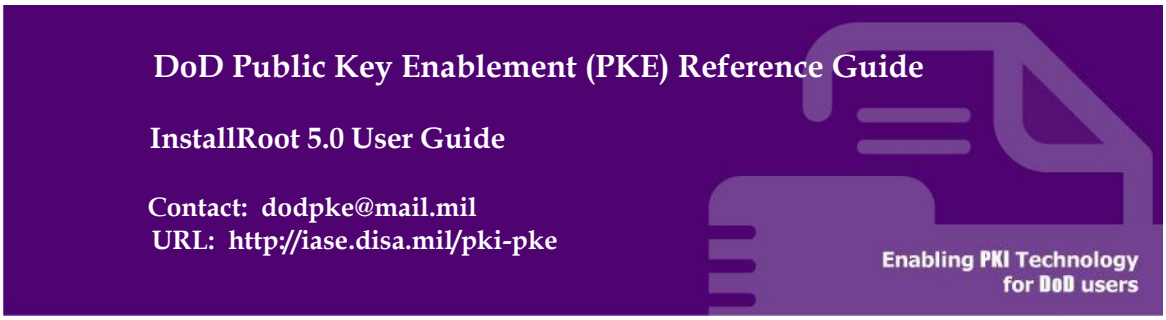


InstallRoot 5.0 User Guide for Unclassified Systems

7 December 2015

Version 1.0

DOD PKE Team

Revision History

Issue Date	Revision	Change Description
12/7/2015	1.0	Initial publication

Table of Contents

OVERVIEW **6**

INSTALLROOT 5.0 SYSTEM REQUIREMENTS **7**

PREREQUISITE SOFTWARE REQUIREMENTS 7
SUPPORTED OPERATING SYSTEMS 7
SUPPORTED BROWSERS 7
SUPPORTED NETWORK SECURITY SERVICE (NSS) 7

VERIFYING THE DIGITAL SIGNATURE OF INSTALLROOT **8**

INSTALLATION **10**

MIGRATING CONFIGURATION SETTINGS TO INSTALLROOT 5.0 11

INSTALLROOT 5.0 QUICK START GUIDE **12**

INSTALLROOT 5.0 INTERFACE INFORMATION 13

CONFIGURATION AND DEPLOYMENT OPTIONS **14**

CONFIGURING INSTALLROOT 14
Registry Configuration *14*
UI Configuration *14*
INSTALLING ENTERPRISE CERTIFICATES 14
InstallRoot Windows Service *14*
Command-line Utility *15*
CONFIGURING TAMP MESSAGE SOURCES 15
DISA source location *15*
Local Server Cache *15*

GETTING TO KNOW INSTALLROOT 5.0 ..... **16**

INSTALLROOT USER PRIVILEGES 16
NAVIGATING THE INSTALLROOT UI 16
Selecting Stores, Groups, and Certificates *17*
Viewing certificate information *17*
Managing certificate subscription and installation *17*

HOME TAB **18**

INSTALLING CERTIFICATES 18
ONLINE UPDATE 19
MANAGING PREFERENCES 19
SAVE SETTINGS 20
RESTART AS ADMINISTRATOR 20

STORE TAB **21**

ADDING AN NSS STORE 22
ADDING A JAVA TRUST STORE 23
ADDING AN ACTIVE DIRECTORY NTAUTH STORE 23
REMOVING A TRUST STORE 23
NTAUTH COMPARISON REPORT 24

GROUP TAB **25**

InstallRoot Group Types 25
Viewing the Digital Signature 26
Selecting a Group 26
Adding Certificate Groups 26
Editing Certificate Groups 27
Removing Certificate Groups 27
Subscribing Groups 27
Unsubscribing Groups 27

CERTIFICATE TAB **28**

Uninstalling Certificates 28
Managing individual certificate subscriptions 28
Exporting Certificates 29
Cleaning Certificates 29
Refresh Certificates 29

HELP TAB **30**

Help 30
About 30
Quick Start 30
Application and Service Logs 30

CERTIFICATE CLEANUP **31**

Locating Certificates 31
Certificates *31*
InstallRoot Stores *32*
Countries *32*
Sorting and Cleaning Certificates 32
Sorting Certificates *32*
Selecting Certificates *33*
Deleting Certificates *33*
Untrusting Certificates *33*
Exporting Certificates *33*

COMMAND-LINE UTILITY **34**

Preparation 34
Running InstallRoot with the Command-Line Utility 34
Using Commands 34
Installing certificates *34*
Removing Certificates *35*
Cache Clearing *35*
Managing Trust Stores *36*
Managing Groups *36*
Managing Individual Certificates *36*
Managing Logs *37*
Exporting certificates *37*
Managing Online Update Options *38*

UNINSTALLING INSTALLROOT **39**

RELEASE NOTES **40**

5.0 UI Changes 40
5.0 General Changes 40

APPENDIX A: SUPPLEMENTAL INFORMATION **42**

Web Site 42
Technical Support 42
Acronyms 42

APPENDIX B: LOG INFORMATION **44**

InstallRoot Error Logging 44
Windows Error Logging 45
Command-line Interface Exit Codes 46
InstallRoot Cache 49

APPENDIX C: INCLUDED CERTIFICATES **50**

DoD PKI Production Certificates 50
External Certification Authority (ECA) PKI Certificates 51
DoD Test PKI (JITC and O&M) Certificates 52

APPENDIX D: ACTIVE DIRECTORY INSTALLATION OVERVIEW **54**

Methods of deployment 54
Creating a distribution point 54
Create a Group Policy Object 55

APPENDIX E: USING INSTALLROOT IN DISCONNECTED ENVIRONMENTS **56**

Obtaining the Latest InstallRoot TAMP Message 56
Option 1: Direct Download *56*
Option 2: InstallRoot Update *57*
Redistributing the Latest TAMP Message 57
Option 1: Hosting the Latest TAMP Message on a Local Web or File Server *57*
Option 2: Placing the Latest TAMP Message Directly onto Workstations *57*
Configuring InstallRoot to Use the Local TAMP Message 57
Automatic Certificate Updates: Windows Service *58*
Manual Certificate Updates *59*

Overview

DoD Public Key Infrastructure (PKI) is built on a trust model which requires the establishment of a trust chain between an end entity certificate and a trusted root certification authority (CA). These root CA certificates are the basis for the trust relationship that must exist between servers and connecting clients, or any other application that uses certificates for digital signature or authentication. The certificate validation process verifies trust by checking each certificate in the chain from the end entity certificate to the root CA. If the root CA is not trusted, all other certificates in the chain, including the end entity certificate, are considered untrusted.

InstallRoot 5.0 installs DoD-specific root and intermediate CA certificates into trust stores on Microsoft servers and workstations, thereby establishing trust of the installed CA certificates. It can also manage DoD PKI CA certificates and other PKI CA certificates that may be necessary for conducting DoD business across a variety of certificate stores in a system. The contents of each certificate store dictate whether applications (such as web browsers, email clients, and document viewers) will trust a particular PKI and the certificates it issues.

A Graphical User Interface (GUI), Command-Line Interface (CLI), and the InstallRoot Windows Service are available to suit different user preferences and needs. Each version is contained within a single .MSI and is available from the DoD Public Key Enablement (PKE) web site at http://iase.disa.mil/pki-pke. Three .MSI installers are available: 32-bit, 64-bit, and a non-administrative (non-admin) version which does not require administrative privileges to install.

InstallRoot is available for both NIPRNet and SIPRNet. SIPRNet .MSIs for the application are available at http://iase.disa.smil.mil/pki-pke and come packaged with a SIPRNet version of this guide.

NOTE: The Windows Service feature is not included in the non-admin version of InstallRoot 5.0.

InstallRoot 5.0 System Requirements

Check the following system requirements before running InstallRoot 5.0 to ensure optimal performance.

Prerequisite Software Requirements

- .NET Framework version 3.5 SP1, 4.0, or 4.5.
- Microsoft Visual C++ redistributable.

  NOTE: The InstallRoot_v5.0-NonAdmin.msi does NOT include the required C++ redistributable packaged in the standard installers. The Microsoft Visual C++ redistributable may be downloaded at https://support.microsoft.com/en-us/kb/2977003.

Supported Operating Systems

- Windows XP (32 and 64-bit)
- Windows Vista (32 and 64-bit)
- Windows 7 (32 and 64-bit)
- Windows 8 and 8.1 (32 and 64-bit)
- Windows 10 (32 and 64-bit)
- Windows Server 2003 and 2003 R2 (32 and 64-bit)

  NOTE: Restricted mode not supported.
- Windows Server 2008 and 2008 R2 (32 and 64-bit)
- Windows Server 2012 and 2012 R2 (32 and 64-bit)

Supported Browsers

- Internet Explorer 7 and above
- Firefox 12 to 42
- Google Chrome 33 to 46

Supported Network Security Service (NSS)

- Version 3.17.2

NOTE: InstallRoot has been tested to function on all listed supported platforms; other platforms may work but have not been tested.

Verifying the Digital Signature of InstallRoot

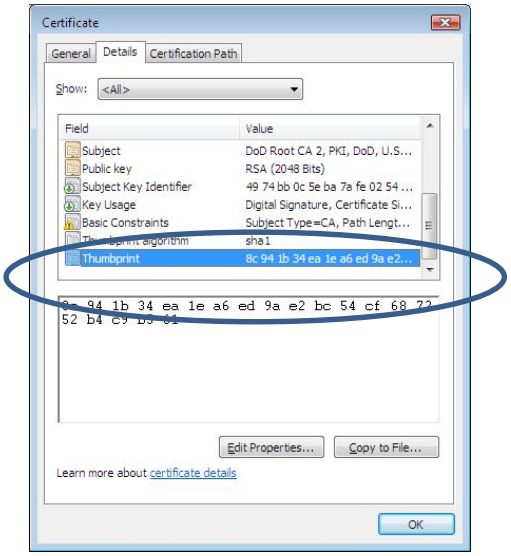
Before proceeding with installation, verify that the installer (.MSI file) has been digitally signed by DoD PKE Engineering. Use the following steps to verify the digital signature:

1) In Windows Explorer, navigate to the directory containing the **InstallRoot_v5.0.msi**, **InstallRoot_v5.0x64.msi**, or **InstallRoot_v5.0-NonAdmin.msi**.
2) Right-click the .MSI file and select **Properties** from the options menu to open the Properties window.
3) Select the **Digital Signatures** tab.
4) Select "CS.DoD PKE Engineering.DoDPKE60003" in the Signature list and click **Details**. This will open the **Digital Signature Details** window.

   NOTE: If DoD Root CA 2 is already installed the message "This digital signature is OK" should display when checking the signature on a machine with the DoD production PKI certificates installed.

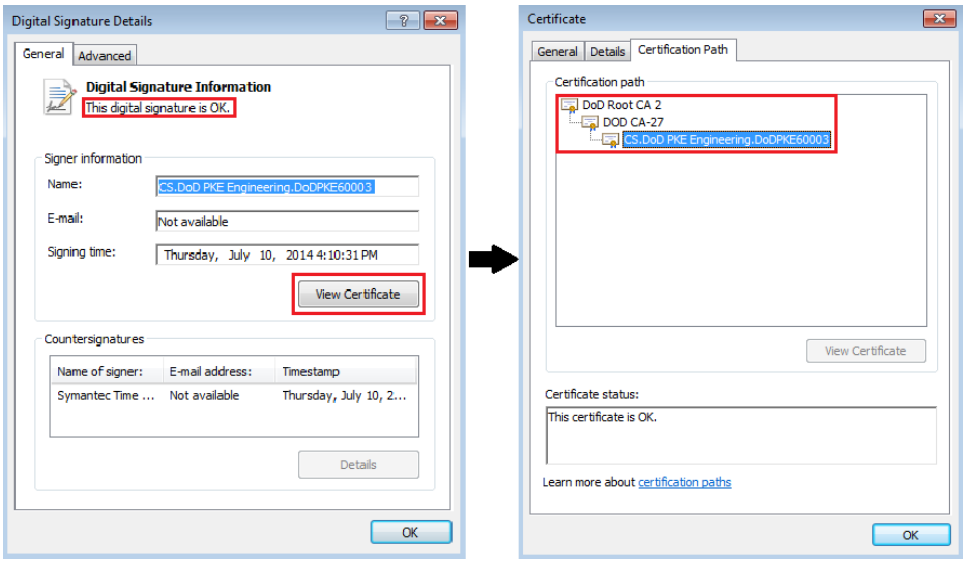
   If DoD Root CA 2 has NOT been installed the message "This signature is untrusted" will display. Perform the following steps to verify the signature should be trusted:

   a) In the **Digital Signature Details** window, click **View Certificate**.
   b) On the **Certificate Path tab**, select **DoD Root CA 2** and click **View Certificate**. Select the DoD Root CA 2 certificate's **Details** tab and scroll to the bottom of the window to view the thumbprint.
   c) Verify the DoD Root CA 2 thumbprint by calling the DoD PKI at (844) 347-2457 or DSN 850-0032.



5) Close the DoD Root CA 2 certificate. If it is not already open, view the CS.DoD PKE Engineering.DoDPKE60002 certificate by clicking **View Certificate** in the **Digital Signature Details** window. Select the **Certification Path** tab to verify the certification path reads "DoD Root CA 2 > DoD CA-27 > CS.DoD PKE Engineering.DoDPKE60003."

NOTE: If the digital signature is not OK, do NOT proceed with installation as the version of the tool may not be authentic.



6) Click **OK** in each of the three open properties windows to close them.

Installation

Use the following steps to install the application on an individual machine. For information on installing the application using an Active Directory Group Policy Object (GPO), see **Appendix D: Active Directory Installation Overview**.

NOTE: Please uninstall any previously installed versions of InstallRoot before proceeding. Configuration changes made using previous versions of InstallRoot will be removed upon uninstallation. See the "Migrating Configuration Settings to InstallRoot 5.0" section for additional details on recovering and importing these settings.

1) After verifying the correct digital signature on the desired InstallRoot .MSI file (see **Verifying the Digital Signature of InstallRoot**), double-click **InstallRoot5.0.msi**, **InstallRoot5.0_x64.msi** or **InstallRoot5.0_non-admin.msi** to launch the installation wizard.

   See the **InstallRoot 5.0 System Requirements** section to ensure the proper software requirements are met for the MSI chosen.

   NOTE: SIPRNet versions of the application are also available. SIPRNet .MSIs for the application are available at http://iase.disa.smil.mil/pki-pke and come packaged with a SIPRNet version of this guide.

