

HTML ACCESS (CLIENTLESS INTERNET ACCESS)

NOTE:

The Internet connection method does not support the use of two-way audio and video (i.e. USA Voice and Skype for Business video chat will not be available).

HTML Access depends on HTML5 and is only compatible with the following Web browsers, (USAO recommends using Microsoft Internet Explorer):

Internet Explorer 10 or later

Firefox 21 or later

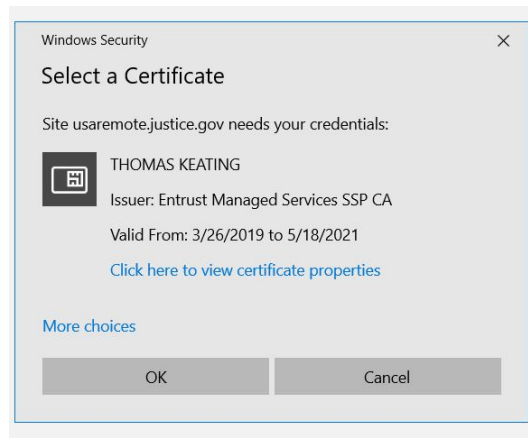
Chrome 28 or later

Safari 6 or later

Mobile Safari on iOS devices running iOS 6 or later

Establishing a Connection with the HTML Access

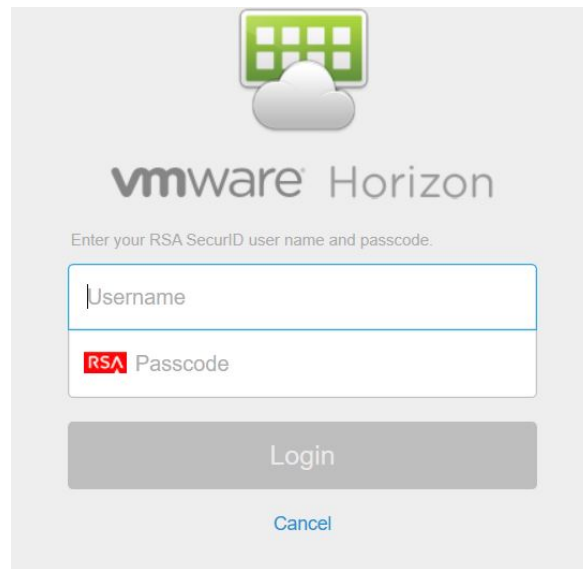
1. Start *Internet Explorer* (or another compatible web browser of your choice).
2. Type in the following URL: <https://usaremove.justice.gov>
You may get a prompt to provide a Certificate, like the one below, just hit cancel:



3. The *USAO Virtual Desktop Portal* should appear. To begin a *Remote Access 2.0* session, select the icon to the right, which is labelled **VMware Horizon HTML Access**:



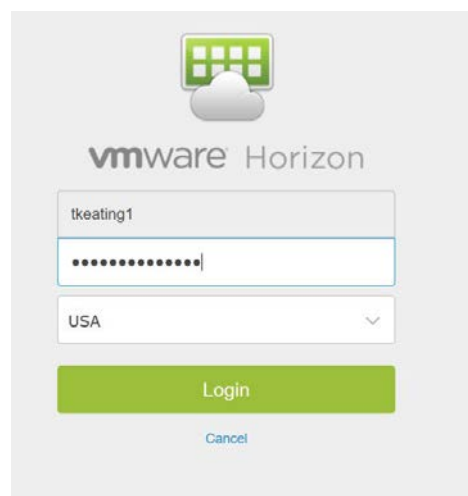
4. At the *RSA SecurID* dialog box, enter your USAO *[username]* and RSA *[passcode]* and then select the **Log In** button.
- a. Open the RSA App on your iPhone, type in your 6 digit PIN and the *[passcode]* is the randomly generated eight numbers. Type this number into the RSA Passcode box shown in the window below.
- b. **Hard Token (keyring fob)** - Your RSA *[passcode]* is a combination of your 6 digit PIN and the randomly generated six numbers on your *RSA SecurID token*. For example, if your PIN is **123456**, and your SecurID token is currently showing **260610** the resulting RSA passcode is **123456260610**, which will be the number you type in the RSA Passcode box shown in the window below.



