



Los Angeles County - Department of Health Services

DHS Security Operations

RSA Soft-Token SecurID

&

DHS SSL VPN Instructions



DHS Security Operations
Web SSL VPN



Table of Contents

I. [RSA SecurID Software Installation](#)..... 2

II. [Import SecurID Token](#) 5

III. [Access DHS VPN Services](#) 7

IV. [System Requirements and Troubleshooting](#)..... 15

Technical Assistance

HSA Service Desk – (213) 240-8443

I. RSA SecurID Software Installation

1. RSA SecurID 4.1 Software supported platforms:
 - Windows XP Professional SP3
 - Windows 7 Enterprise 32-bit and 64-bit
 - Windows 7 Professional 32-bit and 64-bit
 - Windows Vista Business SP1 and SP2 32-bit and 64-bit
 - Windows Vista Enterprise SP1 and SP2 32-bit and 64-bit
2. Copy the **username.sdtid** file from the email to your local PC, you will need this file later to import the soft token
3. Download RSA Soft Token software from RSA server
 - <ftp://ftp.rsasecurity.com/pub/agents/RSASecurIDToken410.zip>
4. Extract/Unzip RSASecurIDToken410.zip file to your local PC
5. Run/Execute **RSASecurIDToken410.msi** to start the installation wizard

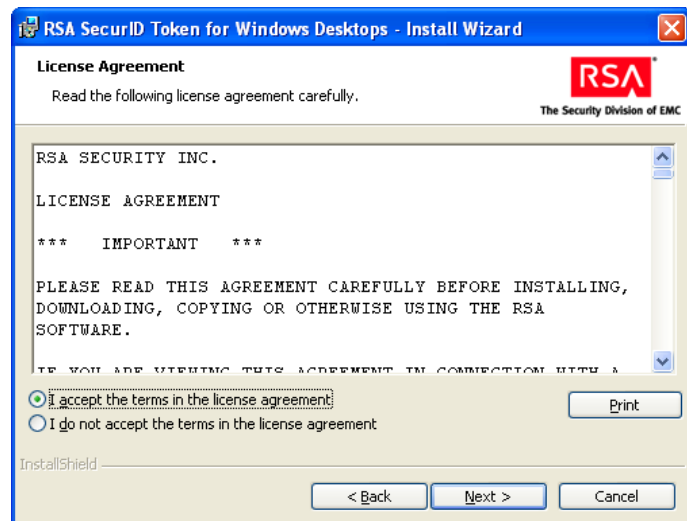
6. Once the installation begins, click **Next**



7. Accept the default settings and click **Next**



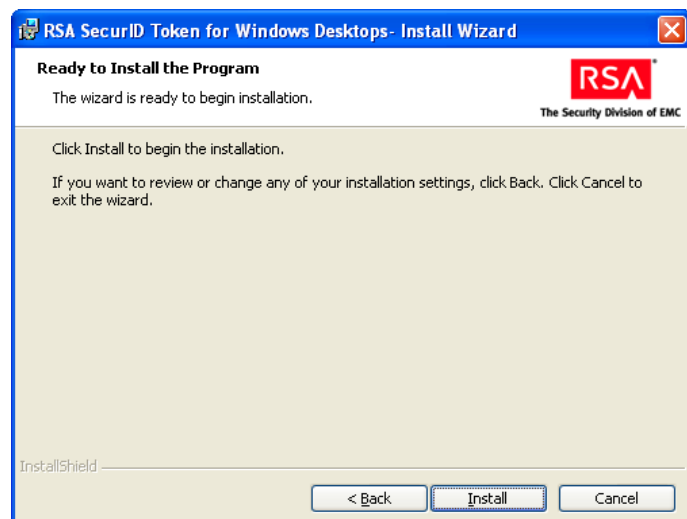
8. Select "I accept the terms in the license agreement" and click **Next**



