aid in understanding how applications are being delivered and ways to take advantage of related features and benefits.

1.4. Point of Contact

If you experience any issues with accessing applications on AVHE, please immediately contact the DHA Global Service Center via email at dha.gsc@mail.mil by calling 1-800-600-9332 (CONUS) or by using the appropriate country access code for OCONUS. To log a support ticket, please search for “AVHE” at the Remedy Center Request Management module (https://support-gsc.health.mil).
2. System Requirements

There are a few basic requirements for accessing AVHE. In many cases, some or all of these requirements are already met for personnel that operate at Medical Treatment Facilities (MTF) and Veteran’s Affairs (VA) facilities.

2.1. DoD Common Access Card (CAC) / VA Personal Identity Verification (PIV)

DoD CAC’s and VA PIV’s, “smart” cards about the size of a credit card, is the standard identification for active duty uniformed service personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel. AVHE requires the use of a CAC or PIV to gain access to published applications.

2.2. Medical Joint Active Directory Account

Each user requiring access to AVHE must have an account in the medical Joint Active Directory Environment. In most cases, this is automatically created for the majority of Army, Navy, Air Force and Tricare Management Activity (TMA) users. If you do not have a Joint Active Directory account, please contact the DHA Global Service Center (https://support-gsc.health.mil).

2.3. Citrix Client and End User Device Configuration Settings

Each end user device that is used to access AVHE must have the following:

2.3.1. Citrix Receiver Client

To access your application on AVHE, you will need to have a Citrix Client installed. The Citrix Receiver 4.2.100 client is the minimum recommended client and can be downloaded from the following URL:


Please consult your desktop administrators if you are not an Administrator on your workstation, as Administrative rights may be required to install the Citrix client. We recommend the Citrix Receiver 4.2.100 client (link above) or a newer Citrix client be installed.

2.3.2. DoD Root Certificates

Installing the DoD Root Certificates will allow your web browser to trust the identity of the AVHE websites that deliver published applications. These certificates may be obtained from http://iasecontent.disa.mil/pki-pke/InstallRoot_NonAdmin_4.1.msi or https://io.dha.health.mil/fls/fls_avh/InstallRoot_NonAdmin_4.1.zip.

2.3.3. Smartcard Reader and Associated Middleware

In order to access published applications from AVHE, your workstation must have a smartcard reader connected with any associated or required middleware installed.

2.4. Additional Requirements

Once the basic requirements listed above are met, each user simply needs to know the URL they need to access for a given application (described in the next section) and must have the appropriate access/credentials to the application that they will access on AVHE (if it requires separate credentials).
3. Accessing Published Applications through a Web Browser

Open your web browser and enter the AVHE URL into the address bar.

**NEW:** All sites now use one URL: https://avhe.health.mil

Select the DOD EMAIL Certificate from your CAC or the correct certificate from your PIV card and then click “OK.”
“ActivClient Login” or “Windows Security Smart Card” box will now be displayed. Enter your pin and click “OK.”

NOTE: If you receive a screen that says “You are not allowed to login. Please contact your administrator” there is a problem with your Joint Active Directory Account. Please refer to the Section 2.2 of this AVHE User’s Guide.

NOTE: If you receive a screen that says “Incorrect Certificate Chosen” then you have NOT selected your DOD EMAIL cert (or the correct PIV cert) from your DOD CAC or PIV card. Please close out your browser, reconnect to the AVHE URL, and select your DOD EMAIL cert when prompted.
The United States Department of Defense banner will now be displayed. Please read and then click “Accept.”

**NOTE:** If you receive an “Error: Access is Denied. Client SSL Certificate Invalid” error message when connecting through a web browser, then you will need to run the FBCA Cross-Certificate Remover tool from DISA.

- DISA tool link: [http://iase.disa.mil/pki-pke/Pages/tools.aspx](http://iase.disa.mil/pki-pke/Pages/tools.aspx)
- Then select tab “Certificate Validation”
- Then select “FBCA Cross-Certificate Remover” current version

On first logon, the “Favorites” tab will display the default system applications in the AVHE browser window.

Later in this document we’ll show you how to add frequently used apps to this page.
Click the “Desktops” tab to see any published desktops that have been made available to you.

The **Apps** tab is intended to work like the Apple or Google Play app stores you may be familiar with on your mobile devices.

You can use the **Categories** menu, the featured **Groups** or the **Search** box to help find the app you are looking for.
When you find an app that you plan to use frequently, click the Details link.

Next, click the Add To Favorites button to move the app to the front page, making it easier to find.

To launch an app, single click your desired application icon.

When the US DOD Warning Statement appears, please click OK.

**NOTE:** If you have access to multiple applications, it is best to wait until your first application has launched before launching another, as this will ensure your applications launch within the same Citrix session leading to faster launch times.
You may see this Citrix File Security Screen when you access your application.

• Select “Permit all access.”

**NOTE:** You may also select “Do not ask me again for this site.” If you receive this popup message consistently, please have your desktop administrator add https://*.health.mil and https://*.mhsi.health.mil to your Internet Explorer Trusted Sites.

Your application’s Security Banner will display. Click “Acknowledge” or “Accept.”

The application login window should now display.

• Enter your Username/ID and Password or CAC PIN for login

• Next click “OK.”

**NOTE:** You may save your credentials for Single Sign On (SSO) in the Citrix Password Manager if the application allows for SSO. Not all applications have SSO enabled.
When prompted, if you want to have Citrix SSO store your credentials:

- Select “Yes”

Enter your credentials for your application, then click “Finish.” SSO will then automatically submit your credentials into your application and will continue to automatically submit your logon credentials the next time you login to your application through AVHE.

