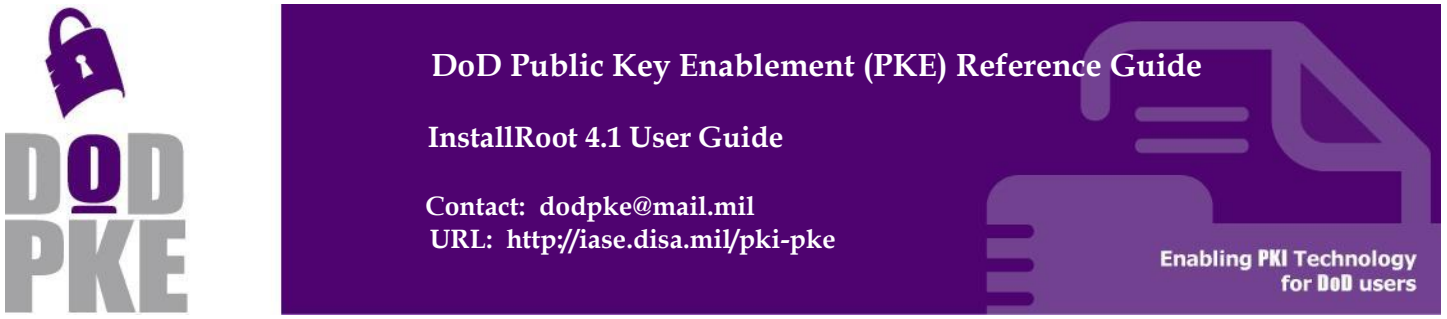


InstallRoot 4.1 User Guide for Unclassified Systems

13 February 2015

Version 1.0

DOD PKE Team

Revision History

Issue Date	Revision	Change Description
02/13/2015	1.0	Initial publication

Contents

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 is a utility which 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 also provides interfaces for managing these CA certificates in the certificate stores on a system.

A Graphical User Interface (GUI), a Command-Line Interface (CLI), and the InstallRoot service, which is used to perform periodic checks for updated Trust Anchor Management Protocol (TAMP) messages, are available to suit different users' preferences and needs. Each version is contained within a single .msi that 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. The non-admin version does not include the InstallRoot service.

System Requirements

Supported Platforms

Supported operating systems (32- and 64- bit):

- Windows XP
- Windows Vista
- Windows 7
- Windows 8 and 8.1
- Windows Server 2003 and 2003 R2

  NOTE: Restricted mode not supported.
- Windows Server 2008 and 2008 R2
- Windows Server 2012 and 2012 R2

Supported browsers:

- Internet Explorer 7 and above
- Firefox 12 to 33
- Google Chrome 33 or higher

Supported Mozilla NSS version:

- 3.17.2

Prerequisite software:

- .NET Framework version 3.5 SP1, 4.0, or 4.5

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

User Privileges and Folder Locations

InstallRoot is available in two different versions: A non-admin version that can be installed by a non-privileged user to manage the user's *Current User Certificate Store,* and a standard version which requires administrative privileges to install and use full functionality. The non-admin version does not include the Windows Service functionality.

The default installation directory is:

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

This location can be changed during the installation process.

When InstallRoot is launched with administrative privileges (Using the **Run As Administrator** option or the **Restart as Administrator** button within the **Home** tab of the GUI), the program will manage the *Local Computer Certificate Store*. If logged onto a domain-joined machine as a Domain Administrator, the NTAuth Store can also be managed.

If InstallRoot is launched without administrative privileges, it will manage the *Current User Certificate Store*, making certificates available only to the current user.

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

Verifying the Digital Signature on the Utility

Before proceeding with this installation, verify that the installer (.msi file) has been digitally signed by DoD PKE Engineering. Follow these steps to verify the digital signature:

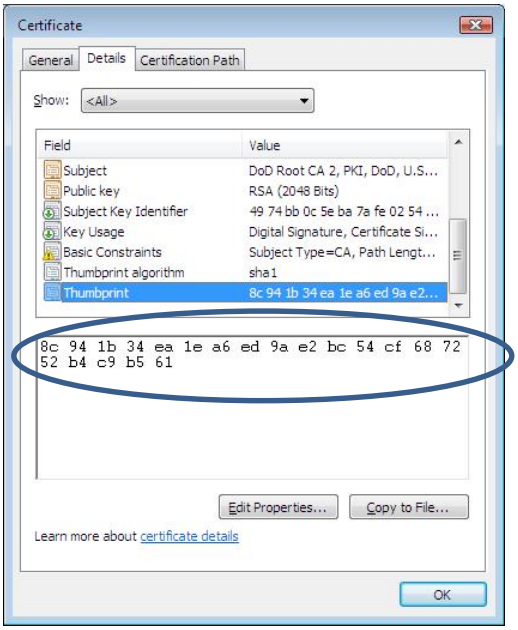
1) In Windows Explorer, navigate to the directory containing the InstallRoot_v4.1.msi, InstallRootv4.1_x64.msi, or InstallRoot_v4.1-NonAdmin.msi.
2) Right-click the .msi and select **Properties** from the pop-up menu to open the Properties window.
3) Select the **Digital Signatures** tab.
4) Select "CS.DoD PKE Engineering.DoDPKE60003" in the Signature list and click **Details**. The **Digital Signature Details** window opens.