2) On the Welcome screen of the wizard, click **Next**.

3) On the Choose a file location screen of the wizard, enter the desired installation location for InstallRoot and click **Next**. The default path for both versions of InstallRoot 5.0 is:

   C:\Program Files\DoD-PKE\InstallRoot

4) On the InstallRoot Features screen of the wizard, check the features desired for installation. By default, all features will be installed. Unless there is a specific reason not to install a feature, it is recommended that all features are selected and installed.

   NOTE: The option to install the Windows Service feature is not present in the non-admin version of InstallRoot 5.0.

5) On the Begin Installation screen, click **Install** to install the program. If prompted, click **Yes** in the Microsoft User Account Control (UAC) window to allow the installer to run with administrative rights.

6) When the wizard completes installation, click **Close** to exit or **Run InstallRoot** to launch the GUI.

Migrating Configuration Settings to InstallRoot 5.0

Uninstalling InstallRoot 4.1 or other previous InstallRoot versions will remove the configuration information from the registry. Use the following steps to migrate those settings to InstallRoot 5.0.

1) Export the current InstallRoot 4.1 configuration settings.
   a) Run the **Registry Editor** (regedit.exe) with administrative rights.
   b) Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\DoD-PKE\InstallRoot\4.1.
   c) Right-click the 4.1 Key and select **Export.**
   d) Save the registry file with a familiar name such as *Install_Root_41_settings.reg* to an easily accessible location.
   e) Close the Registry Editor.
2) Uninstall InstallRoot 4.1.
   a) Navigate to the Control Panel.
   b) Select **Uninstall Programs.**
   c) Uninstall *InstallRoot 4.1* (or another previous version).
3) Import the saved settings created in Step 1.
   a) Navigate to the location where the registry settings file was saved from Step 1.
   b) Double-click the file to apply the settings to the registry.

      NOTE: Double-clicking will prompt Microsoft's UAC to ask for permission to allow this file to make changes to the machine. Select "Yes" to continue.

   c) The registry editor will prompt with a warning about making changes to the system. Select "**Yes**" to continue.
   d) The Registry Editor will acknowledge that the Keys and Values have been added to the registry. Select **Ok** to confirm.
4) Install InstallRoot 5.0.
   a) Install InstallRoot 5.0 using the .msi file appropriate for the system. For instructions, see the **Installation** section of this guide.
   b) The installer will migrate the settings in the registry to the new key created with the installation of InstallRoot 5.0
5) Right-click the InstallRoot 5.0 application and select **Run as administrator**.

InstallRoot 5.0 Quick Start Guide

Upon first use, the InstallRoot 5.0 **Quick Start Tutorial** on installing certificates will launch automatically. After the initial run, the tutorial can be re-launched at any time from the **Help** tab of the InstallRoot GUI.

1) By default, InstallRoot will launch without administrative privileges. This will open the *Microsoft Current User* trust store upon launch and limit some features of the tool.

   To launch InstallRoot with administrative privileges, right-click and select **Run as Administrator** or, if InstallRoot is already open, select **Restart as Administrator** from the InstallRoot **Home** tab. This will launch InstallRoot and open the *Local Computer Certificate Store* instead of the default *Microsoft Current User Store.* See the **InstallRoot User Privileges** section for additional information on Administrator features.

2) InstallRoot will scan for new NSS or Java stores upon startup**.** Click **Yes** to add any new stores detected to InstallRoot. By default, InstallRoot will combine all known NSS or Java store locations into a single store, known as a **Multi-Store**. Stores may be added individually or as multi-stores using the **Add** button in the **Store** tab.

3) Use the **Store** and **Group** tabs to **Add, Remove,** or toggle **Subscriptions** for each. Administrator rights and domain access are required to add the NTAuth store. To modify the online update locations for each group, use the **Edit** button. Select **Restore defaults** to restore the default DoD, ECA, and JITC groups to a trust store.

4) **Subscribe**, **Export**, and **Uninstall** certificates in the **Certificates** tab. Use **Certificate Cleanup** to filter and remove problematic certificates from configured InstallRoot stores. See the **Certificate Cleanup** section for more information.

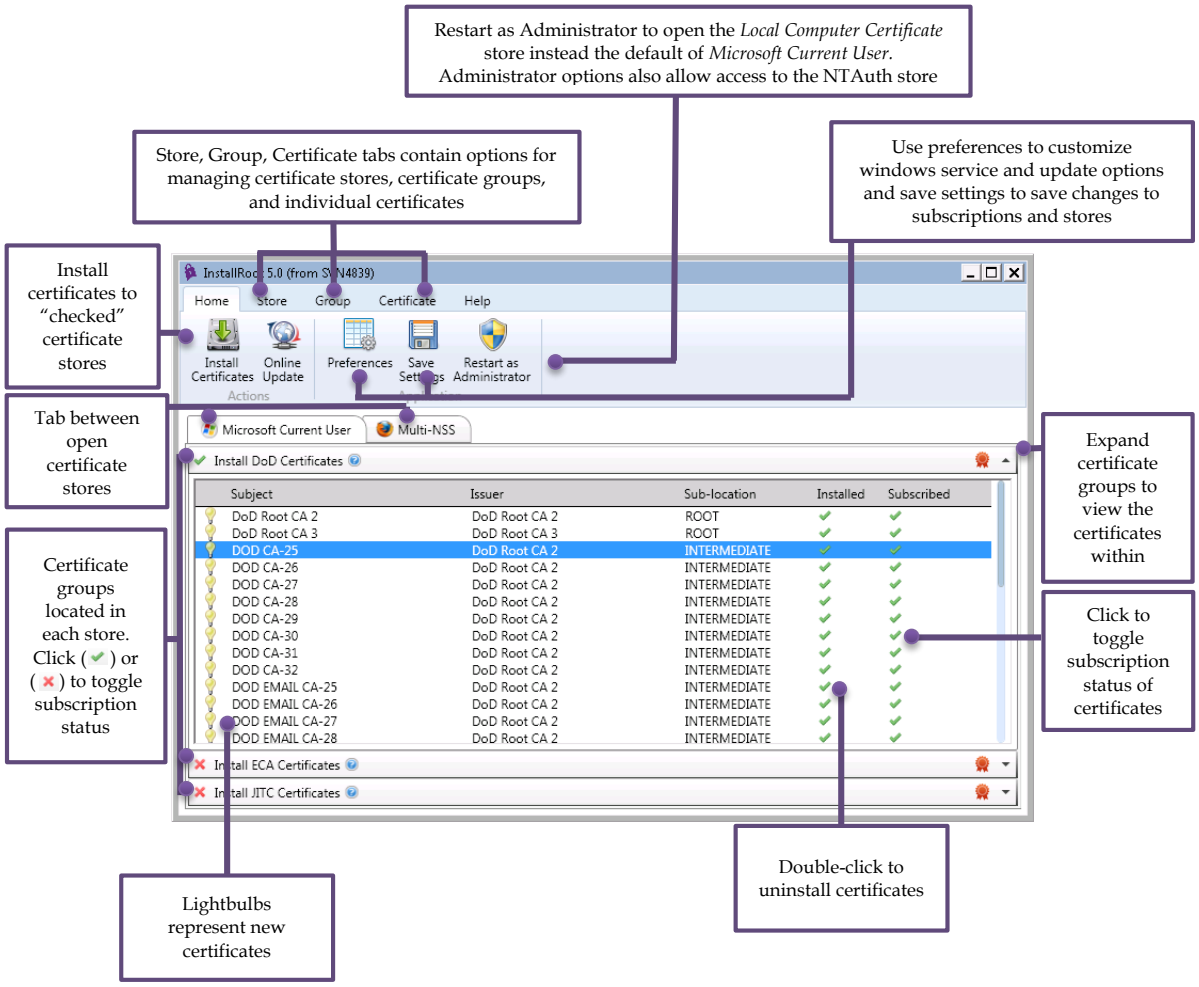
5) To install certificates, click the certificate store and ensure the store is subscribed (✔) to the desired certificate groups or individual certificates. Subscriptions to certificate groups and individual certificates may be toggled by selecting the (✔) and (✖) icons located next to each group or certificate name, or by using the functions located in the corresponding **Group** or **Certificates** tab.

   Once ready, select **Install Certificates** from the **Home** tab.

6) Use Online Update to check for new Trust Anchor Management Protocol (TAMP) messages from the Information Assurance Support Environment (IASE) website. Online updates may occur automatically by selecting the setting in the **Preferences** window. For more information on TAMP messages, see the Online Update section.

7) Use **Preferences** to customize automatic online update timing, add proxy servers and ports, or modify the windows service. Select **Save settings** to save any subscription changes to individual certificates or certificate groups, as well as any changes to certificate stores.

InstallRoot 5.0 Interface Information



Configuration and Deployment Options

InstallRoot 5.0 has been designed with a number of flexible deployment options, allowing for multiple ways of configuring the application, installing certificates, and customizing TAMP message sources across a variety of network workstations.

NOTE: Information on deploying InstallRoot in a disconnected environment is available in Appendix E: Using InstallRoot in Disconnected Environments.

Configuring InstallRoot

Registry Configuration

Administrators in enterprise environments may wish to use the registry to configure InstallRoot across a large number of workstations. Use the registry keys found under the HKLM\Software\DoD-PKE\InstallRoot registry to deploy to other workstations.

UI Configuration

InstallRoot users with administrative privileges may make configuration changes using the InstallRoot UI. Administrative privileges allow access to features such as Windows service management, NTAuth store, and the local computer certificate store. See the **InstallRoot User Privileges** section for more information about access and features for configuration.

Installing Enterprise Certificates

InstallRoot Windows Service

The windows service is the primary method for certificate installation within InstallRoot and can be configured using the InstallRoot UI provided a user has administrator privileges. When running, the service will check for updated InstallRoot TAMP messages at the interval specified by the **Perform online check after** interval. This setting can be modified in the Error! Reference source not found. section of the **ome** tab. Notifications for the service will be sent to the **Windows Event Log** in the DoD-PKE InstallRoot folder. See the **Windows Error Logging** section for more information.

Instructions for starting and stopping the service are described in the Managing Preferences section of this document. An administrator can also control the service directly by using the **Services MMC** (services.msc) in Windows.

NOTE: By default, the InstallRoot 5.0 service runs using the Local System Account which usually does not have permissions to access files located on network shares. If using InstallRoot 5.0 to access TAMP messages located on network file shares, the account used by the InstallRoot service may need to be updated to one that has the correct permissions.

Command-line Utility

Organizations who want to use user logon scripts to update certificate installations across multiple workstations may also use the --update argument of the command-line. This command will pull new InstallRoot TAMP messages from the DISA IASE. See the **Command-line Utility** section for more information.

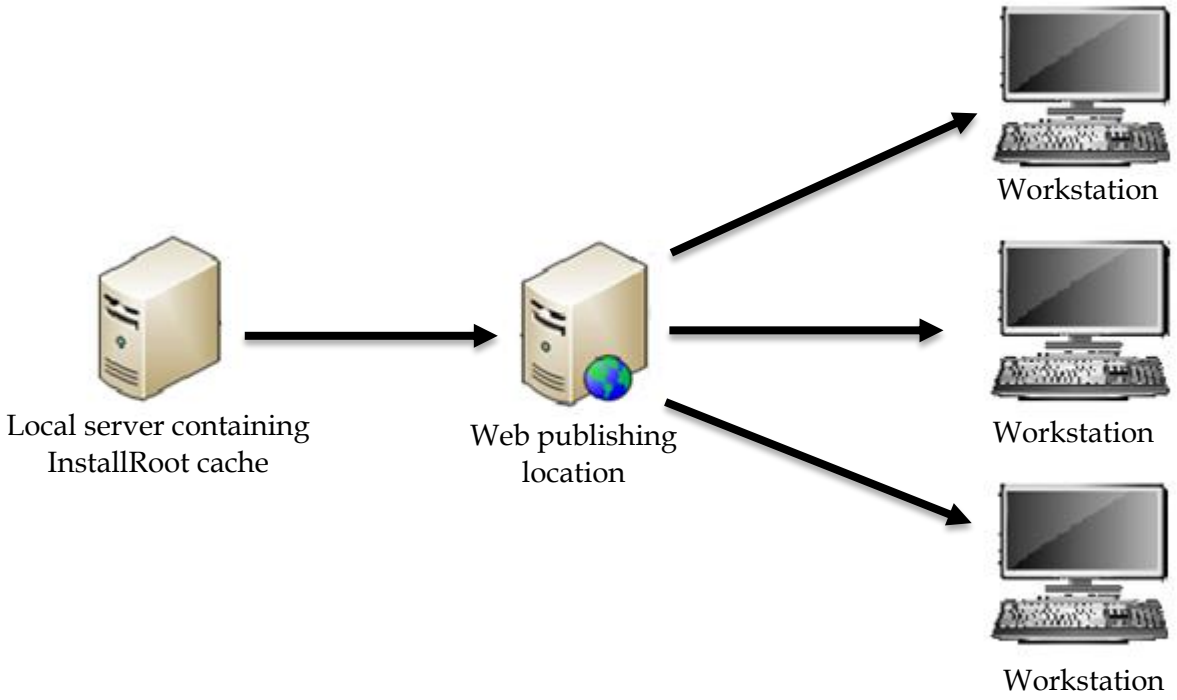
Configuring TAMP Message Sources

DISA source location

During an Online Update, InstallRoot checks for new InstallRoot TAMP messages on the IASE website. This is the default source location for InstallRoot TAMP message updates. See the **Editing Certificate Groups** section for instructions on configuring a new source location for InstallRoot TAMP messages.

Local Server Cache

Organizations who want to use a local server to cache TAMP messages have the option to do so with InstallRoot 5.0. A server may be used to host the InstallRoot TAMP message (.ir4 file) cache which may be copied to a new location for web publishing. Once published, local workstations running InstallRoot 5.0 may be pointed to that location to download TAMP messages. The figure below depicts a high-level deployment example of how InstallRoot might be used with a local cache server.



Getting to Know InstallRoot 5.0

InstallRoot User Privileges

It is important to note that InstallRoot 5.0 may be launched as two different versions:

1) A non-admin version that can be installed by a non-privileged user. If InstallRoot is launched without administrative privileges, the *Current User Certificate Store* will be opened by default, making certificates available only to the current user.

   NOTE: The non-admin version of InstallRoot 5.0 does not include the Windows Service functionality.