9. Click on Typical and click **Next**



10. Click **Install**, this will begin the installation



11. Click **Finish** to complete installation

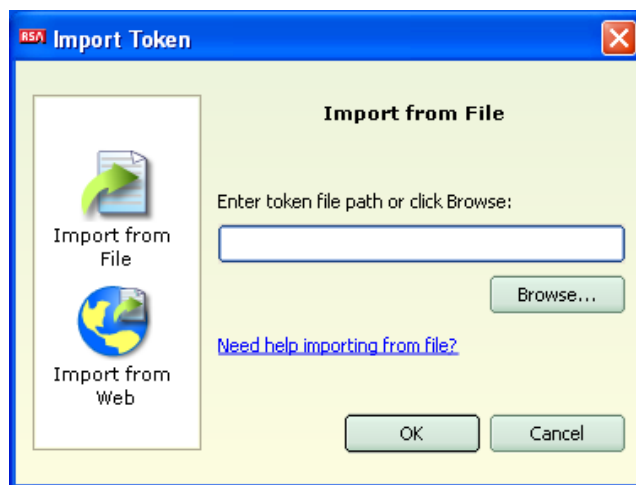


II. Import RSA SecurID Token

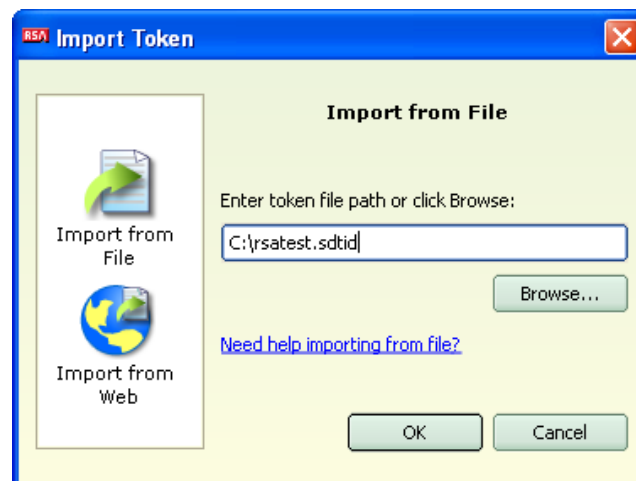
1. Click on **Start** → **All Programs** → **RSA** → **RSA SecurID Token**, then click on RSA SecurID Token shortcut to launch the application



2. Next, you will be asked to import the **username.sdtid** file that was sent to you by email, click on **“Import from file”**



3. Click on **Browse** and locate the file you previously saved on your PC

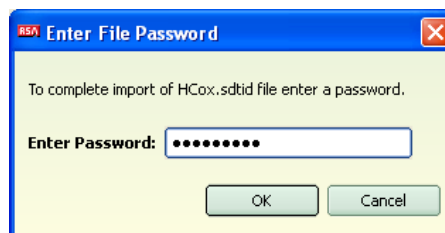


4. Click **OK** to import file into RSA Soft token

- Before the token file can be imported, you will need to provide a password. This password should have been provided to you by phone or via email

Note: This password will **ONLY** be used to import the token

- Type the password and click **OK**



- Click on **Change Name** and input your VPN username that was provided to you. (This is optional but is recommended if you are going to import more than one soft token.)



- Click **OK** to change the name



- This concludes the installation of the RSA SecurID soft token software on your PC.



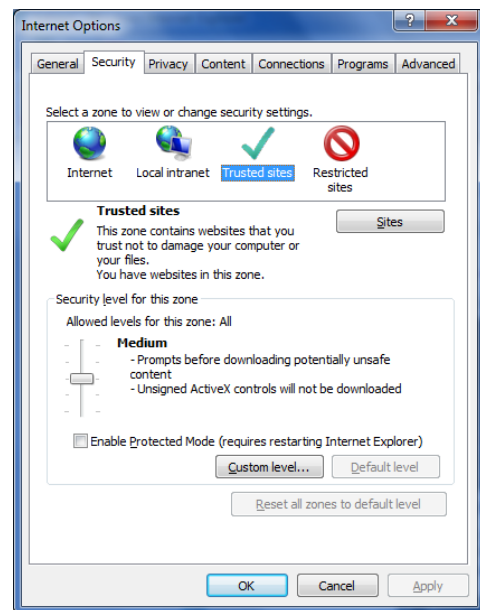
III. Access DHS VPN Services

1. VPN supported browsers:
 - Internet Browser (IE 7 and above)
 - Firefox (3.x+)
 - Other browsers may work but will not be supported

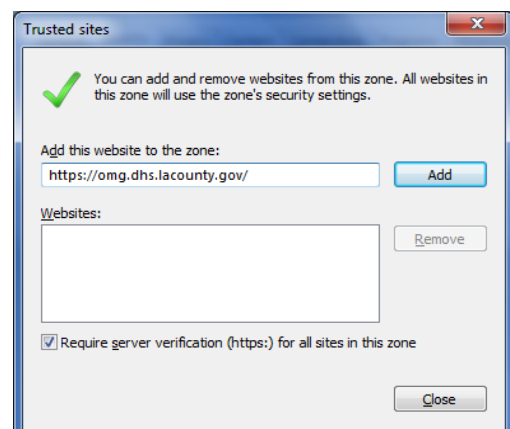
2. Cisco VPN “AnyConnect” Client supported platforms:
 - Windows 7 (32-bit and 64-bit)
 - Windows Vista (32-bit and 64-bit)—SP2 or Vista Service Pack 1 with KB952876.
 - Windows XP SP2 and SP3.