   If DoD Root 2 is already installed (e.g. by previously running the tool), the message "This digital signature is OK" should display when checking the signature on a machine with the DoD production PKI certificates installed.

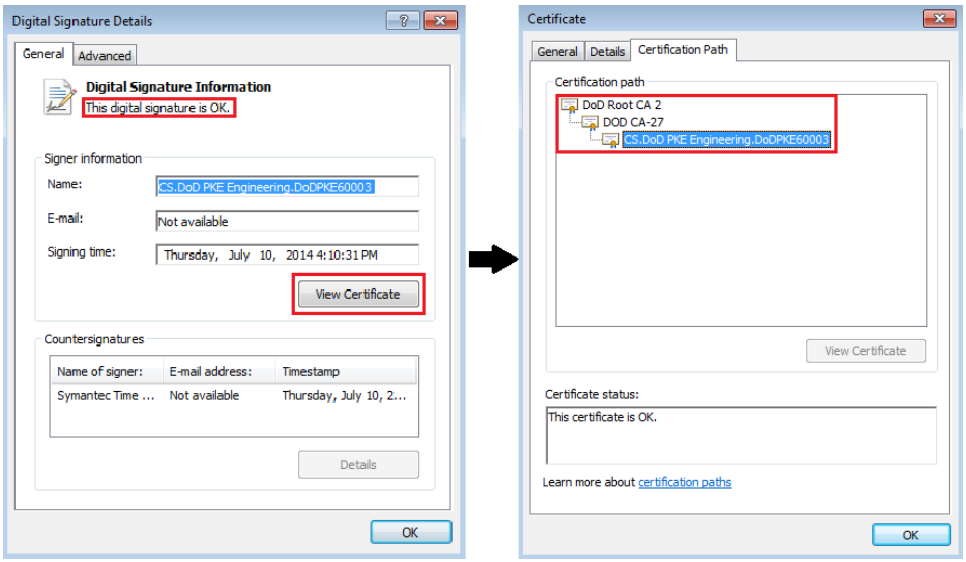
   If DoD Root 2 has NOT been installed (e.g. because InstallRoot has never been run on the machine before), the message "This signature is untrusted" will display. Perform the following steps to verify the signature should be trusted:

   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 Help Desk at (800) 490-1643 or DSN 339-5600.



5) Close the DoD Root CA 2 certificate. If it is not already open, view the CS.DoD PKE Engineering.DoDPKE60003 certificate by clicking **View Certificate** in the **Digital Signature Details** window. Select the **Certification Path** tab to verify the certification path. The certification path should read "DoD Root CA 2 > DoD CA-27 > CS.DoD PKE Engineering.DoDPKE60003." If the digital signature is <u>not</u> OK, do not proceed with installation as the version of the tool you have may not be authentic.



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

Installing InstallRoot

NOTE: Please uninstall any previously installed versions of InstallRoot before proceeding.

1) After verifying the correct digital signature on the desired InstallRoot MSI file as described in the Verifying the Digital Signature on the Utility section of this guide, double-click **InstallRoot4.msi**, **InstallRoot41_x64.msi** or **InstallRoot4.1_non-admin.msi** to launch the installation wizard

   NOTE: SIPRNet versions of the application are available. The SIPRNet version of this guide is packaged within the SIPRNet InstallRoot MSIs.

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 is:

   C:\Program Files\DoD-PKE\InstallRoot

4) On the **InstallRoot Features** screen of the wizard, check the features that should be installed by the wizard. 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: In the non-admin version, the option to install the Windows Service feature is not present.

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

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

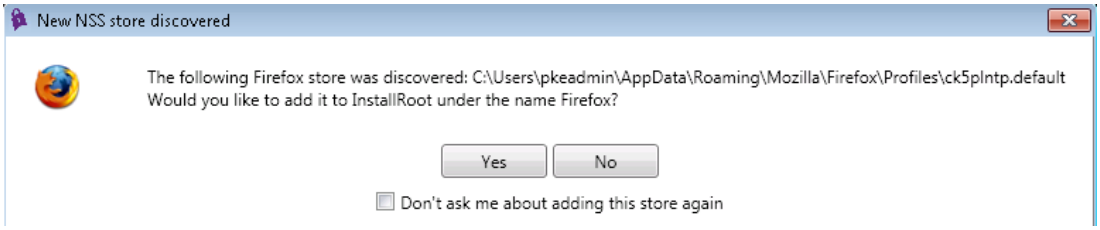
Quick Start

When InstallRoot is run for the first time, a **Quick Start** tutorial describing how to install certificates will automatically launch. After the initial run, the tutorial can be re-launched at any time from the **Help** tab of the InstallRoot GUI.