2) An administrator version which provides full functionality but requires administrative privileges. Administrator features include access to Windows service management, NTAuth store, NTAuth comparison reports, and Windows service log files. If InstallRoot is launched with administrative privileges, the *Local Computer Certificate Store* will be opened by default.

   The NTAuth Store may only be managed if the administrator is logged onto a domain-joined machine as a Domain Administrator. The NTAuth store will be disabled if both of these criteria are not met.

   Right-click and select **Run as Administrator** to open the administrative version of InstallRoot. To switch to the administrator version after having already opened InstallRoot as a non-admin, select the **Restart as Administrator** button from the **Home** tab of the interface.

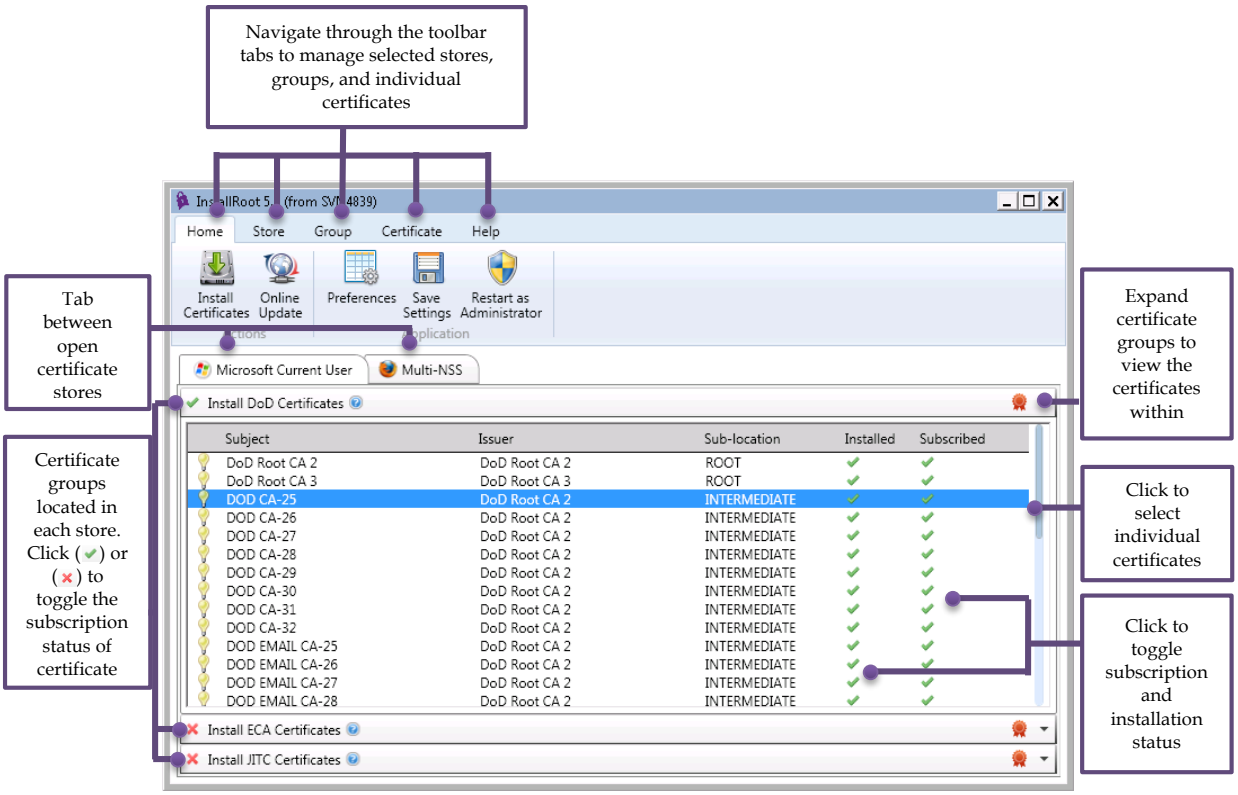
   NOTE: If Microsoft certificates are installed first by an unprivileged user and then an administrator, two copies of the Microsoft certificates will appear in the unprivileged user's Microsoft certificate store.

Navigating the InstallRoot UI

The InstallRoot 5.0 UI contains a tabbed listing of **Certificate Stores** that InstallRoot is configured to manage. Within each store is a listing of **Certificate Groups**, each of which may be expanded to show a detailed listing of certificates within each group.

Each tab on the ribbon command bar contains buttons for performing different types of actions with the **Certificate Stores**, **Certificate Groups**, and individual certificates displayed in the main pane.

Upon launching InstallRoot 5.0, the **Home** Tab screen will be displayed by default.



NOTE: If run as an administrator, InstallRoot will open the *Microsoft Local Computer* store. The Restart as Administrator button will no longer be visible.

Selecting Stores, Groups, and Certificates

1) A certificate group or individual certificate must first be selected before they can be installed.
2) To select a certificate group, click its name.
3) To select an individual certificate within a group, expand the certificate group and click the desired certificate.

Viewing certificate information

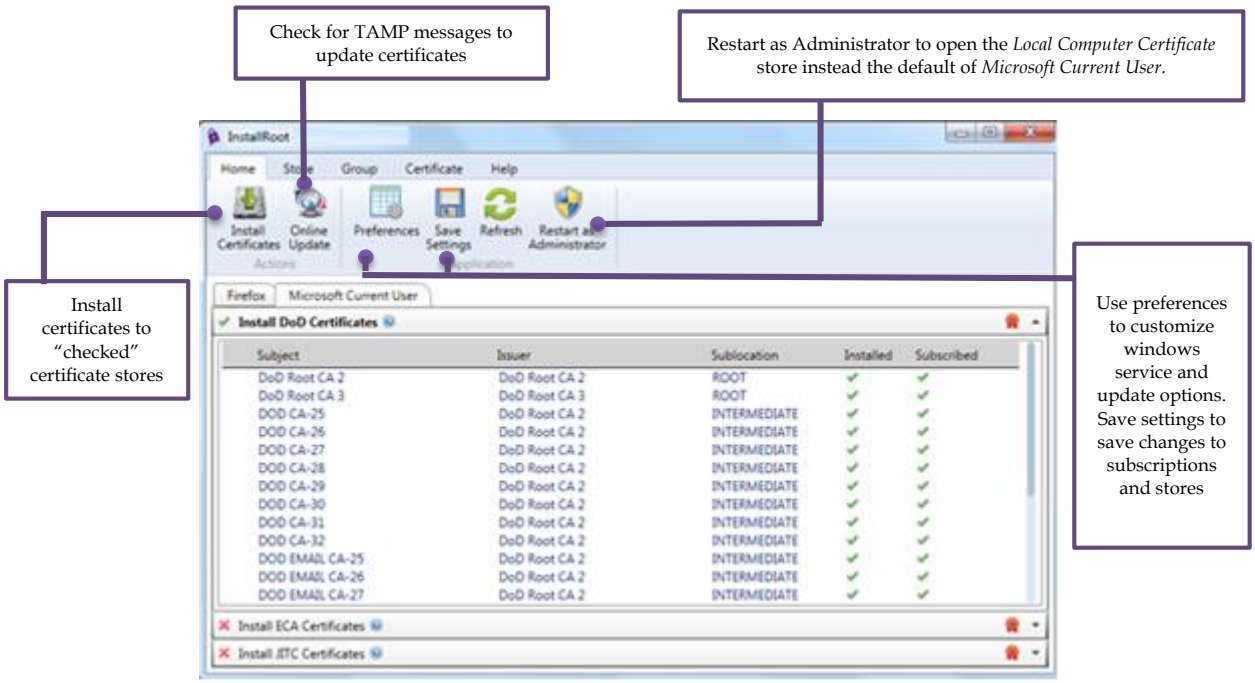
1) Tab between certificate stores to view the certificate groups under each.
2) Click the drop-down arrow of each certificate group to view individual certificates.
3) Double-click any individual certificates within a certificate group to view the certificate properties.

Managing certificate subscription and installation

1) The subscription and installation status for both certificate groups and individual certificates within each group can be toggled by clicking on its subscription indicator (✔) or (✖).

Home Tab

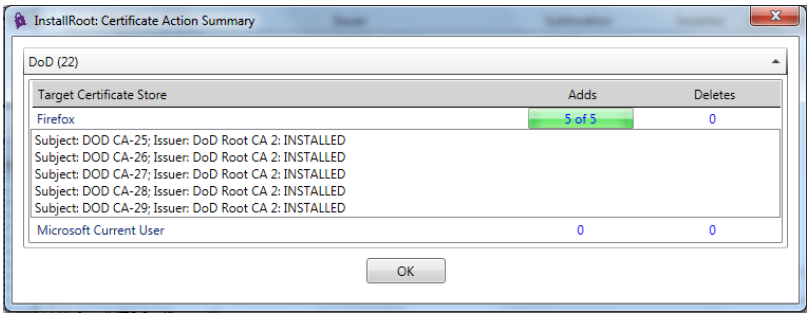
The Home tab is the first tab of the InstallRoot toolbar and contains the primary functions of InstallRoot.



Installing Certificates

To install certificates to a trust store, subscribe to the relevant certificate groups by selecting the (✔). This will mark the certificates contained within for installation. The subscription status for individual certificates may also be toggled in the same manner. Once the desired groups and certificates have been subscribed, select **Install Certificates**.

Once installed, the results of the installation will be displayed in the **Certificate Action Summary** window shown below:



NOTE: The desired subscriptions must be configured individually for each trust store before the subscribed certificates will be installed for each.

Important! An NSS store cannot be modified while an application that uses it, such as Firefox or Thunderbird, is running. If InstallRoot is launched or a request to install certificates is issued while an NSS application is running, a warning will be displayed and the operation will not be performed. To update the NSS store, close all applications using that store and then perform the desired operation. Contact the system administrator if unsure of the application(s) using the NSS store on the system.

Online Update

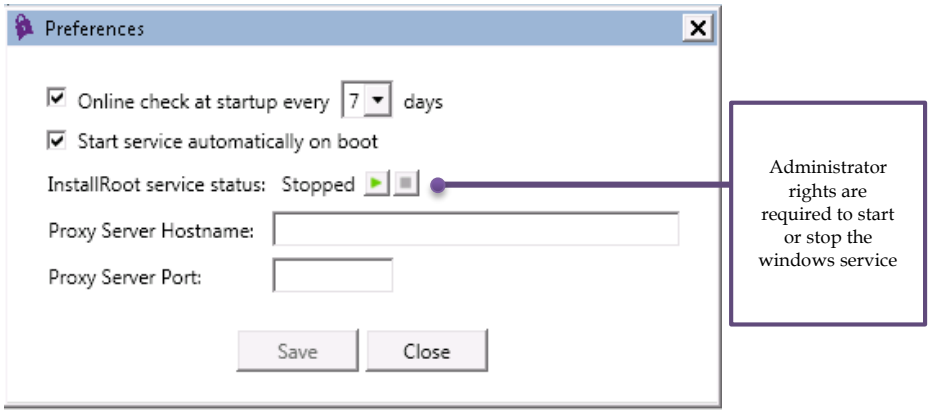
InstallRoot checks for and accepts TAMP messages in order to update certificate information within the tool. TAMP messages are digitally signed files containing CA certificates and associated instructions (such as add or remove) that can be used by InstallRoot to update trust stores.

Select **Online Update** to check if there are new InstallRoot TAMP messages available and, if so, download and process the messages. By default, InstallRoot will check for new messages coming from the IASE website. This location may be changed using the group **Edit** button located in the **Group** tab. See **Editing Certificate Groups** for more information.

NOTE: Online Update requires internet access. Online updates will happen automatically if the InstallRoot service is running, but can be performed manually if desired.

Managing Preferences

InstallRoot 5.0 contains several options for update scheduling and customizing windows service preferences.



- **Online check at startup**: If selected, InstallRoot will check to see if an online update needs to be performed when the application is launched.
- **Perform online check after:** Specifies the length of time that InstallRoot should wait between performing online update checks.

  NOTE: When running as an administrator, this setting is shared between the InstallRoot GUI and the Windows Service. If an online update is performed by either application, the interval will be reset. Updates for the default certificate groups do not occur very frequently; approximately once every six months for DoD.

  NOTE: To configure the following options, InstallRoot must be run as an administrator. See *Restart as Administrator* **for more information.**
- **Start service automatically on boot:** Indicates whether the InstallRoot service is set to start automatically**.** If InstallRoot is being run as a user without administrative privileges, the option will be greyed out but will display the current configuration.
- **InstallRoot Windows Service**: A status message will indicate whether the InstallRoot Windows service is **Running** or **Stopped**. Use the play (▶) and stop (■) buttons to start and stop the service accordingly.
- **Adding a proxy server hostname:** If desired, a proxy server hostname may be specified in the text field.
- **Adding a proxy server port:** If desired, a proxy server port may be specified in the text field.

Save Settings

Selecting **Save Settings** will save any changes that have been made to certificate subscriptions, added certificate stores, or to the InstallRoot UI.

Restart as Administrator

Use **Restart as Administrator** to restart the application with administrative privileges. Administrator features can be found in the **InstallRoot User Privileges** section. Clicking this button provides the same functionality as launching InstallRoot by right-clicking the program and selecting **Run as administrator**.

NOTE: Users restarting as an administrator will be prompted for the proper credentials prior to opening InstallRoot as an administrator. Any settings that were selected when running without administrative privileges are not preserved when the tool is re-launched with administrative privileges.