3. If you’re using Internet Explorer (IE) browser, follow the steps below; otherwise skip to [Step #4](#)

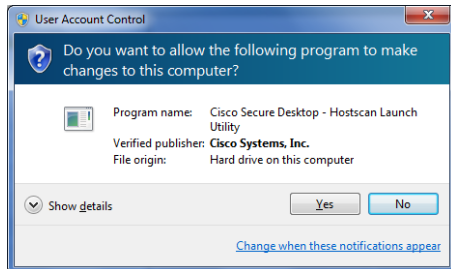
- Internet Explorer -> Tools -> Internet Options
- Select **Security** tab, select **Trusted Sites**
- Click on **Sites**
- Add <https://omg.dhs.lacounty.gov> as trusted site



- Enter: <https://omg.dhs.lacounty.gov>, click **Add**
- Click **Close**, then click **OK**



4. Open a supported browser and navigate to <https://omg.dhs.lacounty.gov>
 - Click **Yes** to run Cisco Secure Desktop when prompted



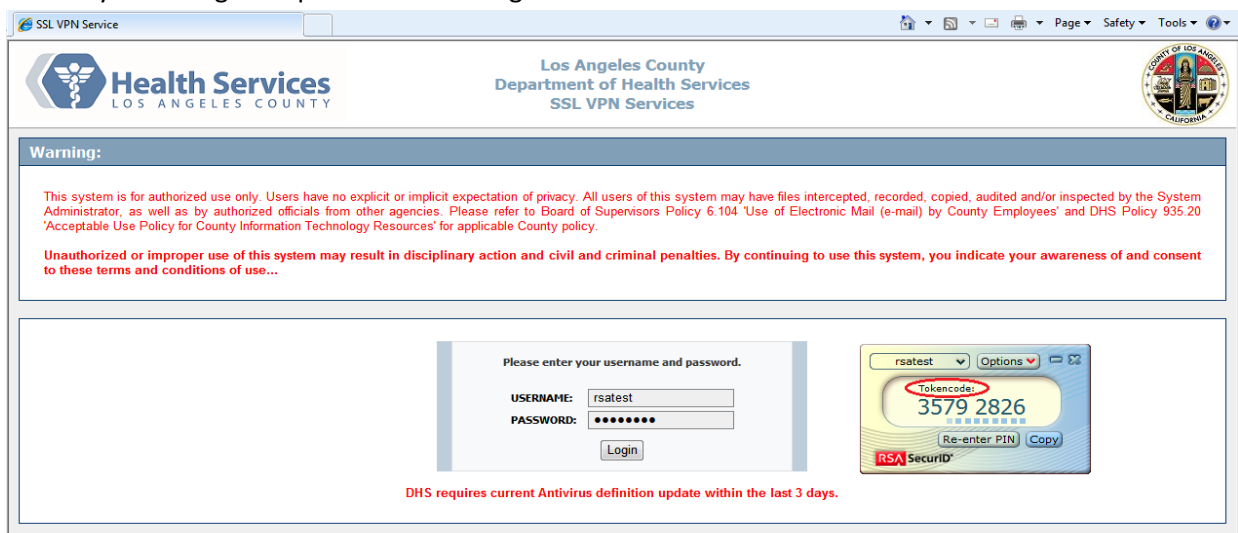
5. Login to DHS VPN Services
 - 5.1. FIRST TIME customers ONLY or customers that have their PIN reset

NOTE: If you already have a PIN, please skip to [Step 5.2 on page 12](#)

- Launch the RSA ID Software
- To generate a **TOKENCODE**, click on the **arrow** button on the RSA SecurID application. (**NOTE: DO NOT** enter anything on the Enter PIN)



- At the login Window, enter your VPN username & **TOKENCODE** as the password – this will take you through the process of creating a new **PIN**



- You will then be prompted to create a new **PIN**.
- Your **PIN** can only consist of numbers and not letter or symbols. For example, you can create a pin using 1234 or 865482



DHS Security Operations Web SSL VPN



Department of Health Services

Health Services
LOS ANGELES COUNTY

Los Angeles County
Department of Health Services
SSL VPN Services

Warning:

This system is for authorized use only. Users have no explicit or implicit expectation of privacy. All users of this system may have files intercepted, recorded, copied, audited and/or inspected by the System Administrator, as well as by authorized officials from other agencies. Please refer to Board of Supervisors Policy 6.104 'Use of Electronic Mail (e-mail) by County Employees' and DHS Policy 935.20 'Acceptable Use Policy for County Information Technology Resources' for applicable County policy.