1) Using the Windows Start Menu, navigate to **All Programs > DoD-PKE > InstallRoot 4.1.**

2) InstallRoot will launch, displaying the GUI screen.

   NOTE: If InstallRoot detects that there is a new Mozilla NSS Store, the following window will appear:

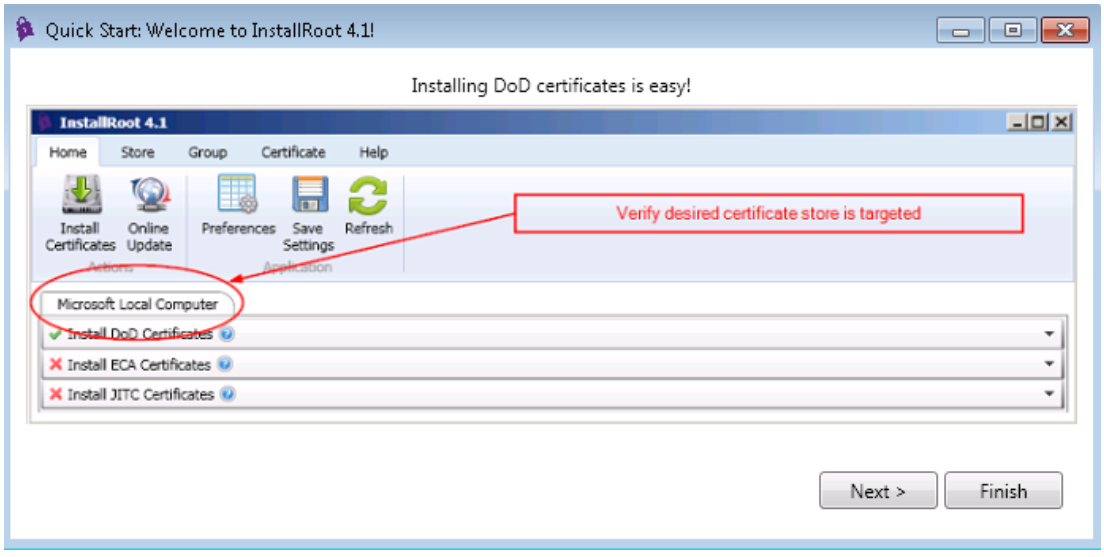


   Click **Yes** to add the NSS Store to the InstallRoot management interface. By default, a new store will be added called Firefox or Thunderbird depending on the version found. To add certificates to the NSS Store, select the Firefox store and then follow the steps starting at step 3a.

3) When running InstallRoot for the first time, the **Quick Start: Welcome to InstallRoot 4.1** tutorial will display. The **Quick Start** tutorial walks through the process of installing DoD certificates.

   NOTE: The Quick Start tutorial can be positioned next to the InstallRoot GUI to enable the user to execute each step described by the tutorial within the GUI while progressing through the tutorial.

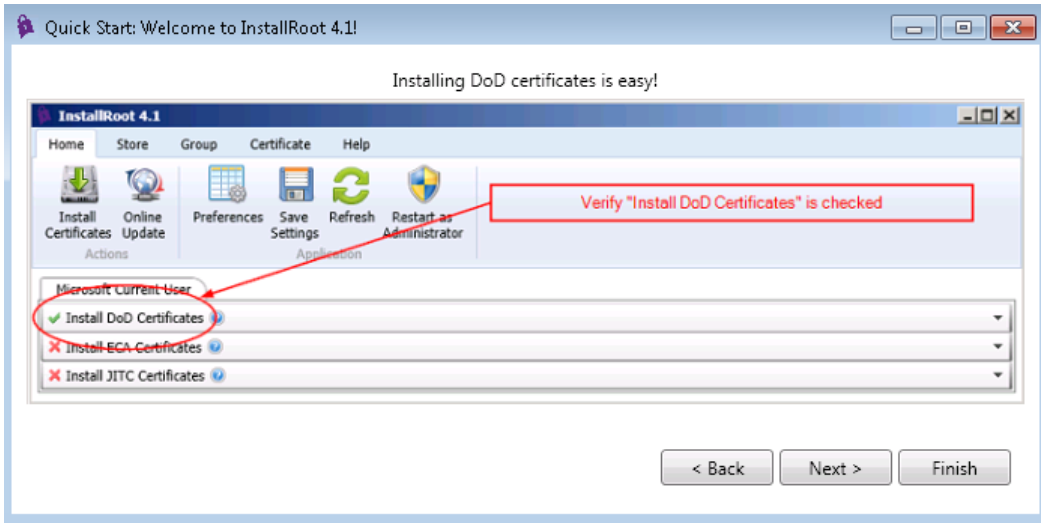
   a. Ensure the desired certificate store is selected.