Store Tab

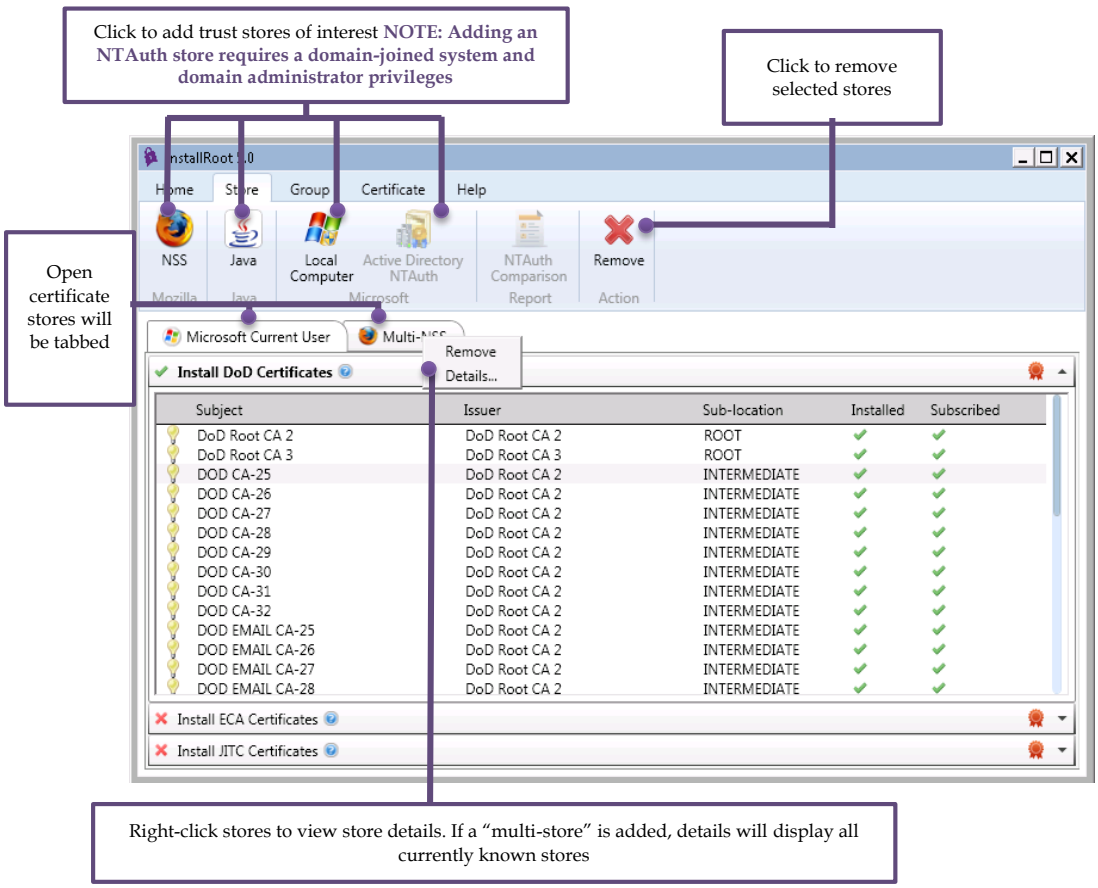
The **Store** tab displays options for managing the three types of certificate trust stores in InstallRoot:

- NSS stores are used by Mozilla Firefox, Thunderbird, and Apache web server when run with mod_nss. InstallRoot supports NSS stores with passwords and in FIPS mode.
- Java key stores are contained in Java Runtime Environment (JRE) and Java Development Kit (JDK) installations, which are used for the basis of trust for Java applets running in web browsers and for Java apps.
- The Microsoft Current User and Local Computer (Administrator only) stores control which PKIs Microsoft applications (e.g. Internet Explorer, Microsoft Outlook, etc.) trust. Many third-party applications that run on Microsoft operating systems (e.g. Google Chrome) also use the Microsoft certificate stores.

If InstallRoot is being run as a user without administrative rights, the **Microsoft Current User** store will be opened by default. Selecting the **Restart as Administrator** button will restart InstallRoot with administrative privileges and display the **Microsoft Local Computer** store.

- The Active Directory NTAuth store controls which PKIs can be used for domain smart card logon.

NOTE: A Microsoft trust store can be removed, but it will return upon restarting the GUI. If deleted and restarted, the group subscription information will need to be re-enabled.



Adding an NSS Store

1) Within the **Store** tab of the primary toolbar, select the **NSS** button.

2) The **Select an NSS Store** dialogue will appear and automatically present any Firefox or Thunderbird profiles that InstallRoot has found on the system. By default, InstallRoot will add all NSS profiles into a single multi-store.

   Stores may be added individually by selecting the **Manage a single (selected) NSS key store** option. If the desired NSS profile is not listed, use the **Browse…** button to navigate to the correct location.

   NOTE: If a NSS store is managed individually and it was part of a multi-store, that NSS store will be removed from the multi-store.

3) In the **New Store Name** field, choose a name for the NSS trust store. InstallRoot will suggest a name based on the application that uses it, which can be changed as desired.

4) Once the store's name and location has been determined, select **OK.**

Adding a Java trust Store

1) Select the **Java** button within the **Store** tab of the primary toolbar.

   The **Add a Java Store** dialogue will appear and automatically present any Java profiles that InstallRoot has found on the system. By default, InstallRoot will add all Java profiles into a single multi-store. This option is recommended for the simplicity of managing multiple stores at once. As new Java versions are installed on the computer, the multi-store will automatically find those new installations and manage the certificates appropriately.

   Stores may be added individually by selecting the **Manage a single (selected) Java key store** option. If the desired Java profile is not listed, use the **Browse…** button to navigate to the correct location.

   NOTE: If a Java store is managed individually and it was part of a multi-store, that Java store will be removed from the multi-store

2) In the **New Store Name** field, choose a name for the Java trust store. InstallRoot will suggest a name based on the Java store type, which can be changed as desired.

3) Once the store's name and location has been determined, select **OK.**

Adding an Active Directory NTAuth Store

NOTE: The machine running InstallRoot must be domain-joined, with the user running InstallRoot having domain administrator rights in order to add the Active Directory NTAuth store. To manage the NTAuth store, it is not necessary to run InstallRoot from a domain controller; just a machine in the domain.

1) Select the **Active Directory NTAuth** button within the **Store** tab of the toolbar.

2) Upon selection, a security window will appear warning that any actions in the NTAuth store impact the entire domain. Select **OK** to continue.

   NOTE: The Active Directory NTAuth button will be active so long as the machine is a member of a domain and the user has administrative rights. The NTAuth Store will be disabled if both of these criteria have not been met.

3) A new store called NTAuth will be created. The certificates in the NTAuth store can now be managed using the same procedures as for any other store types.

Removing a Trust Store

1) Select the tabbed store name desired for removal.

2) Click the **Remove** button located in the **Store** tab of the toolbar.

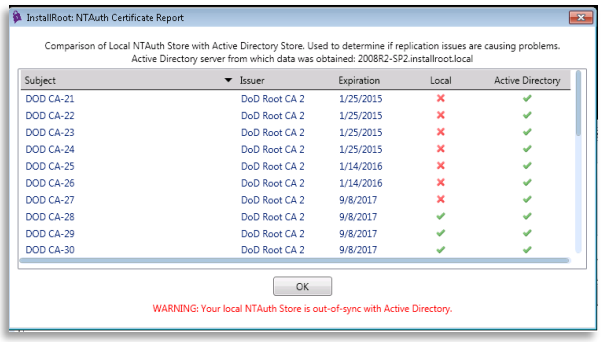
3) Confirm the removal.

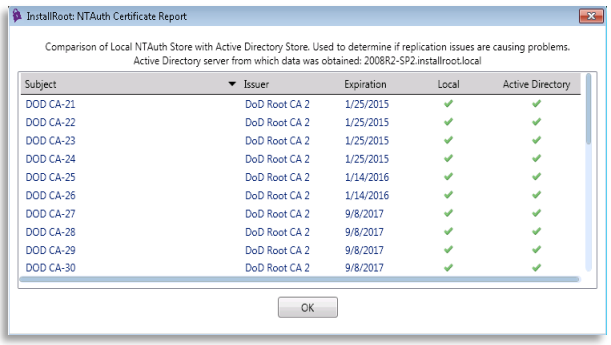
NOTE: InstallRoot may reopen stores which have been previously removed upon launch. Select *Save settings* before closing InstallRoot to prevent removed stores from opening upon future launches.

NTAuth Comparison Report

Once the NTAuth Store has been created, the **NTAuth Comparison Report** may be selected**.** The NTAuth Comparison report compares the local NTAuth store to Active Directory's NTAuth store. This report can quickly display replication inconsistencies between the two.

Below are two examples of the NTAuth Comparison report. The left example shows an out-of-sync condition. The right example shows that the machine is in sync with the Active Directory.

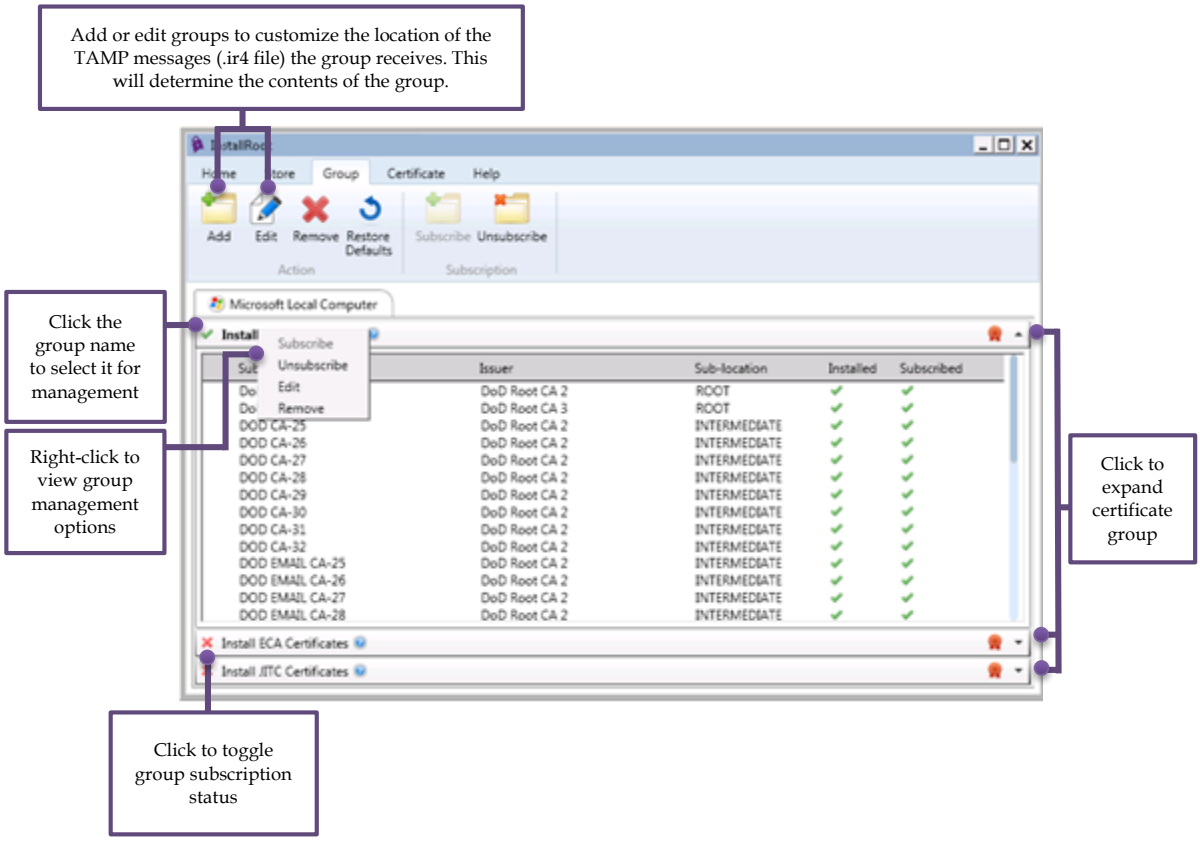




NOTE: It is recommended that an Active Directory sync be initiated before running the report, even on the domain controller. The easiest method to do this is to run `gpupdate /force` from the command-line as an administrator.

Group Tab

Certificate Groups are visible under each trust store tab. Each group is comprised of certificates and actions contained in an InstallRoot TAMP message. Groups may be expanded to view the individual certificates stored within.



InstallRoot Group Types

By default, the following groups are created in InstallRoot:

- **Install DoD Certificates:** Contains DoD PKI **production** CA certificates for the NIPRNet. DoD PKI certificates should be installed on all NIPRNet systems to establish trust of the DoD PKI.
- **Install ECA Certificates:** External Certification Authority (ECA) PKI certificates should be installed on all DoD NIPRNet systems that have a need to interact with DoD external partners. Installing ECA PKI certificates establishes trust of the ECA PKI, which issues certificates to DoD partners who do not possess Common Access Cards (CACs) or other DoD-approved external PKI certificates.

- **Install JITC Certificates:** Joint Interoperability Test Command (JITC) PKI certificates should ONLY be installed in test environments and NOT on operational systems. Installing JITC PKI certificates establishes trust of the JITC test infrastructures that replicate the DoD PKI capabilities and issue certificates for test and development purposes.

Viewing the Digital Signature

Select the ( ) button located on the far right of each certificate group to view the InstallRoot TAMP message signature details such as the signer, certificate chain, date, time, and signature algorithm.

Selecting a Group

1) Select a group by clicking the group name. Selected group names will be highlighted in bold.

   NOTE: Groups must be selected prior to using the edit, remove, subscribe, and unsubscribe functions located in the Group tab of the toolbar.

2) Click the ▼ button on the right side to expand a certificate group and view the certificates within that group. The certificate table lists the following certificate information:

   - **Subject :** The certificate subject common name (CN)
   - **Issuer:** The certificate issuer CN
   - **Sub-location:** The location where the certificate will be installed within the trust store
   - **Installed:** The certificate's installation status in the selected trust store (for installed or for uninstalled)
   - **Subscribed:** The certificate's subscription status in the selected trust store (for subscribed or for unsubscribed) - A certificate will be installed, deleted, or updated depending on the subscription status when the **Install Certificates** button is clicked.

   NOTE: Certificates listed in red are marked for deletion. These certificates will initially display as subscribed, but will display as uninstalled after running the Install Certificates action.

Adding Certificate Groups

1) Click the **Add** button within the **Group** tab of the toolbar.
2) When prompted, specify the **Location** of the group as desired. Administrators hosting InstallRoot TAMP files on a local server may wish to specify a local URI

from which InstallRoot pulls TAMP messages. This could be a network file system location or URL of an InstallRoot TAMP message (.ir4 file) that specifies the group's contents.

Editing Certificate Groups

Administrators hosting InstallRoot TAMP files on a local server may wish to customize the URI from which InstallRoot pulls TAMP messages. This is accomplished by editing certificate groups using the following steps:

1) Select the group to edit.
2) Click the **Edit** button. Alternatively, right-click the group name and select **Edit** in the menu that appears.
3) Type the new address of the InstallRoot TAMP message (.ir4 file) that specifies the group's contents in the **URI** field or use the **Browse** button to navigate to another address.
4) Press **OK** to confirm group edits.

Removing Certificate Groups

1) Click the group name desired for removal to select it.
2) Click the **Remove** button located in the **Group** tab of the toolbar.
3) Certificate groups may also be removed by right-clicking the group name and selecting **Remove** from the option list.

Subscribing Groups

Subscribing to groups will mark the certificates they contain for installation. Once subscribed to a certificate group, certificates will be installed after selecting **Install Certificates** from the **Home** tab.