Unauthorized or improper use of this system may result in disciplinary action and civil and criminal penalties. By continuing to use this system, you indicate your awareness of and consent to these terms and conditions of use..

..Enter a new PIN having from 4 to 8 digits.

More information is required to log in.

Response

Continue Cancel

- Re-enter the same PIN in previous step

Department of Health Services

Health Services
LOS ANGELES COUNTY

Los Angeles County
Department of Health Services
SSL VPN Services

Warning:

This system is for authorized use only. Users have no explicit or implicit expectation of privacy. All users of this system may have files intercepted, recorded, copied, audited and/or inspected by the System Administrator, as well as by authorized officials from other agencies. Please refer to Board of Supervisors Policy 6.104 'Use of Electronic Mail (e-mail) by County Employees' and DHS Policy 935.20 'Acceptable Use Policy for County Information Technology Resources' for applicable County policy.

Unauthorized or improper use of this system may result in disciplinary action and civil and criminal penalties. By continuing to use this system, you indicate your awareness of and consent to these terms and conditions of use..

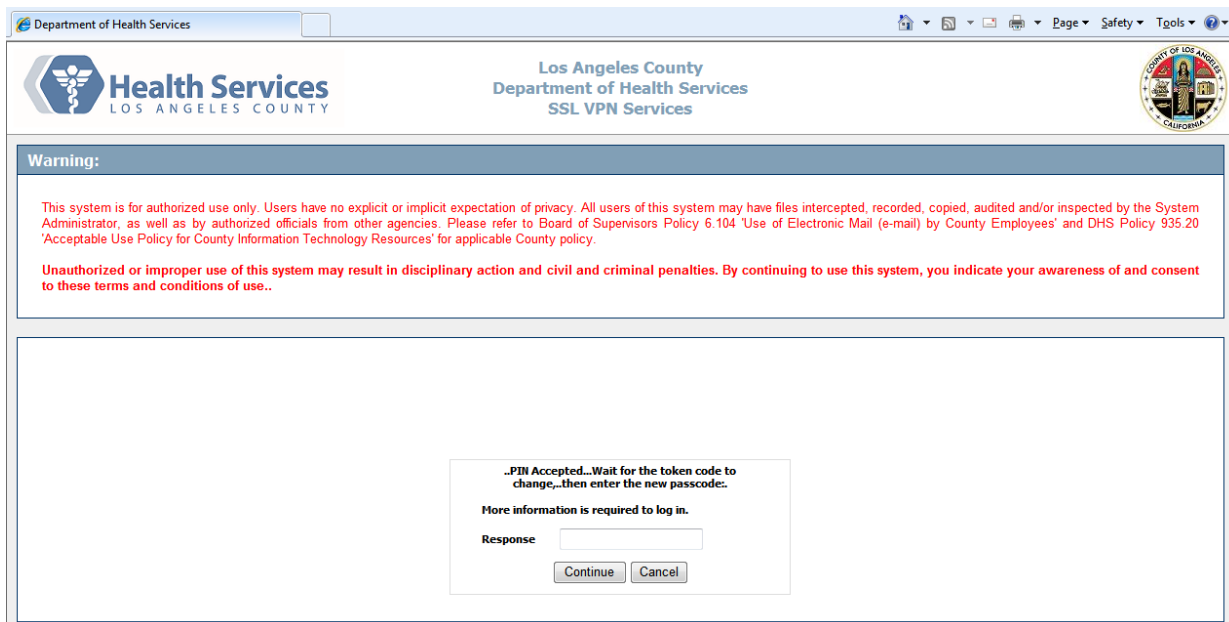
..Please re-enter new PIN.

More information is required to log in.