If running the tool as an administrator, the system will default to the *Microsoft Local Computer* certificate store. If running the tool as a non-privileged user, this will default to the *Microsoft Current User* certificate store. If an NSS store (e.g. for Firefox or Thunderbird) was configured on startup, that will display here as well.

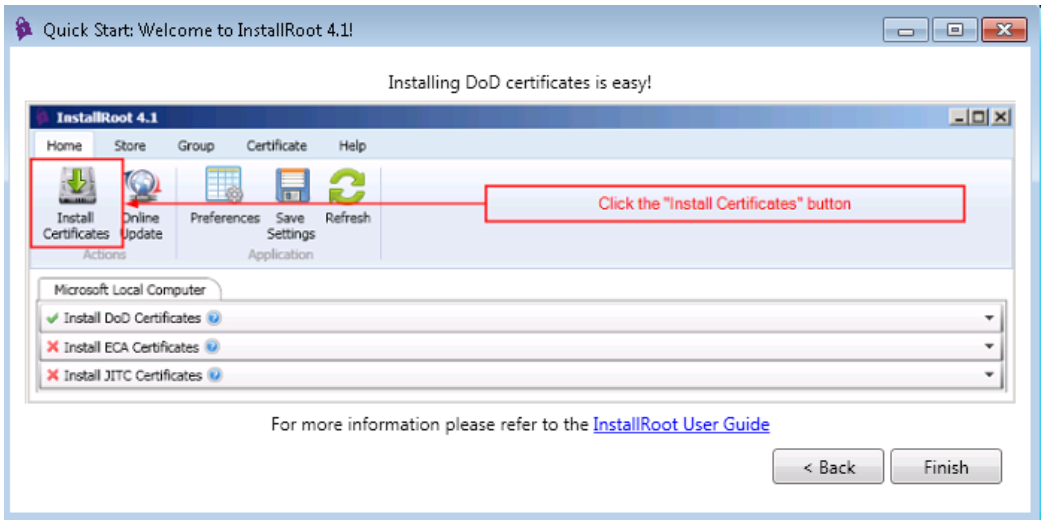
NOTE: If system wide changes are desired, InstallRoot should be run as an administrator.

b. Verify that **Install DoD Certificates** is enabled, as indicated by a green check mark. If it is not, enable it by right-clicking the text circled in the screen shot below and selecting **Subscribe**.



Click **Next** on the **Quick Start** screen.

c. Click the **Install Certificates** button to complete the installation. InstallRoot will display the **Certificate Action Summary** with the status of the installation.

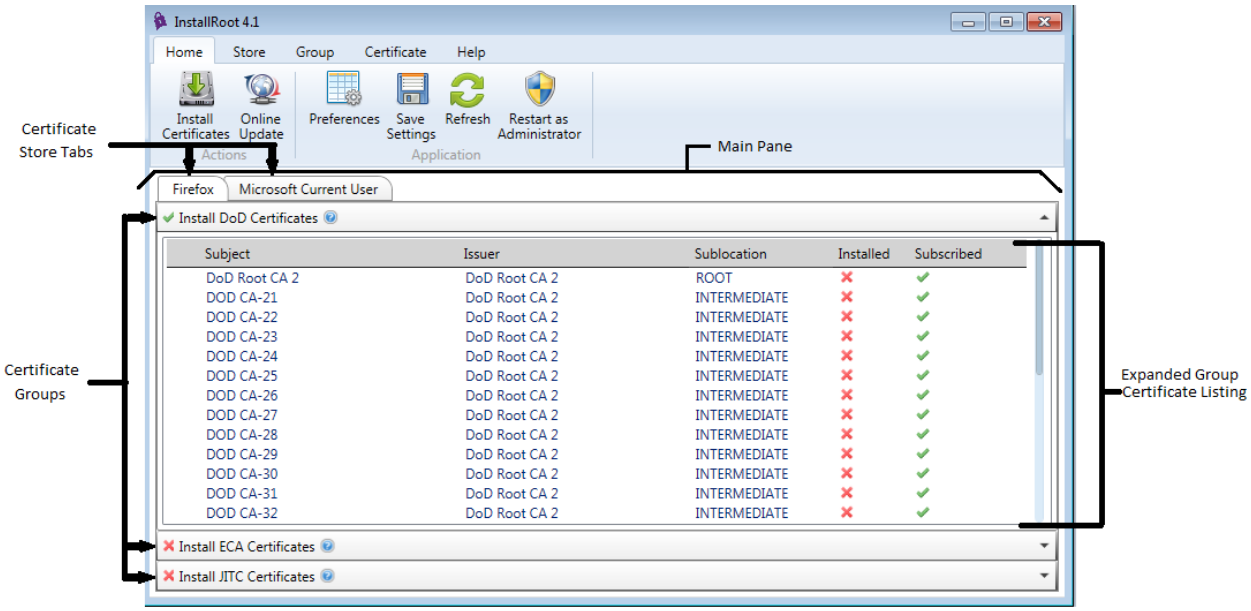


d. Click **Finish** to complete the **Quick Start**.

