

## TRIPLER REMOTE ACCESS INSTRUCTIONS – JUNIPER VPN CAC (VENDORS)

### 1) Hardware/OS/Software Requirements:

- a) Organization's authorized computer
- b) CAC Reader
- c) Windows Server 2K3, Windows XP SP3, VISTA, Windows 7
- d) ActiveClient v6.x (CAC Middleware)
- e) Juniper Installer and NetConnect (Juniper SSL VPN software)
  - Internet Explorer (IE) 7.0 or v8.0
  - SSL 3.0 or TLS 1.0
  - 128 bit encryption or better
- f) McAfee/Symantec (DoD approved Antivirus Program) – NO FIREWALL
  - Signatures must not be older than 10 updates

### 2) Install Juniper Client:

- a) Download and Install the Juniper Installer and NetConnect from:
  - <http://www.tamc.amedd.army.mil/juniper> \*Administrator privilege is required to install.

### 3) Register VeriSign class 3 Public Primary Certificate to IE:

- a) Download and extract the VeriSign Public Primary Certificate from [www.tamc.amedd.army.mil/juniper](http://www.tamc.amedd.army.mil/juniper)
- b) Locate and select "VeriSign Class 3 Public Primary Certification Authority – G5.cer"
- c) Install certificate and store certificate in the Trusted Root Certification Authorities folder.

### 4) Download DOD PKI Root Certs:

- a) Download and install all DOD PKI certificates (refer to detailed instructions found at DISA's website)  
<http://dodpki.c3pki.chamb.disa.mil/rootca.html>  
**\*ALL PKI certificates MUST be imported to the browser.**  
OR  
<https://www.us.army.mil/suite/page/474113> (MUST have an active AKO account to access).
  - Select Downloads (DOD PKE Quick Links Left Frame)
  - Scroll down to download InstallRoot for MS Windows.
  - Download InstallRoot 3.13 for Windows

### 5) Register your CAC card PKI certificates to IE:

- a) The ActivClient program auto-registers the certificates to Windows. If program failed, go to Tools -> Advanced -> Make Certificates Available to Windows.
  - \*To validate certificates, launch IE. Go to Tools->Internet Options -> Content -> Certificates -> Personal TAB. It should have 3 PKI certificates imported.  
i.e

DOE.JANE.M.1234567890	DOD CA-20	9/30/2010
-----------------------	-----------	-----------

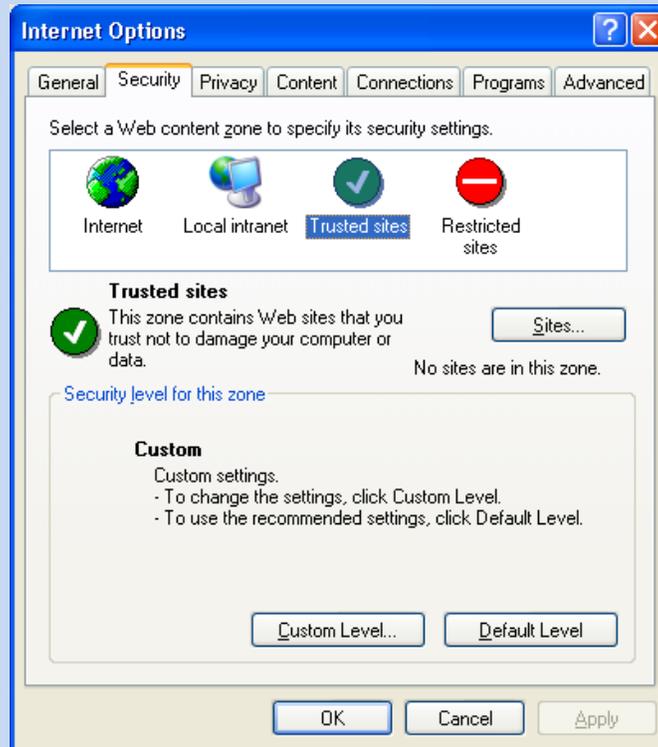
DOE.JANE.M.1234567890	DOD EMAIL CA-20	9/30/2010
DOE.JANE.M.1234567890	DOD EMAIL CA-20	9/30/2010

- *You must have all 3 certificates.*
- *All 3 certificates must all be on the same CA server.*
- *All 3 certificates must be current.*