**NOTE:** If you receive a logon error from your application, please ensure that you have typed your logon credentials correctly into SSO.
To manage your SSO wallet click on the Citrix Password Manager icon. This will allow you to modify your stored credentials for your application.

**NOTE:** You may see an SSO keys icon in your system tray when you are accessing another AVHE application, and you can manage your SSO wallet from there as well.

You can select your application by clicking once to highlight it and then click “Edit” to change your stored credentials.
You can now change your stored username and/or password for your application. When you finish entering this information click "OK." The change will now have been made.

**Figure 20: Citrix SSO Stored Application Credentials (AHLTA)**
4. Printing on AVHE

If you need to print from within your application on AVHE, then select the local printer you want to print from. As shown in the screenshot, local printers from your workstation will be mapped inside your Citrix session and will contain "(from <WORKSTATION_NAME>) in session #" in their description so you can identify the printer you want to print from.

If you experience issues printing in landscape mode or in duplex within your application, then after you have your application launched you can launch the “Printers” published application and modify your printing preferences (landscape/duplex settings). This is not required however for most applications.
You can then select your preferred printer, right click and select Printing preferences.

Then select your printing preferences (Landscape/Portrait, Duplex settings). These print settings will persist in your application until your Citrix session ends.

Then select the preferred printer for which you modified print preferences, and click Print in your application.
5. Saving Files Locally When Using AVHE

If you want to save a file from your application on AVHE, browse to the “C$ on ‘Client’” drive. This drive is your local workstation drive.

If you save a file to “My Documents” within an AVHE application, this is really the “My Documents” folder on the Citrix server and you won’t have that file stored locally on your workstation.

**NOTE:** Network mapped drives from your workstation may **not** be mapped within your Citrix session, however, you can always save files locally to your “C$ on ‘Client’” drive and then copy them to a network mapped drive from your local workstation if you so choose.

Clipboard Mapping is enabled for your AVHE published applications, meaning that you can copy and paste between programs on your local workstation and your Citrix session.

Copy the line or image from either your desktop program or the virtual application, and paste it to the other just as in you usually do with desktop apps.
6. Timeouts within AVHE

There are a couple of different timeouts configured in AVHE to meet mandated DoD security requirements.

6.1. StoreFront Timeout

There is a timeout for the StoreFront web page that displays on the web page itself and asks you to click for more time if needed. If the StoreFront page times out, it does not close out your applications that are already open. You would simply have to re-launch a browser connecting to the AVHE URL (https://avhe.health.mil) in order to launch additional applications from AVHE through your browser. Nothing is required to continue working in your applications that are already open.

![AVHE StoreFront Timeout Warning](image)

**Figure 28: AVHE StoreFront Timeout Warning**

**NOTE:** The Website will count down starting from 5 minutes. Once the timeout has been reached, the website will automatically be redirected to [http://www.health.mil](http://www.health.mil).

![Health.mil Redirect After Timeout](image)

**Figure 29: Health.mil Re-Direct After Timeout**

6.2. Idle Timeout for Citrix Sessions

There is an idle timeout of 30 minutes for AVHE Citrix sessions that applies to any applications you have open on AVHE that have no mouse clicks, movement, or keystrokes being entered into the application. In other words, if you have an application such as AHLTA, CHCS, or Essentris open on AVHE for 30
minutes and do not click on it or move your mouse across it or enter a keystroke then the application will go into a disconnected state on the AVHE Citrix server.

When the application is in a disconnected state, it is on “pause”; no work is lost and the application is waiting for you to reconnect to it and resume work. This is the functionality that allows you to roam your applications from one workstation to another and maintain your application state across those different workstations (we call this smooth roaming). You can reconnect to a disconnected application by accessing the AVHE StoreFront page through a browser (https://avhe.health.mil) and the application should automatically reconnect.

6.3. **Disconnected Timeout for Citrix Sessions**

Lastly, there is a disconnected timeout of 60 minutes for AVHE Citrix sessions that would apply to any applications you have on AVHE that are in a disconnected state *after their idle timeout has expired*. Once your disconnected session reaches that timeout value, your session is terminated and the application closes. For example, if you were to walk away from your desk for longer than 90 minutes, when you return to your desk any applications you had open on AVHE would be closed out and you would be unable to reconnect to that session. It's important for you to save your work if you expect to be away for an extended amount of time.

Please note that these timeouts are separate from any application specific timeouts. AHLTA, for example, typically has a timeout that locks the application after 15-30 minutes of idleness. Application timeouts will continue to be in affect and operate as they normally would when accessed on AVHE.
7. Accessing AVHE Apps via Citrix Receiver

You may be able to access AVHE StoreFront applications without using your browser. If you are on a JAD domain-joined computing device, contact your local desktop support team for guidance and they can reach out to the DHA Global Service Center if needed.

If you are connecting from a non-domain-joined device that meets all of the previously mentioned prerequisites (see section 2 on page 6), you may be able to use the following steps to configure your Citrix Receiver client to directly access AVHE applications and integrate them into your local desktop.

![Figure 30: The Citrix Receiver Add Account Wizard]

When you install the Citrix Receiver client for the first time, you will be prompted to add a server address via the Add Account wizard.

Enter `avhe.health.mil` and click Add.
Select your email certificate and click OK.

**Figure 31: Select the Email Certificate**

Enter the certificate PIN and click **Log On**.

**Figure 32: Enter the CAC PIN**

From this point, if you are using Citrix Receiver version 4.4 or newer, the process is identical to the web browser experience described above in section 3, beginning on page 9. Older Receiver clients may look a little different, but the applications should work the same.