InstallRoot GUI Layout

InstallRoot is designed to facilitate the management of DoD PKI Certification Authority (CA) certificates and other PKI CA certificates that may be necessary to the conduct of DoD business across a variety of different certificate stores. The contents of each certificate store dictate whether applications (such as web browsers, email clients, and document viewers) that rely on that certificate store trust a particular PKI and the certificates it issues.

The main pane of the application contains a tabbed listing of Certificate Stores that InstallRoot is configured to manage. On each Certificate Store tab, there is a listing of Certificate Groups that are available for that Certificate Store. A Certificate Group can be expanded to show a detailed listing of certificates within the group, including each certificate's current installation status and whether it is targeted to be installed (as indicated by the "Subscribed" status). Individual certificates can be viewed by double-clicking on the certificate, and the subscription status for both Certificate Groups and individual certificates within a group can be toggled by clicking on its subscription indicator (✔ or ✘).



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.

The **Home** tab offers core functions like installing certificates, performing an online update to check for new certificates, and configuring preferences for automatic online update and InstallRoot service behavior.

The **Store** tab offers Certificate Store management functions – primarily adding and removing certificate stores to be managed by the tool. It also contains an NTAuth Comparison Report which displays differences between the contents of the local machine's NTAuth store and the domain controller's to help with replication troubleshooting.

The **Group** tab offers Certificate Group management functions – adding, removing, and retargeting the update source for Certificate Groups. It also offers an alternative way to update Certificate Group subscription status, using the Subscribe and Unsubscribe buttons.

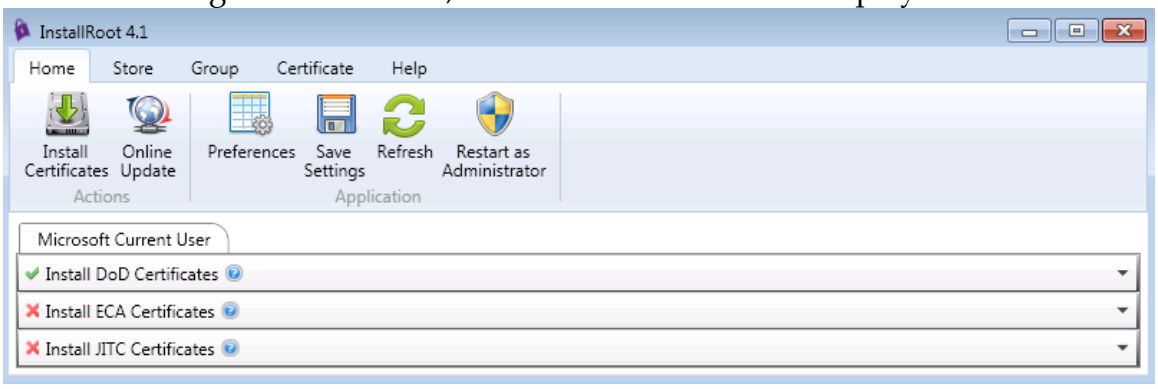
The **Certificate** tab provides the capability to export certificates from the tool in PEM, DER and PKCS7 format, as well as to uninstall certificates from currently managed Certificate Stores. It also offers buttons to update certificate subscription status, which can be helpful when there are several certificates whose status needs to be updated, since multiple certificates can be selected within the main pane prior to clicking the Subscribe or Unsubscribe button once to apply the action across all selected certificates.

Finally, the **Help** tab contains buttons to access this user guide, tool information, re-launch the Quick Start, and view the application logs.

InstallRoot Home Tab

The InstallRoot 4.1 GUI allows the user to select certificate group(s) or individual certificates to install in each Certificate Store managed by the tool.

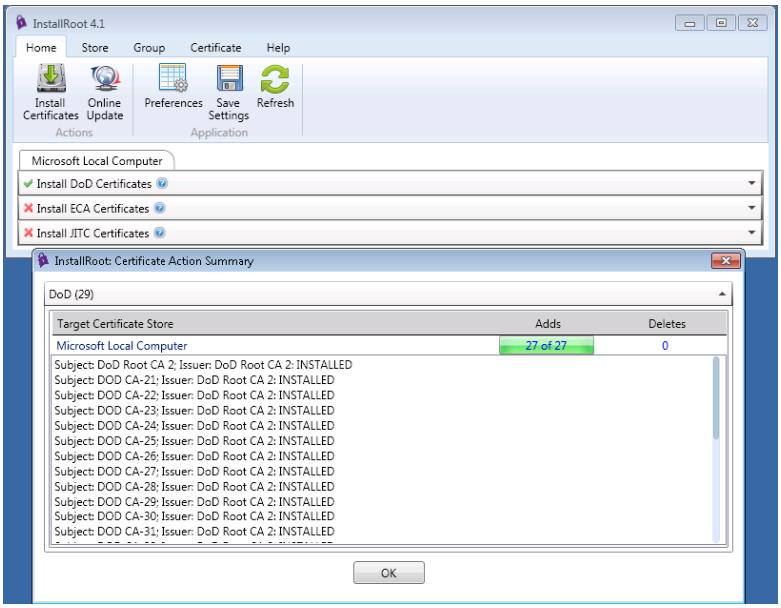
After launching **InstallRoot 4.1**, the **Home** screen will be displayed.