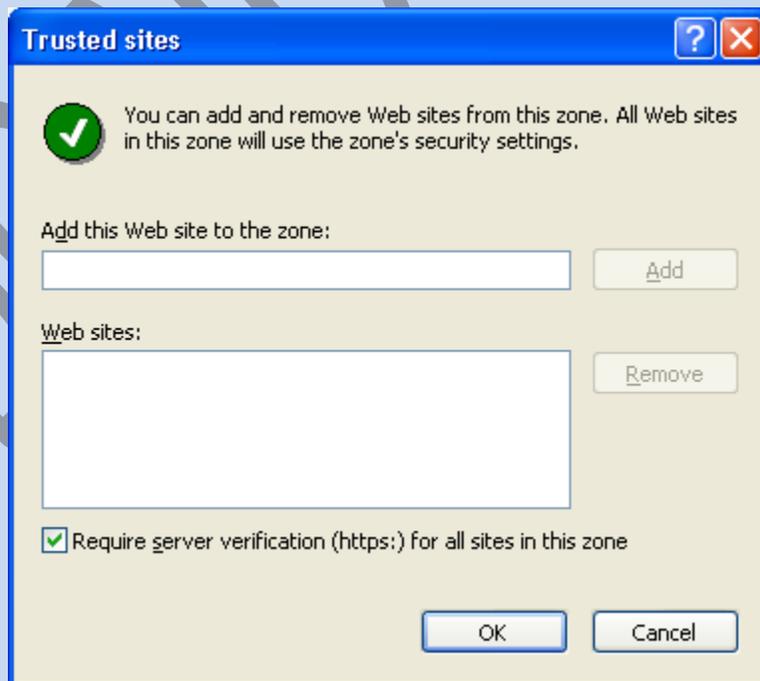
DO NOT COPY

6) **Update IE Trusted Sites (one time only):**

- a) Add <https://SA.TRIPLER.amedd.army.mil> as a trusted site.



- Enter <https://SA.TRIPLER.amedd.army.mil>



7) **Install JUNIPER VPN Certificate:**

a) Install certificate from <https://SA.TRIPLER.amedd.army.mil/cac>

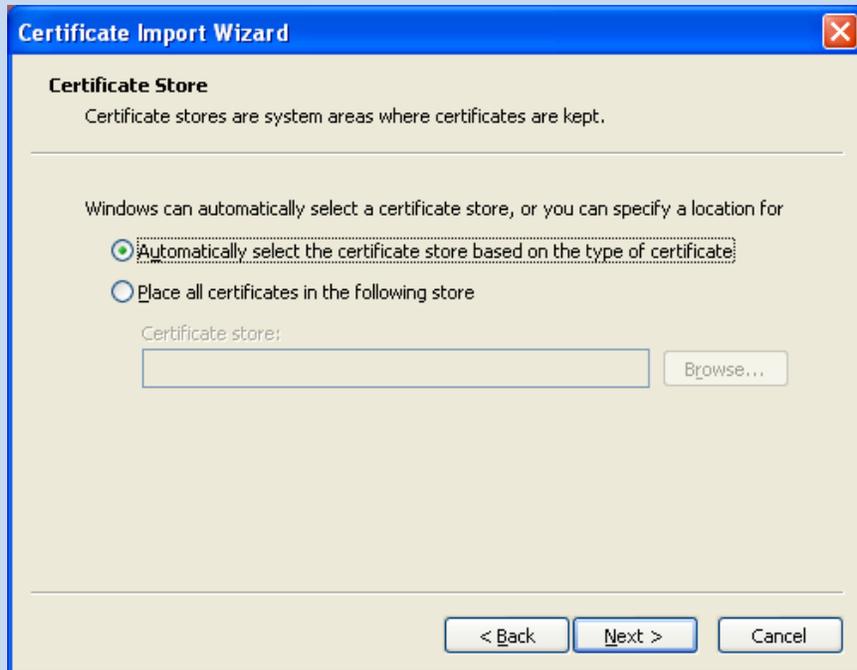
*\*You will get the popup below: Click "View Certificate"*



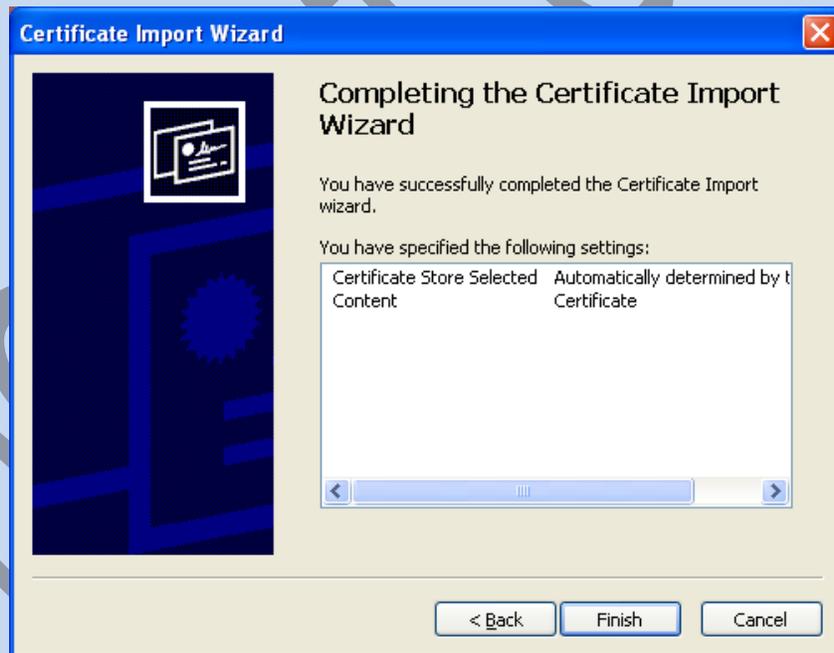
- Click "Install Certificate"
- Click "Next"