Response

Continue Cancel

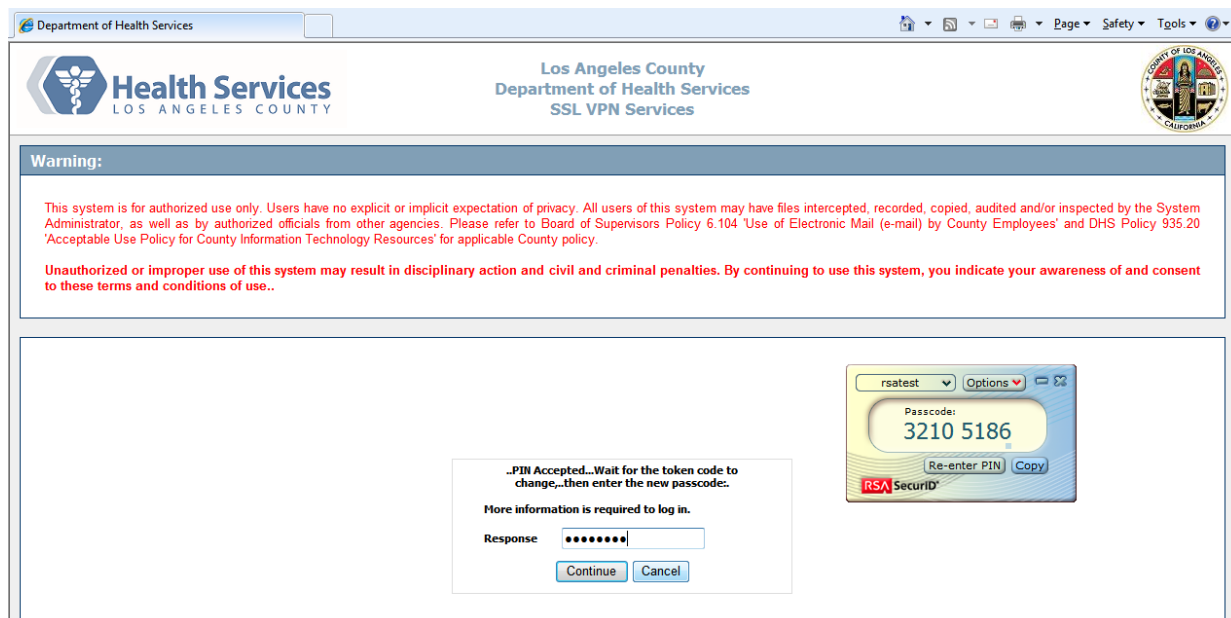
- The page below confirms that your **PIN** has been created successfully



- Next, **wait for the TOKENCODE to change to different numbers**
 - To generate a **PASSCODE**
 - click on **“Re-enter PIN”** on RSA SecurID application
 - Enter your **PIN** (in this example, is the **PIN** that you created previously)
 - Click on the **arrow** button
 - This Number will be your Passcode



- Type the **PASSCODE** in the **Response** field on the web browser and click **Continue**



Department of Health Services

Health Services
LOS ANGELES COUNTY

Los Angeles County
Department of Health Services
SSL VPN Services

Warning:

This system is for authorized use only. Users have no explicit or implicit expectation of privacy. All users of this system may have files intercepted, recorded, copied, audited and/or inspected by the System Administrator, as well as by authorized officials from other agencies. Please refer to Board of Supervisors Policy 6.104 'Use of Electronic Mail (e-mail) by County Employees' and DHS Policy 935.20 'Acceptable Use Policy for County Information Technology Resources' for applicable County policy.

Unauthorized or improper use of this system may result in disciplinary action and civil and criminal penalties. By continuing to use this system, you indicate your awareness of and consent to these terms and conditions of use..

rsatest Options

Passcode:
3210 5186

Re-enter PIN Copy

RSA SecurID

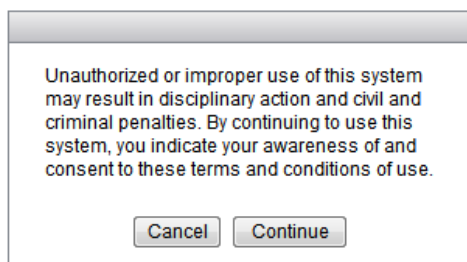
..PIN Accepted...Wait for the token code to change...then enter the new passcode:.

More information is required to log in.

Response: [.....]

Continue Cancel

- Once this dialog box appeared, you have logged in successfully, read the disclaimer and click **Continue**



Unauthorized or improper use of this system may result in disciplinary action and civil and criminal penalties. By continuing to use this system, you indicate your awareness of and consent to these terms and conditions of use.