NOTE: In this screen shot, InstallRoot is running in the user context. If run as an administrator, the store displayed will be *Microsoft Local Computer* and the Restart as Administrator button will not be visible.

Install Certificates

The core capability of InstallRoot is to install certificates into trust stores. Click the **Install Certificates** button to install select groups and certificates. Information about how to select certificates by group or individually is covered in greater detail in the **Subscribing to Groups** or **Subscribing/Unsubscribing to Certificates Individually** sections. After the certificates are installed, the **Certificate Action Summary** window with the results of the installation will be displayed as shown below:



NOTE: Install Certificates only needs to be run once to install certificates in all managed trust stores; however, the desired subscriptions must be configured individually for each trust store.

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 that use NSS and then perform the desired operation. In most circumstances, NSS will only be used by Mozilla products such as Firefox or Thunderbird. Contact the system administrator if unsure of the application(s) using the NSS store on the system.

Online Update

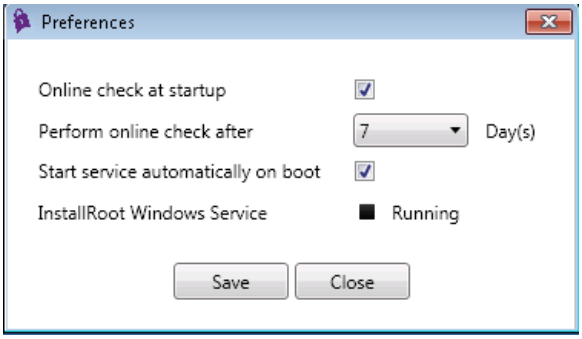
InstallRoot has the ability to accept InstallRoot TAMP messages to update certificate information within the tool. TAMP messages are digitally signed files containing CA certificates and associate instructions (such as add or remove) that can be used by InstallRoot to update managed trust stores. The **Online Update** function checks if there are new InstallRoot TAMP messages available and, if so, downloads and processes the messages.

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

1) To manually initiate an online update, navigate to the **Home** tab and click the **Online Update** button. InstallRoot will initiate a check and report back if there were new TAMP messages to process.
2) To control how InstallRoot automatically performs online updates, use the **Preferences** button. See the **Preferences** section below for an overview of options.

Preferences

InstallRoot has several settings that can be configured within the **Preferences** window. Navigate to the **Home** tab and click the **Preferences** button. The window below will be displayed.



- **Online check at startup**: Checking this will have InstallRoot check to see if an online update needs to be performed when the GUI is launched.
- **Perform online check after:** A drop-down menu that specifies the length of time that InstallRoot should wait between performing online update checks. The available options are 7 days, 14 days, 30 days, and 60 days.

  NOTE: When running as 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.
- **Start service automatically on boot:** Indicates if 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 indicator that shows whether the Windows service is stopped or running. If InstallRoot is being run with administrative privileges, clicking the square to left of the word **Running** will stop the service. If the service is stopped, clicking the play button will start the service. If logged on as a user without administrative privileges, the option will be greyed out, but the status of the service will still be displayed.

Save Settings

This setting will save any changes that have been made within the GUI. If changes have been made and the user attempts to close InstallRoot's GUI without saving, a window will prompt the user to save changes.

Refresh

This button will refresh information that may have been changed outside of the tool, such as the installation status of a certificate.

Restart as Administrator

If InstallRoot was launched without administrative privileges and the application needs to be run with administrative privileges, click this button to restart the application with administrative privileges (user will be prompted to provide appropriate credentials). Clicking this button provides the same functionality as launching InstallRoot by right-clicking the program and selecting **Run as administrator**.

NOTE: Any settings that were selected when running without administrative privileges are not preserved when the tool is re-launched with administrative privileges.