- Click "Next"



- Click "Finish"



- Click "Yes"



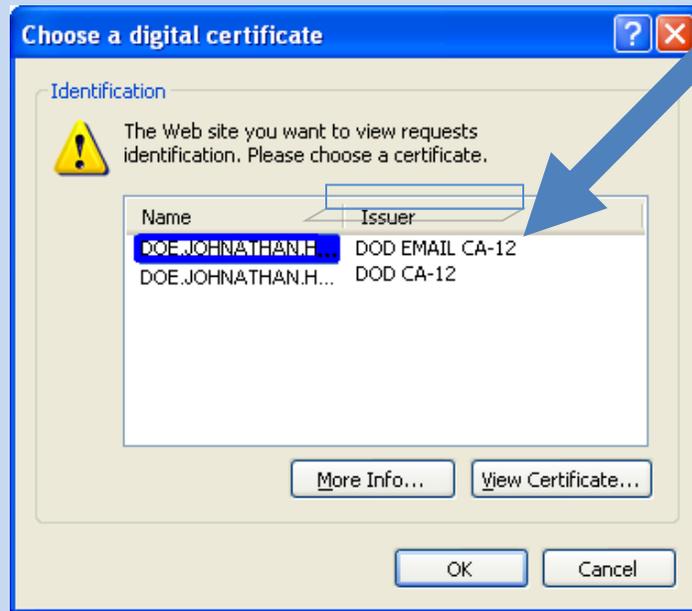
- Click “Yes”



## 8) Connect to the TAMC Network:

- a. Launch IE and type <https://SA.TRIPLER.amedd.army.mil/cac> in the address space.
- b. Your system will be placed in a **Secure Virtual Workspace (SVW)** environment and Host Checker will validate your system. Choose yes to all prompts to load modules.

- c. If your system passes the Host Checker, you will be prompted for your CAC credentials. Select your **EMAIL** certificate as indicated in the screenshot below.



- d. Enter PIN



*Wait for all modules to load...*

- e. After Network Connect has completed, you can launch Remote Desktop Connection and enter the IP address or hostname of the server you support.

**TIPs:**

- Unable to connect?
  - Ans: Your machine must be in Secure Virtual Workspace (SVW) to successfully connect to Juniper. If you do NOT have the yellow/gold padlock shown at your taskbar, then you are not connected to Juniper.
- Unable to login. Access Denied.
  - Ans: Ensure you have entered your PIN# correctly.

- I am prompted with username/password when trying to RDP to the server.
  - Ans: Upgrade to Windows XP SP3.
- Host Checker keeps loading.
  - Ans: Host Checker files are corrupted. Go to Add/Remove Programs from Control Panel and uninstall Juniper Networks Host Checker.
- **[NEW]** I am prompted with “**Please Wait...**”screen for the application to launch. It either launches or nothing happens.
  - Ans: This will require your local administrator to review the install.log and check for the following sequence of entry:

```
2011/10/04 11:03:43.819 1 dsVerifyHelper.cpp:184 - 'DSVerifyHelper::verify()'
Enter: C:\DOCUME-1\tester\LOCALS-1\Temp\JuniperSetupClientInstaller.exe
dsVerifyHelper.cpp:184 - 'DSVerifyHelper::verify()' WinVerifyTrust() failed,
800B010A
2011/10/04 14:58:04.833 1 dp59 - 'DSVerifyHelper::verify()' Enter:
C:\Documents
and Settings\tester\
Application Data\Juniper Networks\Setup Client\JuniperSetupDLL.dll
dsVerifyHelper.cpp:184 -
'DSVerifyHelper::verify()' WinVerifyTrust() failed, 8008010A
```

If the entry exists, user or the admin will have to download or install the VeriSign Class 3 Public Primary Certification Authority – G5. The certificate is available at [www.tamc.amedd.army.mil/Juniper](http://www.tamc.amedd.army.mil/Juniper).

- **[NEW]** Unable to import VeriSign Certificate. ERROR: The import failed because the store was read-only, the store was full, or the store did not open correctly.
  - Ans: Requires an administrator to complete the below instructions:
    - Launch certmgr.msc
    - Locate and Right-click Trusted Root Certificate
    - All Tasks
    - Import Browse and select **VeriSign Class 3 Public Primary Certification Authority - G5.cer**
    - Next
    - Browse
    - Select Trusted Root Certification Authorities folder
    - \*Show Physical Stores ~must be checked~
    - Select Local Computer
    - Ok
    - Next
    - Finish