Cancel Continue

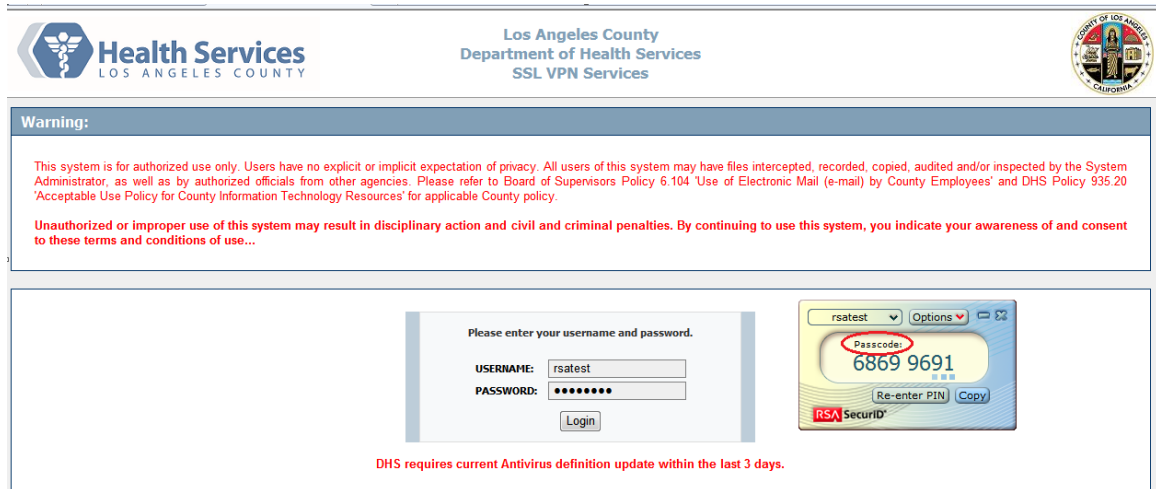
- Continue on to [Step #6 on page 13](#)

5.2 Customers that already have a RSA PIN

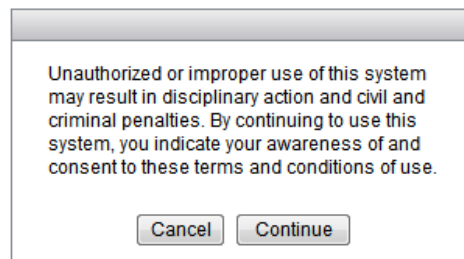
- Launch RSA SecurID software from **Start** → **All Program** → **RSA** → **RSA SecurID Token**
- Enter your **PIN**
- Click on the **arrow** button to generate the **PASSCODE**



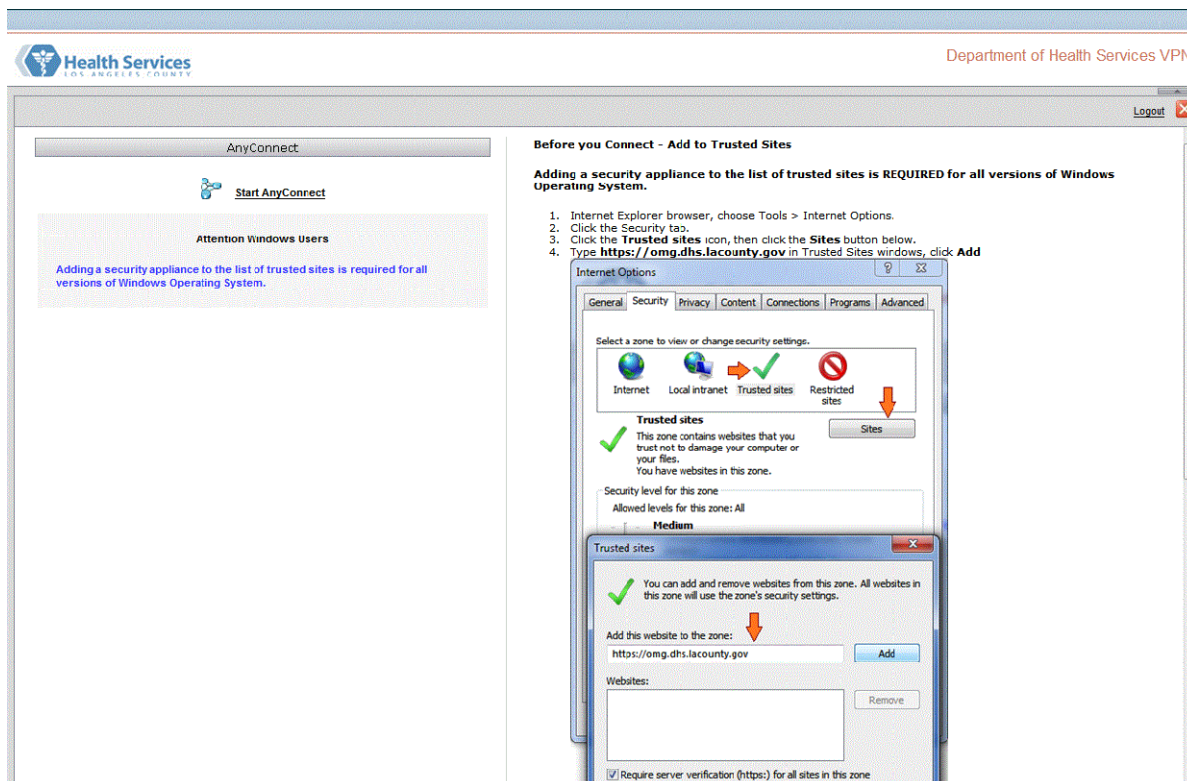
- At the login window, enter your VPN username & **PASSCODE** in the password field
- Click **Login**