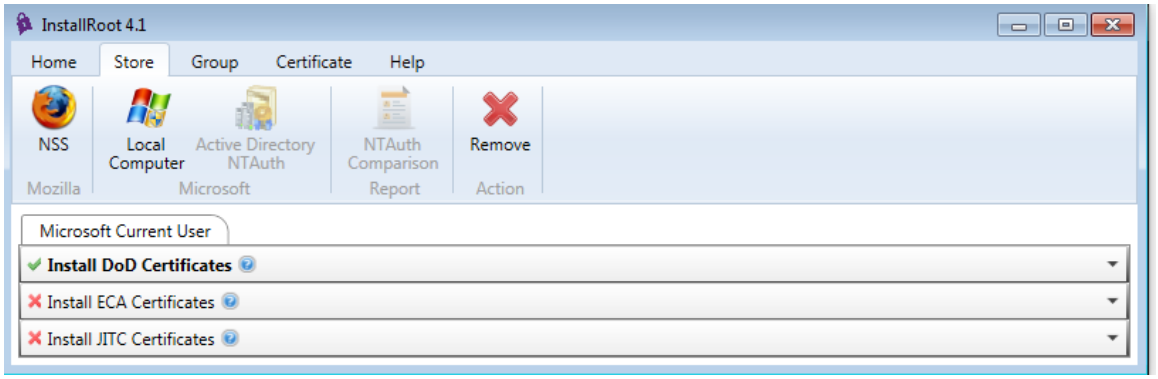
Store Tab

This tab displays the types of stores that are available to be managed by InstallRoot.

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

If the machine is domain-joined and the user has domain admin rights, the **Active Directory NTAuth** store will be available to add; otherwise it will be greyed out. For more information on the NTAuth store, refer to the **Active Directory NTAuth Store** section.

The screen shot below shows InstallRoot running without administrative privileges.

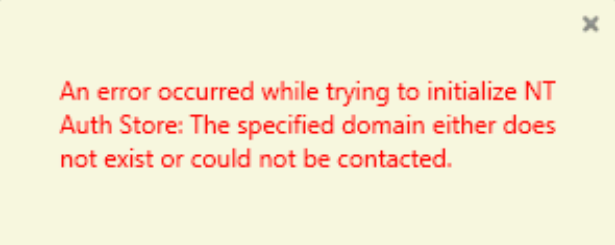


To add additional trust stores, refer to **Adding and Removing Managed Trust Stores** below.

Active Directory NTAuth Store

InstallRoot can be used to manage the Active Directory NTAuth store. In order to manage an NTAuth store, the user running InstallRoot must be a Domain Administrator. To manage the NTAuth store it is not necessary to run InstallRoot from a domain controller; just a machine in the domain.

NOTE: The Active Directory NTAuth button will be active when logged on to a machine as a local administrator if the machine is member of a domain. However, to manage an NTAuth store, domain administrative rights are required. If the button is clicked without those privileges, the below error will be displayed.

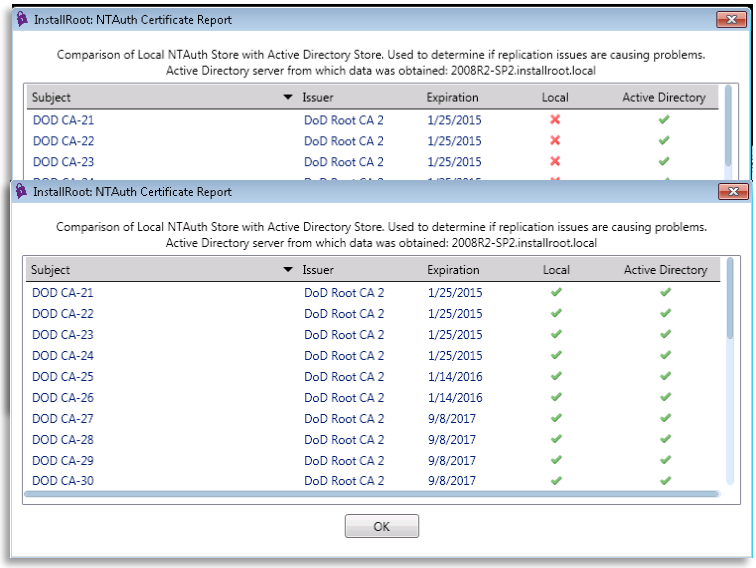


NOTE: InstallRoot cannot be used to initialize an NTAuth store within an Active Directory domain. It is recommended that the command line utility `CERTUTIL` be used to add at least one Certification Authority to the domain to initialize the NTAuth store; once the store has been initialized, InstallRoot can be used to manage it. See the Initializing the NTAuth Trust Store section in Appendix B.

1) To manage the **NTAuth** store, start InstallRoot and navigate to the **Store** tab.
2) Click the **Active Directory NTAuth** button.
3) A pop-up window will appear with a security warning stating that any actions in the NTAuth store impact the entire domain. Click **OK**.
4) A new store called **NTAuth** will be created. Select that tab.
5) The certificates in the NTAuth store for the domain can now be managed using the same procedures as for any other store types.
6) Once the NTAuth Store has been created, the **NTAuth Comparison Report** button becomes active**.** 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 top example shows an out-of-sync condition. The bottom example shows that the machine is in sync with 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.



Adding and Removing Managed Trust Stores

Currently InstallRoot can manage three types of trust stores: Microsoft Current User/Local Computer, Active Directory NTAuth, and NSS.