1) Click the group name desired to select it.
2) Select the **Subscribe** button located in the **Group** tab of the toolbar. By default, the **Install DoD Certificates** group will be subscribed.
3) Groups subscriptions may also be toggled by selecting the (×) or (✔) icons located to the left of the group name.

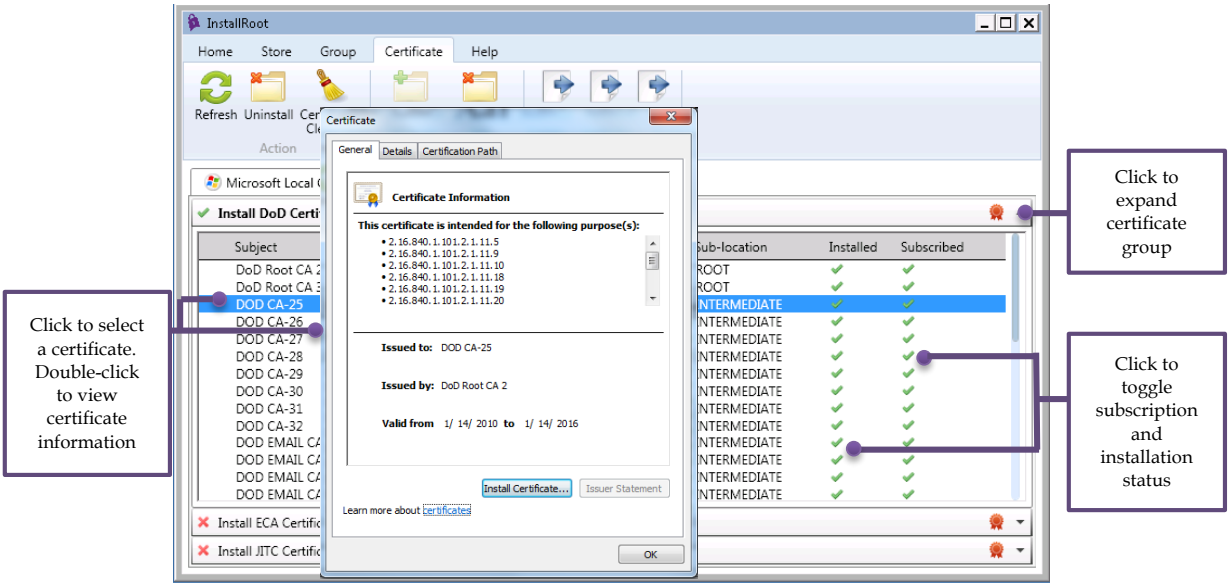
Unsubscribing Groups

1) Click the group name desired to select it.
2) Select the **Unsubscribe** button located in the **Group** tab of the toolbar.

NOTE: Unsubscribing will stop any future updates from being processed for that group, but will not uninstall certificates.

Certificate Tab

The **Certificate** tab displays options for managing individual certificates. Expand a certificate group by clicking the ▼ button located to the far right of the group name in order to view the individual certificates located within.



Uninstalling Certificates

To uninstall individual and/or multiple certificates from a selected trust store:

1) Navigate to the **Certificate** tab in the InstallRoot toolbar.
2) Select the appropriate trust store.
3) Select the **drop-down arrow** for the desired group to expand the list of certificates.
4) Select the certificate(s) to be uninstalled. **Ctrl+click** can be used to select multiple individual certificates and **Shift+click** can be used to select a list of adjacent certificates. Using **Ctrl+A** will select all of the certificates in the group.
5) Select the **Uninstall** button in the **Certificate** tab.

NOTE: Individual certificates may also be uninstalled by double-clicking the (✔) in the Installed column of the certificate grid.

Managing individual certificate subscriptions

Although it is recommended to manage subscriptions at the group level for most functions, individual certificate installation and subscription status may also be toggled.

To toggle the subscription status or installation of an individual certificate, click the (✖) and (✔) icons. Subscription status and installation can also be managed for individual

certificates using the **Uninstall**, **Subscribe**, and **Unsubscribe** buttons in the **Certificate** tab.

NOTE: Unsubscribing to an individual certificate will prevent that certificate from being installed.

Once the desired subscriptions have been configured, navigate to the **Home** button and click **Install Certificates.**

Exporting Certificates

To export certificates:

1) Select the **Certificate** tab in the InstallRoot toolbar.
2) Expand the desired certificate group and select the certificate(s) to be exported. **Ctrl+click** can be used to select multiple individual certificates and **Shift+click** can be used to select a list of certificates.
3) Select the **PEM**, **DER**, or **PKCS7** button, depending on the format desired.
4) In the pop-up window, specify the directory to which the certificate(s) should be exported and click **OK**.

   NOTE: When exporting as a PKCS7, please choose an appropriate name for the file. By default, InstallRoot will choose YYYY-MM-DD.p7b. (ex. 11-19-2015.p7b)
5) Click **Save**.

Cleaning Certificates

The certificate cleanup tool is a new feature within InstallRoot 5.0. Selecting this option will open a new window within InstallRoot for filtering and cleaning certificate stores. See the **Certificate Cleanup** section for more information.

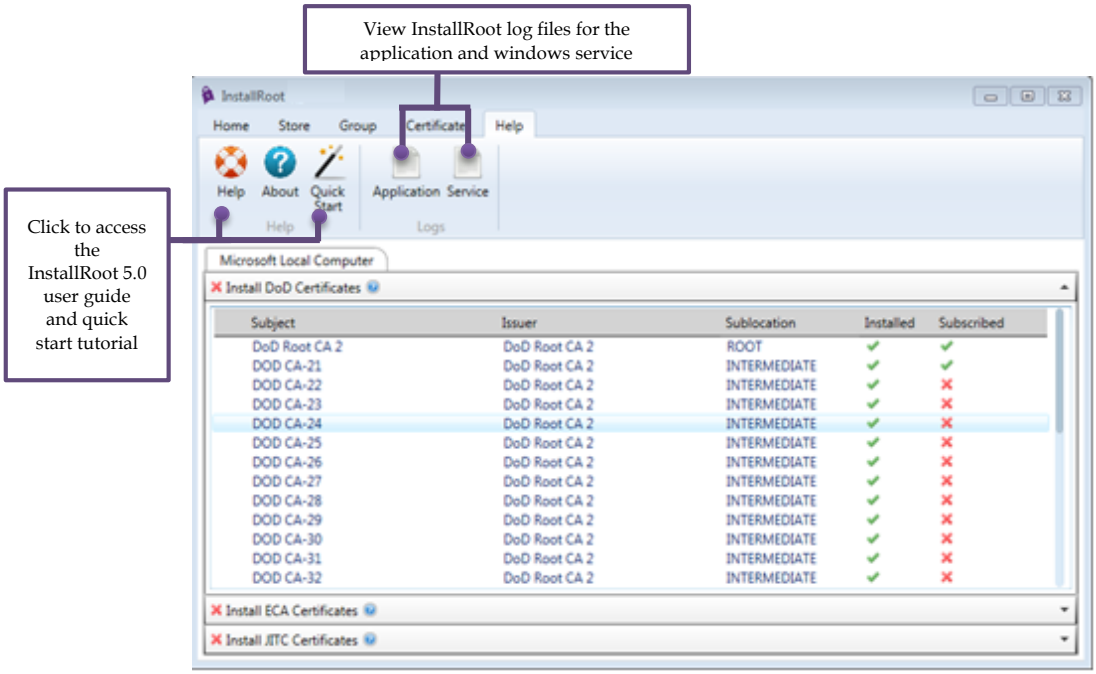
Refresh Certificates

Changes to subscription or installation status may cause some inconsistencies in the certificate UI list. Use the **Refresh Certificates** button to refresh certificate lists within the InstallRoot UI.

Help Tab

The help tab includes links to log files, the user guide, and the quick start guide.

Note: Administrative privileges are required to view windows service logs.



Help

Displays a PDF version of this user guide.

About

Displays the version number, the DoD PKE web site, and the DoD PKE email address.

Quick Start

Opens the InstallRoot Quick Start tutorial that is presented at the first use of the tool.

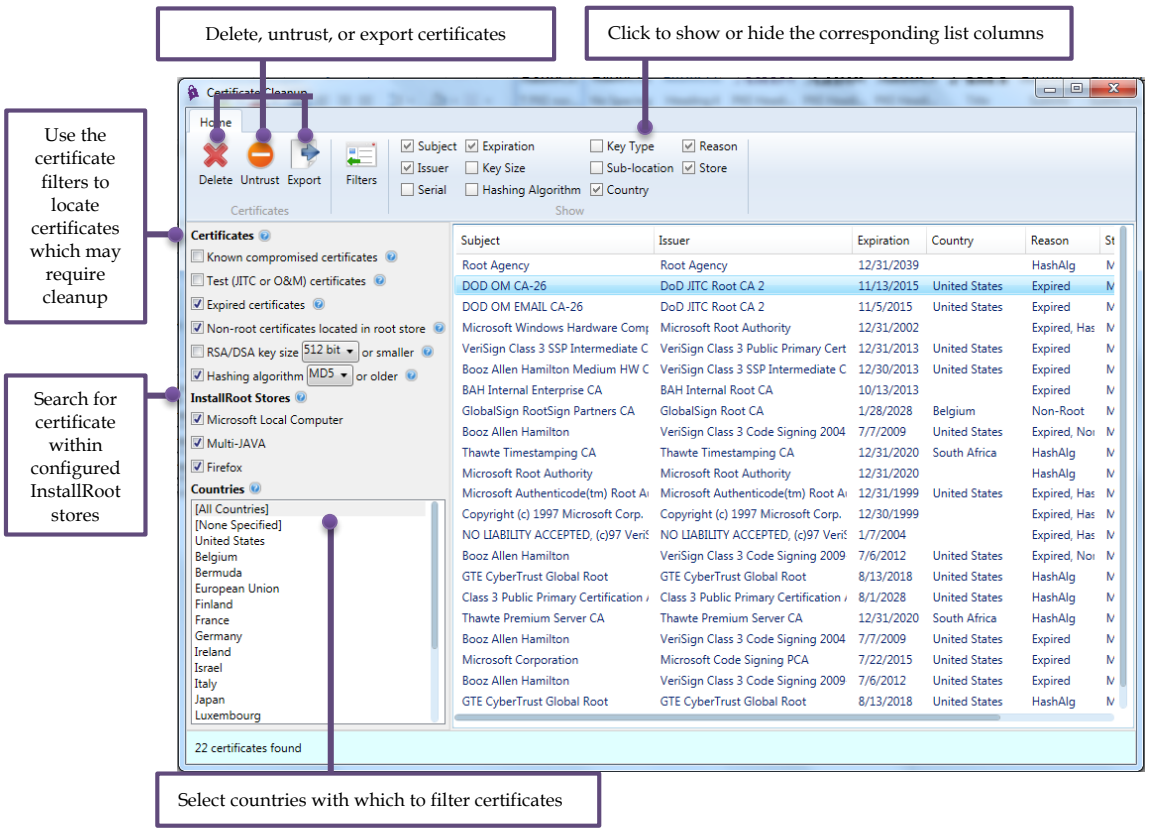
Application and Service Logs

This area will vary depending on the user's permissions. When running the tool with administrative privileges, both the **Application** and **Service** log buttons will be present. When running the tool without administrative privileges, only the **Application** log button will be present. For more information on logging, see **Appendix B: Log Information**.

Certificate Cleanup

The certificate cleanup function is a new feature in InstallRoot 5.0 designed to help remove undesirable certificates across any certificate stores configured within InstallRoot. Certificates may be deleted, exported, or untrusted using the cleanup tool.

To open the cleanup tool, select the **Certificate Cleanup** button located in the Certificates tab. This will open a new window alongside the primary InstallRoot UI.



Locating Certificates

The InstallRoot cleanup tool contains a variety of options for locating certificates which should be considered for cleanup.

Certificates

- **Known compromised certificates:** Check to locate compromised certificates known to DoD PKE. It is recommended to remove any compromised certificates found.

- **Test (JITC) certificates:** Check to locate test certificates. Test certificates (JITC) should not be installed on production systems and are recommended for removal.
- **Expired certificates:** Check to locate expired certificates. Users who validate historically signed documents may wish to keep expired certificates on their system.
- **Non-root certificates located in the root store:** Check to locate non-root certificates inappropriately located in the root store.
- **RSA/DSA key sizes 1024, 2048, 4096 or smaller:** Check to locate the selected RSA or DSA key sizes. Certificates using key sizes smaller than 1024 should be removed at the recommendation of the National Institute of Standards and Technology (NIST).
- **Hashing algorithms MD5, SHA 1, SHA 256 or older:** Check to locate the selected hashing algorithm type. Certificates using hashing algorithms MD5 or older should be removed.

InstallRoot Stores

The cleanup tool searches for certificates contained within configured InstallRoot stores. By default, all configured stores will be checked upon launch of the cleanup tool. Unchecking a store selection will prevent InstallRoot from locating any certificates within that store.

Countries

Select countries to view their certificates. Selected countries will serve as a basis for further certificate searches.

Sorting and Cleaning Certificates

Once located, certificates may be deleted, untrusted, or exported using the corresponding functions in the ribbon bar of the cleanup tool.

Sorting Certificates

Sort certificates by clicking on the desired column. Show or hide columns using the checkboxes located at the top of the ribbon bar. To maximize the size of the certificates list, hide the certificate filters panel using the ( ) button.

As users apply filters to the certificates list, take note that the **Reason** column displays why certificates may require cleanup. The reasons displayed are based off of what filter selections have been made by the user. The following certificate reasons may be shown:

- Compromised

- Expired
- Test
- Non-Root
- KeySize
- HashAlg
- Country

Selecting Certificates

Click to select a certificate, or select multiple certificates using **CTRL+click** and **SHIFT+Click**. Once certificates have been selected, they may be deleted, untrusted, or exported.

Deleting Certificates

Select the delete button (✖) to delete the selected certificates from the trust store.

NOTE: Deleting certificates using the cleanup tool will PERMANENTLY delete them from the trust store. It is recommended to backup certificates by exporting them to a PKCS#7 file before deletion.

Untrusting Certificates

Select the untrust button (⛔) to move certificates in Microsoft certificate stores to the untrusted sub-store. This function is only supported for Microsoft Local Computer and Microsoft Current User trust stores.