- Once this dialog box appeared, you have logged in successfully, read the disclaimer and click **Continue**



6. Start the VPN Connection by clicking on **Start AnyConnect** Link

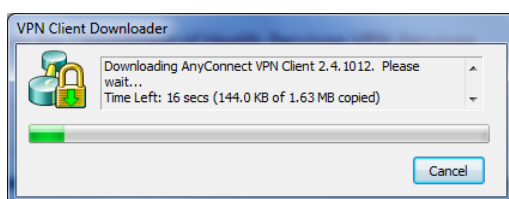


Before you Connect - Add to Trusted Sites

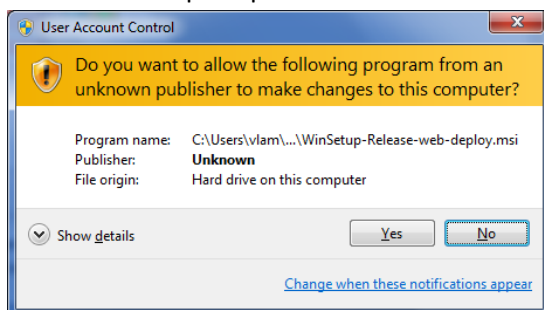
Adding a security appliance to the list of trusted sites is **REQUIRED** for all versions of Windows Operating System.

1. Internet Explorer browser, choose Tools > Internet Options.
2. Click the Security tab.
3. Click the **Trusted sites** icon, then click the **Sites** button below.
4. Type **https://omg.dhs.lacounty.gov** in Trusted Sites windows, click **Add**

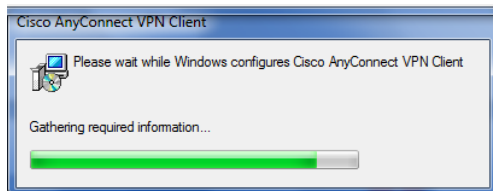
- **VPN Client Downloader** will attempt to install AnyConnect client on the local computer (**NOTE:** Depends on your Internet Connection speed, this process may take a few minute)



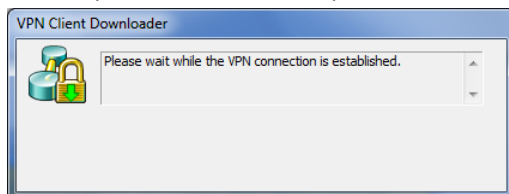
- Click **Yes** when prompted




- Cisco AnyConnect VPN Client will go through the installation process, select all default settings and click next if prompted



- VPN AnyConnect will attempt to establish a VPN connection




- Once connected, you will notice a connected icon  displayed on your system tray as indicated in the picture below:



- Now you're fully connected to DHS VPN services. You can close the browser and access DHS resources.

7. To terminate your VPN session

- Right-click on the icon  in system tray and select **disconnect/quit**
- Upon disconnecting your VPN session, the VPN client will close the browser application to erase any cached content.
- Please be advised to complete and/or save your work on all browser sessions before disconnect.

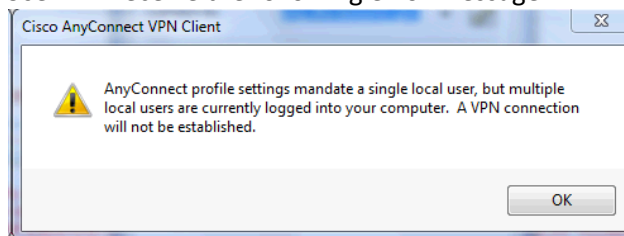
NOTES: Please note that once you have the AnyConnect Client installed on your computer, you can initialize the VPN connection by going to

- **Start -> All Program -> Cisco -> Cisco AnyConnect Client -> Cisco AnyConnect Client**
- **And login with your VPN user name and PASSCODE**