The screenshot shows the VMware Horizon login interface. At the top is the VMware logo (a green square with a white grid) and the text "vmware Horizon". Below this is the instruction "Enter your RSA SecurID user name and passcode." There are two input fields: the first is labeled "Username" and the second is labeled "RSA Passcode" with a small red "RSA" logo to its left. Below the input fields is a large grey "Login" button and a smaller blue "Cancel" link.

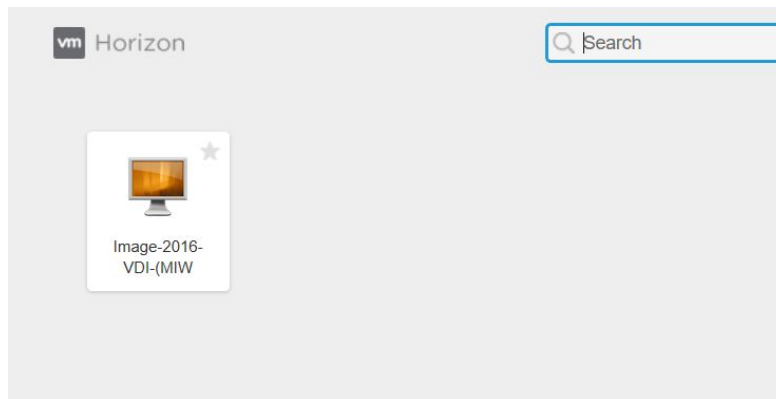
5. At the *Log In* dialog box, enter your 14 character USAO Network *[password]* and then select the **Sign In** button. (See the window below)

Note: This is **NOT** your PIV Card PIN. This is your windows network password.



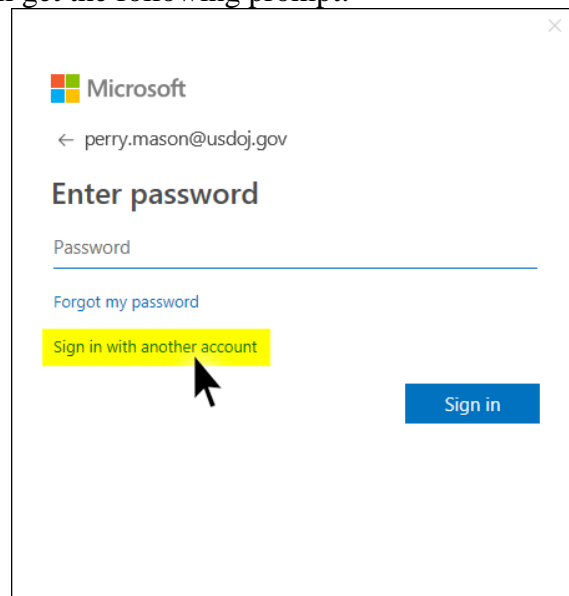
The screenshot shows the VMware Horizon "Log In" dialog box. At the top is the VMware logo (a green square with a white grid) and the text "vmware Horizon". Below this are three input fields: the first contains the text "tkeating1", the second contains a series of dots representing a masked password, and the third is a dropdown menu showing "USA". Below the input fields is a large green "Login" button and a smaller blue "Cancel" link.

6. Once your credentials have been verified, the *USAO Virtual Desktop Portal* will display any desktop pools for which you have been granted access. For *Remote Access 2.0*, select the **Image-2016-VDI (MIW)** pool.



7. Acknowledge the standard *USAO Security Warning* by selecting the **OK** button.
8. Please allow 30 to 60 seconds for the Desktop to initialize.
9. Use your *Remote Access 2.0* desktop as you would use your USAO workstation. All of the standard Image 2016 applications have been pre-loaded for your convenience.

Note: The first time you launch Outlook, you will have to create your Office 365 profile. You will get the following prompt:



DO NOT ENTER YOUR PASSWORD. Click on the Sign in with another account link. At the next screen, remove your external email address and replace it with your internal email address as shown in the image below:



Click the Next button and your Outlook profile will load and populate all of your emails. This may take a while depending on the amount of emails that you have.

10. To end the session, select the **Start** button and then select **your name at the top of the menu** and choose Sign out. Logging off your desktop will close all applications, save all of your profile data for your next session, and disconnects your desktop.
11. Select the **Close** button on the *Desktop Disconnected* message and then close your web browser.

Note: Make sure to log off and disconnect so your Remote Access 2.0 profile does not interfere with your profile in the office.