Because Java, NSS, and NTAuth stores do not have untrusted stores, an error message will be produced. InstallRoot will request certificates belonging to Java, NSS, and NTAuth stores be deleted as an alternative. This prevents the certificates from being trusted. It is recommended to backup any certificates before untrusting them by exporting to a PKCS #7 file.

Exporting Certificates

Select the export button ( ) to export certificates to a desired file location in PKCS #7 format.

Command-Line Utility

The command-line utility can be used to manage InstallRoot trust stores. The utility may be run locally, from portable media, or as a logon script. **Command-line Interface Exit Codes** are provided in **Appendix B: Log Information** to facilitate using the utility in batch scripts.

Preparation

For InstallRoot 5.0, the .MSI file must be used to install the command line utility. The utility requires .NET framework version 2.0 or above.

Running InstallRoot with the Command-Line Utility

To run the utility locally or from portable media:

1) In a command prompt, navigate to the directory containing the command-line executable. The default path is:

```
C:\Program Files\DoD-PKE\InstallRoot\
```

   NOTE: If the 32-bit version is installed on a 64-bit system, the CLI will be located in c:\program files(x86)\DoD-PKE\InstallRoot\ .

2) Enter the desired command arguments when running InstallRoot. See the **Using Commands** section below for available command arguments.

To run the utility as part of a logon script, see the **Microsoft Windows: Deploying DoD PKI CA Certificates Using Group Policy Objects** guide available on the DoD PKE website at http://iase.disa.mil/pki-pke under *PKE A-Z* > *Guides*.

Using Commands

The command-line utility provides a number of options for manipulating certificates and groups. Some of the more commonly-used commands are listed below along with examples. For help within the CLI use: **InstallRoot.exe --help .**

Installing certificates

InstallRoot.exe: When run without command arguments, will install all DoD certificates into the appropriate Microsoft certificate store: Microsoft Current User for non-privileged users and Microsoft Local Computer for privileged users.

InstallRoot.exe –-insert: Used to install certificates. By default, it will install all of the certificates from the DoD group into the appropriate Microsoft certificate store (Local Computer if run as administrator, Current User if not). Example usage:

- To install all DoD certificates into the appropriate Microsoft certificate store: **InstallRoot.exe –-insert**

- To install just ECA certificates into the appropriate Microsoft certificate store: **InstallRoot.exe –-insert –-group ECA**
- To install JITC and DoD certificates into an NSS store (arbitrarily named for the example): **InstallRoot.exe –-insert –-group DoD,JITC –-store NSS --storepath %APPDATA%\Roaming\Mozilla\Firefox\Profiles\vvof92ga.default**

  NOTE: InstallRoot will request a password if the NSS or Java database is password-protected. To automate the password input, use the --password parameter followed by the password.

Removing Certificates

InstallRoot.exe –-delete: Used to delete certificates. The certificates and targets for this command are defined in the exact way as the insert command above. However, the delete command removes certificates and the insert command adds them. Example usage:

- To delete all DoD certificates from the appropriate Microsoft certificate store: **InstallRoot.exe –-delete**
- To delete ECA certificates from the appropriate Microsoft certificate store: **InstallRoot.exe –-delete –-group ECA**
- To delete JITC and DoD certificates from an NSS store (arbitrarily named for the example): **InstallRoot.exe –-delete –-group DoD,JITC –-store NSS --storepath %APPDATA%\Roaming\Mozilla\Firefox\Profiles\vvof92ga.default**

  NOTE: InstallRoot will request a password if the NSS or Java database is password-protected. To automate the password input, use the --password parameter followed by the password.
- To delete all certificate groups from the appropriate Microsoft certificate store: **InstallRoot.exe –-delete –-group ECA,DoD,JITC**

InstallRoot.exe –-deletekey [KEY]: Used to delete certificates by their public key. Use the **--listkey** command to determine the [KEY] prior to running this command.

Cache Clearing

InstallRoot.exe --clearcache: Used to clear the InstallRoot cache folder located at %LOCALAPPDATA%/DoD-PKE/InstallRoot/5.0/cache .

InstallRoot.exe –-addtocache [FILE]: Used to add a TAMP message file to the UI or command line cache folder.

Managing Trust Stores

InstallRoot.exe –-store [STORE]: Used to identify a Microsoft certificate store against which to perform an operation. This argument is not run on its own; instead, it is used to identify targets for other commands.

InstallRoot.exe –-liststores: Used to list all of the stores that can be used as inputs for the **–-store** command. The available stores are: **MSCAPI_LC**, **MSCAPI_CU**, **NT_AUTH**, **NSS, JAVA, MULTI_NSS, MULTI_JAVA.**

InstallRoot.exe –-storepath [PATH]: Used to identify the path of a NSS or Java store against which to perform an operation. This argument is not run on its own; instead, it is used to identify targets for the --store argument.

For example: **InstallRoot.exe –-insert –-group DoD,JITC --store NSS --storepath %APPDATA%\Roaming\Mozilla\Firefox\Profiles\vvof92ga.default**

Managing Groups

InstallRoot.exe –-listgroups: Lists all of the groups that can be used as inputs for the **–-group** command. The available groups are **DoD**, **JITC**, and **ECA**.

InstallRoot.exe –-group [GROUP]: This command is used to identify targets for other commands. Multiple groups can be specified by separating groups with commas.

For example: **InstallRoot.exe --delete –-group ECA,DoD,JITC** or **InstallRoot.exe --insert --group JITC**

Managing Individual Certificates

InstallRoot.exe –-list: Used to list certificates. The certificates and targets for this command are defined in the same way as for the **--insert** and **--delete** commands above. The difference is that the list command displays all certificates in the chosen group(s) and whether or not they are installed in the chosen store. The certificate number next to each certificate can be used with the **--certs** command explained below. Example usage:

- To list all certificates in the Microsoft certificate store: **InstallRoot.exe –-list**
- To list just ECA certificates in the Microsoft certificate store: **InstallRoot.exe –-list –-group ECA**
- To list DoD and ECA certificates in an NSS store (arbitrarily named for the example): **InstallRoot.exe –-list –-group DoD,ECA –-store NSS --storepath %APPDATA%\Roaming\Mozilla\Firefox\Profiles\vvof92ga.default**

InstallRoot.exe –-certs [NUMBERS]: Specifies an action to be performed with a specific certificate(s). Use the **--list** command to display the certificate number.

Example usage: **InstallRoot.exe --delete --group ECA --certs 2,3,4**

InstallRoot.exe --listkeys: Used to list the public keys for all certificates. The --listkey argument displays all certificates in the chosen group(s). Example usage:

- To list all the public keys: **InstallRoot.exe --listkeys**

  NOTE: This argument is not recommended to be run with output to the command line since the list will be very long and typically will require the screen buffer size on the command line to be increased in order to display all keys. It is recommended that this argument be used in conjunction with the --group argument. It is also recommended to redirect output to a file.

- To list the public keys for certificates in the ECA group: **InstallRoot.exe --listkeys --group ECA**
- To output the public keys for certificates in the DoD group to a file: **InstallRoot.exe --listkeys --group DoD > %USERPROFILE%\dod_keys.txt**

Managing Logs

InstallRoot.exe –-level [LEVEL]: Used to define the logging level. Used with Fatal, Error, Warn, Info, or Debug. Default is set to Info. Example usage: **InstallRoot.exe --level Debug**

InstallRoot.exe –-logfile [FILE]: Used to define the path to the log file. Can be used with the **--level** argument. Example usage:

- To specify a location and to capture Info (default) information: **InstallRoot.exe --logfile %USERPROFILE%\InstallRoot.log**
- To specify a location and to capture debugging information**: InstallRoot.exe --logfile %USERPROFILE%\InstallRoot.log --level debug**

Exporting certificates

InstallRoot.exe –-export [EXPORT]: Specify the path location when exporting certificates. When exporting PKCS7 format certificates, include the file name with the path location. If a format type is not specified using the **–-exportformat** argument, certificates will be exported in PEM format. Example usage:

- Export all DoD certificates in PEM Format: **InstallRoot.exe --export c:\exported_certficates**
- Export all DoD Certificates in DER format: **InstallRoot.exe --export c:\exported_certficates\ --exportformat DER**
- Export all ECA Certificates in PKCS7 format: **InstallRoot.exe --export c:\exported_certficates\DoD_certs.p7b --exportformat pkcs7 --group ECA**

  NOTE: If the file name is not specified along with the path location, the CLI will produce an error.

InstallRoot.exe –-exportformat [FORMAT]: Specifies the format type to be used when exporting certificates. PEM, DER, or PKCS7 are acceptable.

Managing Online Update Options

InstallRoot.exe –-uri [URI]: Retrieve TAMP messages from a specified URI instead of the default InstallRoot URIs.

InstallRoot.exe --update: Initiates an online check for new TAMP messages.

Example usage:

- **InstallRoot.exe –-update –-uri http://server.local/InstallRoot/DoD.ir4**
- **InstallRoot.exe –-update –-uri \\netshare\network\location\DoD.ir4**

InstallRoot.exe --nocache: Used with **--update** to direct InstallRoot not to cache downloaded TAMP message updates to disk. Not recommended.

Uninstalling InstallRoot

Uninstall any currently installed InstallRoot versions before updating InstallRoot to a newer version.

NOTE: Registry settings will be deleted on uninstall in most cases.

To uninstall InstallRoot:

1) Navigate to the **Windows Control Panel.**
2) Select **Programs and Features.**
3) Select **Uninstall a program.**
4) Select **InstallRoot** from the list of programs on the system.
5) Click **Uninstall**.

Release Notes

5.0 UI Changes

- **Added Certificate Store Cleanup Capability**
  Developed an add-on tool to allow users to easily locate undesired certificates for deletion. Users may search for and filter certificates to identify a range of problematic certificates which may be deleted, untrusted, or exported.
- **Added a Multi-Store option**
  When adding a new store, users now have the option to create a multi-store which has InstallRoot locate and combine all NSS or Java stores found into a single InstallRoot store. InstallRoot may then install certificates based on the subscriptions chosen for that store.
- **Added a button to view the digital signature on InstallRoot TAMP messages**
  Located on the far right of each certificate group, the ( ) button allows users to view the InstallRoot TAMP message signature details, like signer, chain, date/time, and signature algorithm.
- **Load local InstallRoot TAMP message and specify update URI**
  Users may now specify a local file (TAMP message) to load as a new group. Users may now double-click messages to import using Windows Explorer.
- **Save button is now disabled if no changes have been made**
  The save button now only enables when configuration changes have been made.

5.0 General Changes

- **Support for Java Trust Stores**
  Java trust store support allows users to add and configure Java stores within InstallRoot.
- **Added network proxy support**
  Users may now configure a network proxy server (and port) for all outbound communication using the command line utility or the **Preferences** option in the InstallRoot UI.
- **Added a timestamp and stapled OCSP response to InstallRoot TAMP messages**
  Embedded a timestamp and OCSP response in InstallRoot TAMP message for offline validation. Added DoD Root CA 3 as trusted root for message signing as well as included intermediates in signature.

- **NTAuth enhancements**
  InstallRoot will now create an NTAuth store automatically if it does not already exist.
- **Improved messages when installing or deleting certificates to MSCAPI Local Machine and Current User**
  Improved messaging should reduce confusion regarding certificates which can exist in both places simultaneously.
- **Improve start-up error reporting to intelligently display error messages versus multi-symptom messages**
  Improved error messages to provide clarity on the causes of problems. InstallRoot will now check for and report on network connectivity problems and similar issues separately for easier troubleshooting.

Appendix A: Supplemental Information

Please use the information below for troubleshooting and support.

Web Site

Visit the URL below for the PKE website.

http://iase.disa.mil/pki-pke

Visit the **Tools** page to download the latest InstallRoot version.

Technical Support

Contact the DoD PKE Team for technical support, bug reporting, and feature requests through the email address below.

dodpke@mail.mil

Acronyms

AD	Active Directory
CA	Certification Authority
CAC	Common Access Card
CN	Common Name
CRL	Certificate Revocation List
CLI	Command-Line Interface
DER	Distinguished Encoding Rules
DoD	Department of Defense
ECA	External Certificate Authority
FIPS	Federal Information Processing Standard
GDS	Global Directory Service
GPO	Group Policy Object
GUI	User Interface
IASE	Information Assurance Support Environment
JDK	Java Development Kit
JITC	Joint Interoperability Test Command
JRE	Java Runtime Environment
MMC	Microsoft Management Console
MS CAPI	Microsoft Cryptographic Application Programming Interface
MSI	Microsoft installer
NIPRNet	Non-Classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSS	Network Security Service
OCSP	Online Certificate Status Protocol
PEM	Privacy Enhanced Email

PKCS7	Public Key Cryptographic Standard 7
PKE	Public Key Enablement
PKI	Public Key Infrastructure
SIPRNet	Secret Internet Protocol Router Network
TAMP	Trust Anchor Management Protocol
URI	Uniform Resource Identifier

Appendix B: Log Information

InstallRoot Error Logging

By default, InstallRoot activities are logged to the following log files:

- Service logs:

  `C:\Program Files\DoD-PKE\InstallRoot\service\logs\InstallRoot.log`

- GUI logs:

  `%LOCALAPPDATA%\DoD-PKE\InstallRoot\5.0\InstallRoot.log`

Both log files can be found in the **Help** tab of the InstallRoot toolbar. Refer to these log files if unexpected behavior is observed or unexpected errors are encountered.

By default, the logs are set to capture **Information**, **Warning**, **Error**, and **Fatal** messages. If more logging information is desired, the logs can be set to **Debug** mode. This is done via the registry.

1) Run **regedit.exe**.
2) To set the **DebugMode** flag for the administrator GUI and service events, navigate to:

   `HKEY_LOCAL_MACHINE\SOFTWARE\DoD-PKE\InstallRoot\5.0\`

   To set the **DebugMode** flag for the user GUI events navigate to:

   `HKEY_CURRENT_USER\Software\DoD-PKE\InstallRoot\5.0`

   For both keys, double-click the **DebugMode** value.
3) Change the value from 0 to 1.
4) Restart the InstallRoot GUI or the service in order for the change to take effect, depending on which log was updated.