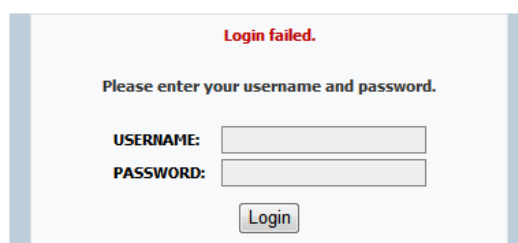
IV. System Requirements & Troubleshooting

1. RSA SecurID Software supported platforms:
 - Windows 7 Enterprise 32-bit and 64-bit
 - Windows 7 Professional 32-bit and 64-bit
 - Windows Vista Business SP1 and SP2 32-bit and 64-bit
 - Windows Vista Enterprise SP1 and SP2 32-bit and 64-bit
 - Windows XP Professional SP3
2. Cisco VPN AnyConnect supported platforms:
 - Windows 7 (32-bit and 64-bit)
 - AnyConnect requires a clean install if you upgrade from Windows XP to Windows 7.
 - If you upgrade from Windows Vista to Windows 7, manually uninstall AnyConnect first, then after the upgrade, reinstall it manually or by establishing a web-based connection to a security appliance configured to install it. Uninstalling before the upgrade and reinstalling AnyConnect afterwards is necessary because the upgrade does not preserve the Cisco AnyConnect Virtual Adapter.
 - AnyConnect requires a clean install if you upgrade from Windows XP to Windows Vista
 - Windows Vista (32-bit and 64-bit)—SP2 or Vista Service Pack 1 with KB952876.
 - AnyConnect requires a clean install if you upgrade from Windows XP to Windows Vista
 - Windows XP SP2 and SP3.
2. If there is terminal services or multiple users logged on to the machine (ie switch user features), SSLVPN AnyConnect client may not work until the second terminal session is logged off.

User will receive the following error message:

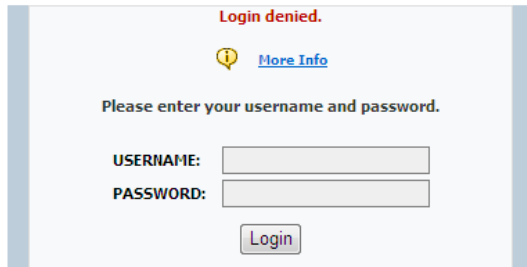


3. Unable to login with the following login failures screenshot



- Ensure that you enter the correct **PIN** to that generates the **PASSCODE**.
Please note: that you can only use a **PASSCODE once**. If you need to retry, wait for the code to change to a different number and then "Re-Enter" PIN to generate a new **PASSCODE**. If login problem persists, contact HSA Service Desk for further assistance.

- If the client machine does not have antivirus application installed and/or antivirus definition is out-of-date, access to DHS VPN will be denied with the following error message.
 - DHS VPN Service requires current Antivirus definition update within the last 3 days



Login denied.

[More Info](#)

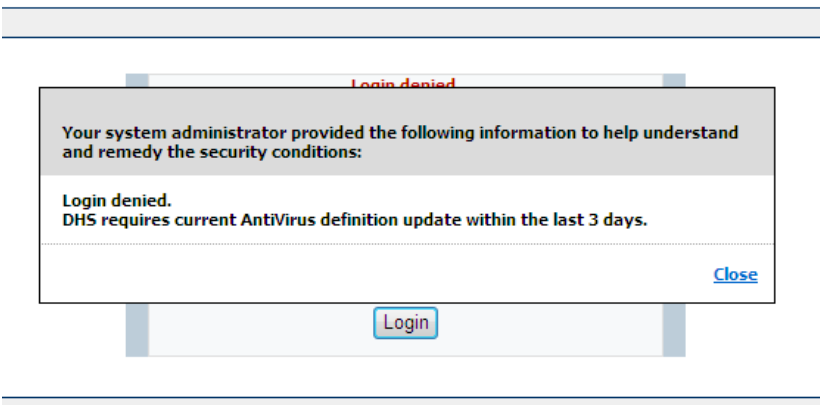
Please enter your username and password.

USERNAME:

PASSWORD:

Login

- Click on “**More Info**” link to identify the specific error message.



Login denied.

Your system administrator provided the following information to help understand and remedy the security conditions:

Login denied.
DHS requires current AntiVirus definition update within the last 3 days.

[Close](#)

Login

- For technical assistance, please contact the HSA Service Desk by calling **213-240-8443** or **Send an Email to: HSASERVICEDESK@DHS.lacounty.gov** and describe your issue. HSA Service Desk technical personnel will contact you to assist with the issue.