The InstallRoot log is configured to roll log files once they reach 10MB in size. The application will also save the last 10 log files; over-writing older logs. These parameters can be changed by editing the configuration file **log4netFileConfig.xml** located here:

`C:\Program Files\DoD-PKE\InstallRoot\`

```
<?xml version="1.0" encoding="utf-8" ?>
<log4net>
  <appender name="RollingLogFileAppender"
type="log4net.Appender.RollingFileAppender">
    <file value="InstallRoot.log" />
    <appendToFile value="true" />
    <maxSizeRollBackups value="10" />
    <maximumFileSize value="10MB" />
    <rollingStyle value="Size" />
```

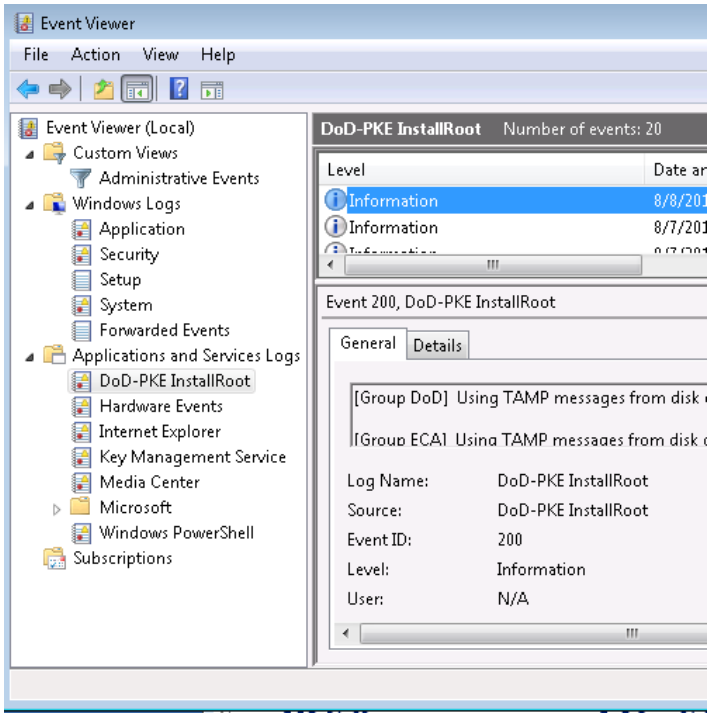
```
    <lockingModel
type="log4net.Appender.FileAppender+MinimalLock" />
    <layout type="log4net.Layout.PatternLayout">
      <conversionPattern value="%date %-5level -
%message%newline"/>
    </layout>
  </appender>
  <root>
    <appender-ref ref="RollingLogFileAppender"/>
  </root>
</log4net>
```

Two lines in the configuration file can be changed if necessary:

- To change the size of when the log file is rolled over, edit the **maximumFileSize value**. Allowable size values are a minimum of one with no maximum, followed by a KB or MB.
- To change the maximum number of files, edit the **maxSizeRollBackups** value. Allowable size values are a minimum of one with no maximum. It is recommended that this value not be changed.

Windows Error Logging

InstallRoot will also log events to the **Windows Event Log** system. To make the events easier to find, InstallRoot creates its own log file under the **Applications and Services Logs** tree called **DoD-PKE InstallRoot**.



Below are the event IDs and their descriptions:

Event ID	Description
200	Successful update operation indicating how many certificates were installed and if the operation was performed via an online update or update from disk/built-in cache.
410	EventID 410 can be generated for the following errors: • Internal Error • TAMP message was signed by an invalid code signer • Signer certificate has been revoked
420	EventID 420 can be generated for the following errors: • Failure to read the update period from the registry • logging failed to initialize
430	Failure to update certificate store(s)

Command-line Interface Exit Codes

If running InstallRoot CLI within batch files, the following exit codes are provided:

Exit Code	Description
1	Invalid argument
2	Initialization errors • Runtime Configuration Generator Initialization error • NSS DLL Load error • Process Runtime Configuration error • InstallRoot attempted to load TAMP messages that were signed with an algorithm that your Operating System does not support • Logfile directory does not exist, Logfile does not exist, or Logfile directory is not writeable
3	Command Argument errors

	• Export format option used without Export option error • No cache option used without Update option error • Unsupported group
4	Permission and domain check errors • Request update of MSCAPI Local Computer store without adequate permissions error • Request update of NT Auth store without adequate permissions error • Request update of NT Auth store without machine being a member of a domain error • Attempt to clear cache without adequate permissions error
5	Certificate Database Processor error (FAILURE)
6	Certificate Database Processor error (SIGVERFAILURE)
7	Certificate Database Processor error (SIGVERFAILUREREVOKED)
8	Certificate Information Processor error
10	Open MSCAPI Local Computer store failed
11	Open MSCAPI Current User store failed
12	Open NSS store failed
13	Open NT Auth store failed
15	Error while retrieving status information for certificates • ArgumentNullException • FormatException • IOException • Generic Exception

16	Error while retrieving key information for the certificates • ArgumentNullException • FormatException • IOException • Generic Exception
17	Error occurred creating the export directory • PathTooLongException • IOException • SecurityException • Generic Exception
18	Error occurred accessing the export directory • PathTooLongException • SecurityException • Generic Exception
20	Failed removal by key
21	Failed to install certificate
22	Certificate removal not possible because it does not exist to remove
24	Failed to remove certificate
30	InstallRoot has identified running NSS processes that will conflict with the importing and removal of certificates
31	Open Multi NSS store failed
32	Open Multi JAVA store failed
33	Open JAVA store failed

InstallRoot Cache

InstallRoot maintains a local cache of the latest TAMP messages received for each group so the online update will only download new TAMP messages when they have been updated. Depending on the method used to download the TAMP messages, they will be stored in different locations, as follows:

- The shared cache for the CLI and GUI is located at:

```
%LOCALAPPDATA%\DoD-PKE\InstallRoot\4.1\cache
```

- The cache for the Windows service is located at:

```
C:\Program Files\DoD-PKE\InstallRoot\service\cache
```

Appendix C: Included Certificates

The following certificates are included in InstallRoot 5.0.

DoD PKI Production Certificates

Target CA Store	Subject CN	Issuer CN
Root	DoD Root CA 2	DoD Root CA 2
Root	DoD Root CA 3	DoD Root CA 3
Intermediate	DoD CA-27	DoD Root CA 2
Intermediate	DoD CA-28	DoD Root CA 2
Intermediate	DoD CA-29	DoD Root CA 2
Intermediate	DoD CA-30	DoD Root CA 2
Intermediate	DoD CA-31	DoD Root CA 2
Intermediate	DoD CA-32	DoD Root CA 2
Intermediate	DoD EMAIL CA-27	DoD Root CA 2
Intermediate	DoD EMAIL CA-28	DoD Root CA 2
Intermediate	DoD EMAIL CA-29	DoD Root CA 2
Intermediate	DoD EMAIL CA-30	DoD Root CA 2
Intermediate	DoD EMAIL CA-31	DoD Root CA 2
Intermediate	DoD EMAIL CA-32	DoD Root CA 2
Intermediate	DoD Email CA-33	DoD Root CA 2
Intermediate	DoD Email CA-34	DoD Root CA 2
Intermediate	DoD Email CA-39	DoD Root CA 2
Intermediate	DoD Email CA-40	DoD Root CA 2
Intermediate	DoD Email CA-41	DoD Root CA 3
Intermediate	DoD Email CA-42	DoD Root CA 3
Intermediate	DoD Email CA-43	DoD Root CA 3
Intermediate	DoD Email CA-44	DoD Root CA 3
Intermediate	DoD ID CA-33	DoD Root CA 2
Intermediate	DoD ID CA-34	DoD Root CA 2
Intermediate	DoD ID CA-39	DoD Root CA 2
Intermediate	DoD ID CA-40	DoD Root CA 2
Intermediate	DoD ID CA-41	DoD Root CA 3
Intermediate	DoD ID CA-42	DoD Root CA 3
Intermediate	DoD ID CA-43	DoD Root CA 3
Intermediate	DoD ID CA-44	DoD Root CA 3
Intermediate	DoD ID SW CA-35	DoD Root CA 2
Intermediate	DoD ID SW CA-36	DoD Root CA 2
Intermediate	DoD ID SW CA-37	DoD Root CA 2
Intermediate	DoD ID SW CA-38	DoD Root CA 2
Intermediate	**DoD Root CA 2	US DoD CCEB Interoperability Root CA 1
Intermediate	**DoD Root CA 2	DoD Interoperability Root CA 1
Intermediate	**DoD Root CA 3	DoD Interoperability Root CA 2
Untrusted	DoD Root CA 2	DoD Interoperability Root CA 1

Untrusted	DoD Root CA 2	US DoD CCEB Interoperability Root CA 1
Untrusted	DoD Root CA 3	DoD Interoperability Root CA 2

External Certification Authority (ECA) PKI Certificates

Target CA Store	Subject CN	Issuer CN
Root	ECA Root CA 2	ECA Root CA 2
Root	ECA Root CA 4	ECA Root CA 4
Intermediate	IdenTrust ECA 3	ECA Root CA 2
Intermediate	ORC ECA 6	ECA Root CA 4
Intermediate	ORC ECA HW 4	ECA Root CA 2
Intermediate	ORC ECA SW 4	ECA Root CA 2
Intermediate	VeriSign Client External Certification Authority - G3	ECA Root CA 2
Intermediate	IdenTrust ECA 4	ECA Root CA 2
Intermediate	Symantec Client External Certification Authority - G4	ECA Root CA 2
Intermediate	ORC ECA HW 5	ECA Root CA 2
Intermediate	ORC ECA SW 5	ECA Root CA 2
Intermediate	** ECA Root CA 2	DoD Interoperability Root CA 1
Intermediate	** ECA Root CA 2	DoD Interoperability Root CA 1
Intermediate	**ECA Root CA 4	DoD Ineroperability Root CA 1
Untrusted	ECA Root CA 2	DoD Interoperability Root CA 1
Untrusted	ECA Root CA 2	DoD Interoperability Root CA 1
Untrusted	ECA Root CA 4	DoD Interoperability Root CA 1

** *Denotes certificates to be deleted from the target store.*

DoD Test PKI (JITC and O&M) Certificates

Target CA Store	Subject CN	Issuer CN
Root	DoD JITC Root CA 2	DoD JITC Root CA 2
Root	DoD JITC Root CA 3	DoD JITC Root CA 3
Root	DoD JITC Root CA 4	DoD JITC Root CA 4
Root	NSS JITC Root CA 1	NSS JITC Root CA 1
Root	NSS JITC Root CA 2	NSS JITC Root CA 2
Root	NSS JITC Root CA 3	NSS JITC Root CA 3
Root	ECA JITC Root CA 2	ECA JITC Root CA 2
Root	ECA JITC Root CA 3	ECA JITC Root CA 3
Root	ECA JITC Root CA 4	ECA JITC Root CA 4
Intermediate	DOD JITC CA-25	DoD JITC Root CA 2
Intermediate	DOD JITC CA-27	DoD JITC Root CA 2
Intermediate	DOD JITC CA-29	DoD JITC Root CA 2
Intermediate	DOD JITC CA-31	DoD JITC Root CA 2
Intermediate	DOD JITC EMAIL CA-25	DoD JITC Root CA 2
Intermediate	DOD JITC EMAIL CA-27	DoD JITC Root CA 2
Intermediate	DOD JITC EMAIL CA-29	DoD JITC Root CA 2
Intermediate	DOD JITC EMAIL CA-31	DoD JITC Root CA 2
Intermediate	DoD JITC Intermediate CA-1	DoD JITC Root CA 2
Intermediate	DOD JITC NPE CA-1	DoD JITC Root CA 2
Intermediate	DOD OM CA-28	DoD JITC Root CA 2
Intermediate	DOD OM CA-30	DoD JITC Root CA 2
Intermediate	DOD OM CA-32	DoD JITC Root CA 2
Intermediate	DOD OM EMAIL CA-28	DoD JITC Root CA 2
Intermediate	DOD OM EMAIL CA-30	DoD JITC Root CA 2
Intermediate	DOD OM EMAIL CA-32	DoD JITC Root CA 2
Intermediate	DoD OM Intermediate CA-2	DoD JITC Root CA 2
Intermediate	DOD OM NPE CA-2	DoD JITC Root CA 2
Intermediate	DOD TEST SHA-256 CA-22	DoD JITC Root CA 2
Intermediate	DOD TEST SHA-256 CA-26	DoD JITC Root CA 2
Intermediate	DOD TEST SHA-256 EMAIL CA-22	DoD JITC Root CA 2
Intermediate	DOD TEST SHA-256 EMAIL CA-26	DoD JITC Root CA 2
Intermediate	NSS DoD JITC Intermediate CA 1	NSS JITC Root CA 1
Intermediate	NSS DoD JITC Intermediate CA 2	NSS JITC Root CA 2
Intermediate	NSS DoD JITC Subordinate CA 1	NSS DoD JITC Intermediate CA 1
Intermediate	NSS DoD OM Subordinate CA 2	NSS DoD JITC Intermediate CA 1
Intermediate	NSS JITC SW-CA- 2	NSS DoD JITC Intermediate CA 1
Intermediate	NSS JITC CA-2	NSS DoD JITC Intermediate CA 1
Intermediate	** DoD JITC Root CA 2	US DoD CCEB JITC Interoperability Root CA 1
Intermediate	** DoD JITC Root CA 2	DoD Interoperability Root CA 1
Intermediate	**DoD JITC Root CA 3	DoD JITC Interoperability Root CA 2
Intermediate	**ECA JITC Root CA 4	DoD JITC Interoperability Root CA 2
Intermediate	**ECA JITC Root CA 4	DoD JITC Interoperability Root CA 2
Intermediate	DOD OANDM ID CA-34	DoD JITC Root CA 2

Intermediate	DOD OANDM ID CA-40	DoD JITC Root CA 2
Intermediate	DOD OANDM ID CA-42	DoD JITC Root CA 3
Intermediate	DOD OANDM ID CA-44	DoD JITC Root CA 3
Intermediate	DOD OANDM EMAIL CA-34	DoD JITC Root CA 2
Intermediate	DOD OANDM EMAIL CA-40	DoD JITC Root CA 2
Intermediate	DOD OANDM EMAIL CA-42	DoD JITC Root CA 3
Intermediate	DOD OANDM EMAIL CA-44	DoD JITC Root CA 3
Intermediate	DOD OANDM ID SW CA-36	DoD JITC Root CA 2
Intermediate	DOD OANDM ID SW CA-38	DoD JITC Root CA 3
Untrusted	DoD JITC Root CA 2	US DoD CCEB JITC Interoperability Root CA 1
Untrusted	DoD JITC Root CA 2	DoD Interoperability Root CA 1
Untrusted	DoD JITC Root CA 3	DoD JITC Interoperability Root CA 2
Untrusted	ECA JITC Root CA 4	DoD JITC Interoperability Root CA 2
Untrusted	ECA JITC Root CA 4	DoD JITC Interoperability Root CA 2

Appendix D: Active Directory Installation Overview

NOTE: Distributing the InstallRoot MSI using the existing software distribution processes is preferred. If such a process is not implemented, the following example can be used.

InstallRoot 5.0 has been tested with Windows Server 2008, 2008R2, and 2012, using Active Directory's GPOs to push the installation to domain member workstations. The following provides a general overview of deployment methods, distribution point creation, and GPO creation. The below steps were performed using Server 2008R2 and each version of Windows Server may have slightly different steps.

Methods of deployment

Group Policy supports two methods of deploying an MSI package:

1) **Assign software** - A program can be assigned per-user or per-machine. If assigned per-user, it will be installed when the user logs on.

   If assigned per-machine, then the program will be installed for all users when the machine starts.

2) **Publish software** - A program can be published for one or more users. This program will be added to the **Add or Remove Programs** list, where users will be able to install it.

NOTE: Most DoD system users will require InstallRoot and it is recommended that InstallRoot be deployed per-machine.

Creating a distribution point

The first step in deploying the MSI through a GPO is to create a distribution point on the publishing server. This can be done by following these steps:

1) Log on to the server as an Administrator.
2) Create a shared network folder (this folder will contain the MSI package).
3) Set permissions on this folder in order to allow access to the distribution package.
4) Copy the MSI in the shared folder.

NOTE: Correct permissions must be set at the share level as well as the file level. If error 1612 is received during the install, verify the domain-joined machine has the appropriate read permissions to the share and file locations of the MSIs.

Create a Group Policy Object

The MSI package is distributed as a Group Policy Object. In order to create an object for the package, follow these steps:

1) Click the **Start** button, go to **Programs > Administrative Tools** and then select **Group Policy Management.**
2) Expand the domain name in the console tree and navigate to the **Group Policy Objects.**
3) Expand the **Group Policy** tab.

   NOTE: At this point, a new Group Policy Object can be created or one that already exists can be edited. For this example, a new Object will be created.
4) Right-click the **Group Policy** tab and select new.
5) Set the name of the policy (for example *InstallRoot_5*) and select **OK.**
6) Right-click the newly created Object and select **Edit**.
7) **Expand** the **Computer Configuration > Policies > Software Settings** tree.
8) Right-click the **Software installation** and select **New > Package.**
9) In the **Open** dialog that appears, change the location to the UNC of the machine and share of where the InstallRoot .msi was placed in the **Creating a distribution point** section above. ***Example:\\machine_name\share_location***

   NOTE: Do not use the Browse button in the Open dialog to access the UNC location. Make sure to use the UNC path to the shared package.
10) **Open** the .msi file.
11) Select **Assigned** and then select **OK.**
12) The information about the installation package will populate the right pane.

    NOTE: This operation may take some time to complete.
13) **Close** the **Group Policy Management Edit** window.
14) In the **Group Policy Management** screen, ensure the new **Group Policy Objects GPO status** is **Enabled**.

NOTE: The above procedures will create the GPO at the domain level. If more granular control is desired, assign the GPO to the correct OU, group, etc. for the domain.

Appendix E: Using InstallRoot in Disconnected Environments

InstallRoot uses the Trust Anchor Management Protocol (TAMP) to obtain instructions for changes it should make to a trust store. Each InstallRoot TAMP message, identified by the .ir4 file extension, contains a set of certificates and associated instructions that tell the tool which certificates should be installed or removed from which trust store location.

In environments with network connectivity, if updates are enabled, the tool will automatically check for new TAMP messages on the DISA Information Assurance Support Environment (IASE) web site. However, in disconnected environments the system will not be able to reach IASE, so the latest TAMP message must be either re-hosted locally or directly installed on the machine where the tool is running. For disconnected enclaves, hosting TAMP messages on a local web site or file share accessible to all machines in the enclave is recommended to facilitate easy updates when new TAMP messages are released. However, for individual disconnected machines, directly installing new TAMP messages on the local machine may be necessary.

For either disconnected deployment method, the tool should also be configured so that it uses the TAMP message in the desired location without attempting to fetch messages from unreachable locations.

NOTE: For InstallRoot Command Line Interface (CLI) commands throughout this appendix, the commands must be executed from within the %ProgramFiles%\DoD-PKE\InstallRoot directory.

Obtaining the Latest InstallRoot TAMP Message

For disconnected environments, the latest TAMP message must be manually retrieved and transferred to the disconnected environment. It can then be either hosted on a local server or network file share to support all machines in the disconnected enclave, or placed directly on the machine(s) running InstallRoot.

There are a couple of ways to obtain the latest TAMP message from a connected machine prior to transferring it to the disconnected environment.

Option 1: Direct Download

Download the desired message(s) directly from the InstallRoot TAMP message directory hosted on IASE at http://iase.disa.mil/pki-pke/data/ir4.

Option 2: InstallRoot Update

From a connected machine running InstallRoot, perform an online update and then copy the latest message from cache. The update can be performed using either the InstallRoot Graphical User Interface (GUI) or Command Line Interface (CLI).

InstallRoot GUI: Click the **Online Update** button on the **Home** tab.

InstallRoot Command Line Interface (CLI): Run the `installroot --update` command.

Once the online update has been performed, the latest InstallRoot TAMP message file can be copied from the local cache directory located at **%USERPROFILE%\AppData\Local\DoD-PKE\InstallRoot\5.0\cache** for transfer to the disconnected system.

Redistributing the Latest TAMP Message

Once the TAMP message has been transferred to the disconnected environment, there are several options for redistributing it.

Option 1: Hosting the Latest TAMP Message on a Local Web or File Server

For disconnected enclaves with multiple machines, establishing a central hosting location for the latest TAMP message(s) can be an efficient way to distribute updates. The hosting location can be either a web server or network file share. The account(s) under which the InstallRoot tool and service (if installed) are run must have permissions to access the hosting location. For web servers that require MIME type configuration, the recommended MIME type for .ir4 files is `application/tamp-update`.

Option 2: Placing the Latest TAMP Message Directly onto Workstations

If maintaining a central hosting location is not feasible, the latest TAMP message(s) can be distributed to each workstation that should receive the certificate updates.

A local directory location where any new TAMP messages will be stored should be identified; for example, C:\TAMP. The tool can then be configured to look for new TAMP messages in that location going forward.

For enterprise deployments, the latest TAMP message(s) can be deployed to the designated directory location on workstations across an enclave via standard organizational practices such as GPO. For individual deployments, users can manually copy the latest TAMP message(s) into the designated directory.

Configuring InstallRoot to Use the Local TAMP Message

When initially deploying InstallRoot in a disconnected environment, the tool should be reconfigured to fetch messages from the local TAMP message location rather than

unreachable locations like IASE. The sections below describe how to configure the different InstallRoot components to consume local TAMP messages rather than the default messages hosted on IASE. All actions should be performed with administrative privileges (e.g., by launching the tool or command prompt using the Run as Administrator option) if available.

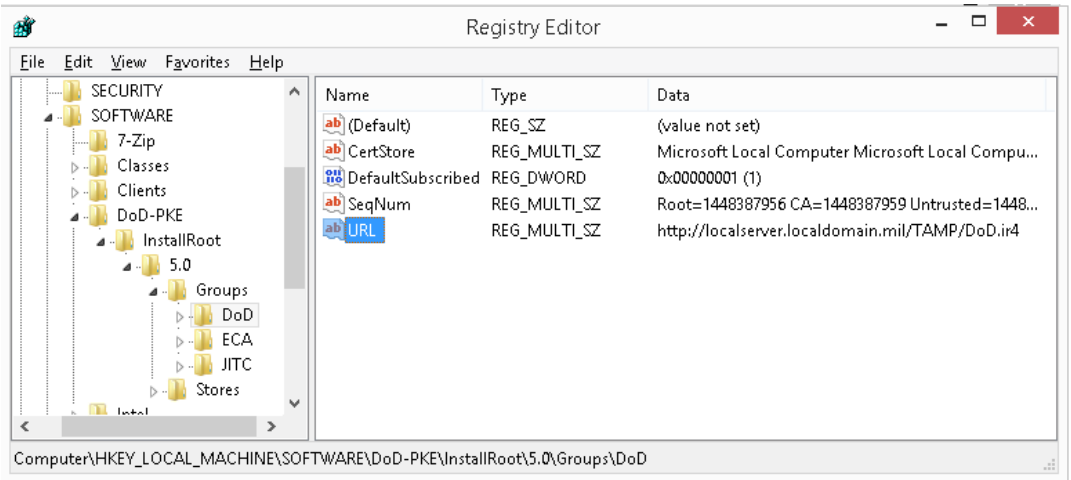
Automatic Certificate Updates: Windows Service

The InstallRoot Windows service must be installed to enable the tool to automatically check for and install certificate updates. Follow these instructions to configure the InstallRoot Windows service to check a local TAMP message location rather than IASE for updates. These configuration steps must only be performed once. Once the InstallRoot Windows Service is configured, the tool will automatically update the workstation's trust store whenever a new TAMP message is made available at the configured location.

NOTE: If hosting TAMP messages on a network file share, the InstallRoot service must be configured to run under an account with access to the share rather than the default Local System account.

Enterprise Deployment

For enterprise deployments, the Windows Service can be configured using the registry as described in the **Configuring InstallRoot** section. For disconnected environments, the **URL** value(s) for the appropriate group(s) under the HKEY_LOCAL_MACHINE\SOFTWARE\DoD-PKE\InstallRoot\5.0\Groups registry key should be set to reflect the local TAMP message location (e.g. within the DoD group key, set the URL value to http://localserver.localdomain.mil/IRTAMP/DoD.ir4, \\localshare.localdomain.mil\IRTAMP\DoD.ir4 or C:\TAMP\DoD.ir4 for a web server, network file share, or local directory location, respectively).



Individual Deployment

For individuals installing the tool on their local workstations, it is recommended that the GUI be installed with the service to eliminate the need to directly configure registry settings. Follow instructions for **GUI Initial Setup** in the **Manual Certificate Updates** section, ensuring that the Windows Service is selected to be installed in Step 1.

Manual Certificate Updates

If the InstallRoot Windows service has not been installed and configured to automatically update the certificate trust store, certificate updates can be performed manually using either the InstallRoot GUI or CLI by following the instructions below.

GUI

Initial Setup

These configuration steps must only be performed once.

NOTE: Prior to beginning, ensure that the latest TAMP message is available locally at one of the locations detailed in the Redistributing the Latest TAMP Message section.

6) Run the InstallRoot installer (MSI) according to the standard installation instructions.
7) Update the tool configuration to point to the local TAMP message(s) rather than IASE.
    a) Launch the InstallRoot GUI. An error message will display indicating that the tool failed to perform an online update. Close the message.
    b) Select the **Group** tab.
    c) Select the certificate group (e.g. **Install DoD Certificates**) for which the TAMP message is being hosted locally and click the **Edit** button on the header ribbon.
    d) Delete the IASE URL (http://iase.disa.mil/pki-pke/data/ir4/DoD.ir4) in the **URI** field and replace it with the URL or local file location for the local TAMP message (e.g. http://localserver.localdomain.mil/IRTAMP/DoD.ir4, \\localshare.localdomain.mil\IRTAMP\DoD.ir4 or C:\TAMP\DoD.ir4). Click **OK**. A message should display indicating that the URI for the selected group was successfully changed.
    e) Select the **Home** tab and click the **Save Settings** button.
8) Remove any of the default groups (e.g. ECA, JITC) not being used by right-clicking the group and selecting **Remove**. This will prevent the tool from generating errors

when attempting to perform updates due to those groups' TAMP messages not being available.

NOTE: Groups can be added back into the tool at any time by clicking the Add button under the Group tab and entering the URL or local file location for the group's TAMP message.

9) Follow the instructions in the **Certificate Updates** section to install the certificates contained within the locally hosted TAMP message.

Certificate Updates

Perform these steps each time a new TAMP message is released.

1) Ensure the updated TAMP message is available from the local server URL or file share.
2) If the machines to be updated have not been configured to automatically install updates from the local server URL using the Windows Service, manually perform the update:
   a) Click the **Online Update** button. The tool should display a message indicating an updated TAMP message was found.
   b) Verify desired certificates for installation display in the appropriate group (e.g. expand the **Install DoD Certificates** line to verify that the latest CAs are listed).
   c) Click the **Install Certificates** button to install the updates.

Command Line

Initial Setup

1) Run the InstallRoot installer (MSI). On the **InstallRoot Features** screen of the **InstallRoot Setup Wizard**, uncheck the **GUI** and **Windows Service** options.

   NOTE: If running the Non-Admin version of the InstallRoot installer, the Windows Service option is not available and therefore unchecking that option is unnecessary.

2) Follow the instructions in the Error! Reference source not found. section to install the certificates contained within the local TAMP message.

Certificate Updates

Perform these steps each time a new TAMP message is released.

1) Ensure the updated TAMP messages for each group to be updated are available from the local server URL, file share, or local file system location.

2) Manually perform the update and installation for each group to be updated:

   a) Retrieve the latest TAMP message:

      From a web server or file share: From a command prompt, run the `installroot --update --group <group_name> --uri <local TAMP message URL>` command to fetch the latest TAMP message from the local server.

      NOTE: *<group_name>* should be the name of the group to be updated, e.g. DoD. *<local TAMP message URL>* should be the local hosting location of the latest TAMP message for that group, e.g. `http://localserver.localdomain.mil/IRTAMP/DoD.ir4` or `\\localshare.localdomain.mil\IRTAMP\DoD.ir4`.

      From a local file system location: From a command prompt, run the `installroot --group <group_name> --addtocache <path_to_new_TAMP_message>` command to register the new TAMP message with the tool.

      NOTE: *<group_name>* should be the name of the group to be updated, e.g. DoD. *<path_to_new_TAMP_message>* should be the new TAMP message file and path noted in step 1 of this section. For example, if the new DoD.ir4 TAMP message file was saved to the C:\TAMP directory, the full command would be `installroot --group DoD --addtocache C:\TAMP\DoD.ir4`.

   b) Run the `installroot --list` command to verify that desired certificates for installation display in the appropriate group (e.g. run `installroot --list --group DoD` and verify that the latest DoD CAs are listed).

   c) Run the `installroot --insert --group <group_name>` command to install the updates.

      NOTE: *<group_name>* should be the name of the group to be updated, e.g. DoD.