The Microsoft Current User/Local Computer stores control which PKIs Microsoft applications, such as Internet Explorer and Microsoft Outlook, trust. Many third-party applications that run on Microsoft operating systems, such as Google Chrome, also use the Microsoft stores.

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

The NSS store is used by Mozilla Firefox and Thunderbird, as well as certain other applications such as the Apache web server when run with mod_nss. InstallRoot supports NSS stores with passwords and in FIPS mode.

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.

To add a new store to be managed:

1) On the **Store** tab, click the button for the desired store type.
2) If adding an NSS store:
    a) The **Select an NSS Store …** dialogue will appear and automatically present any Firefox or Thunderbird profiles that InstallRoot has found on the system. Select the desired profile to add. If the desired profile or NSS store location is not listed, use the **Browse…** button to navigate to the correct location.
    b) In the **New Store Name** field, choose a unique name for the NSS trust store.
    c) Click **OK** when the trust store's name and location have been selected.

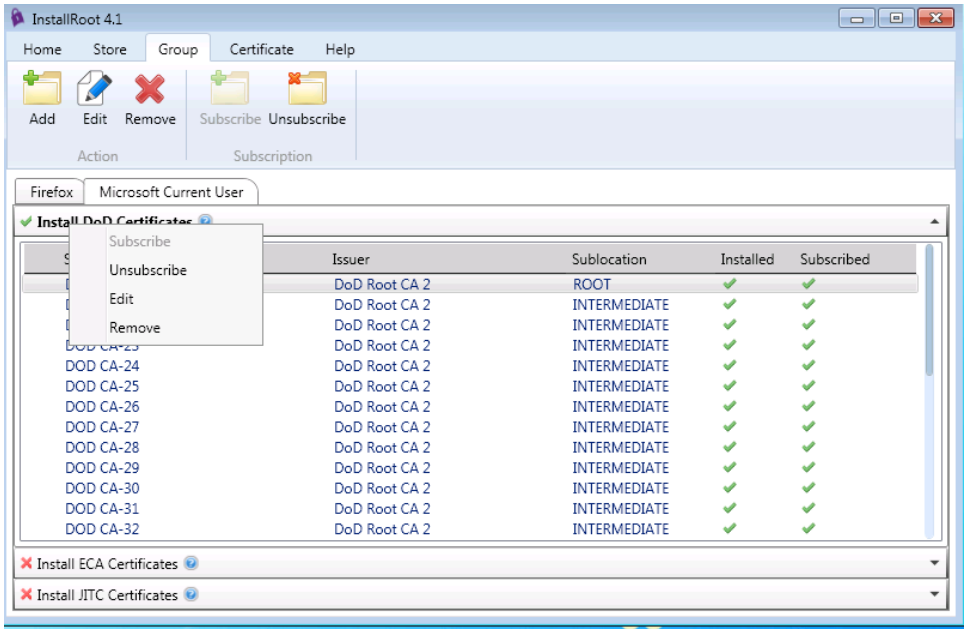
To remove a managed store:

1) On the **Store** tab, select the tab for the desired store to be removed**.**
2) Click the **Remove** button.
3) Confirm the deletion.

    NOTE: Once a store is removed, the configuration must be saved in order for the removal to be completed.

Group Tab

Certificate Groups are displayed throughout the InstallRoot application; the groups are visible in each trust store tab. Certificate groups are comprised of certificates and actions contained in an InstallRoot TAMP message. Options available in the **Group** tab are also available by right-clicking the group name as shown in the picture below.



By default, the following groups are created:

- **Install DoD Certificates:** Contains DoD PKI production Certification Authority 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.

Once a certificate group has been selected, the group name will become bold. To view all of the certificates within that group, click the ▼ button on the right side to display all the certificates in the table. For each listed certificate, the table displays the following:

- **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 Yes or ✕ for No)
- **Subscribed:** The certificate's subscription status in the selected trust stores (for Yes or ✕ for No). A subscribed certificate will be installed, deleted, or updated when the **Install Certificates** button is clicked.

NOTE: Certificates listed in red are marked for deletion. These certificates will display as subscribed, but after running an Install Certificates action should display as not installed, which is the desired behavior.

Adding Certificate Groups

To add Certificate Groups or to replace one that was removed, follow these steps:

1) Select the **Group** tab in the InstallRoot application toolbar.
2) Click the **Add** button that appears in the toolbar.
3) When prompted, specify the **Location** of the group. This will be a file system location or URL of an InstallRoot TAMP message (.ir4 file) that specifies the group's contents.
4) Click **OK**. The group will be added to the list in the main InstallRoot window.

Editing Certificate Groups

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.
4) Press **OK**.

Removing Certificate Groups

Select the group to be removed and click the **Remove** button, or right-click the group name and select **Remove** from the picklist.

Subscribing to Groups

Select the desired group and click the **Subscribe** button. By default, the **Install DoD Certificates** group will be subscribed.

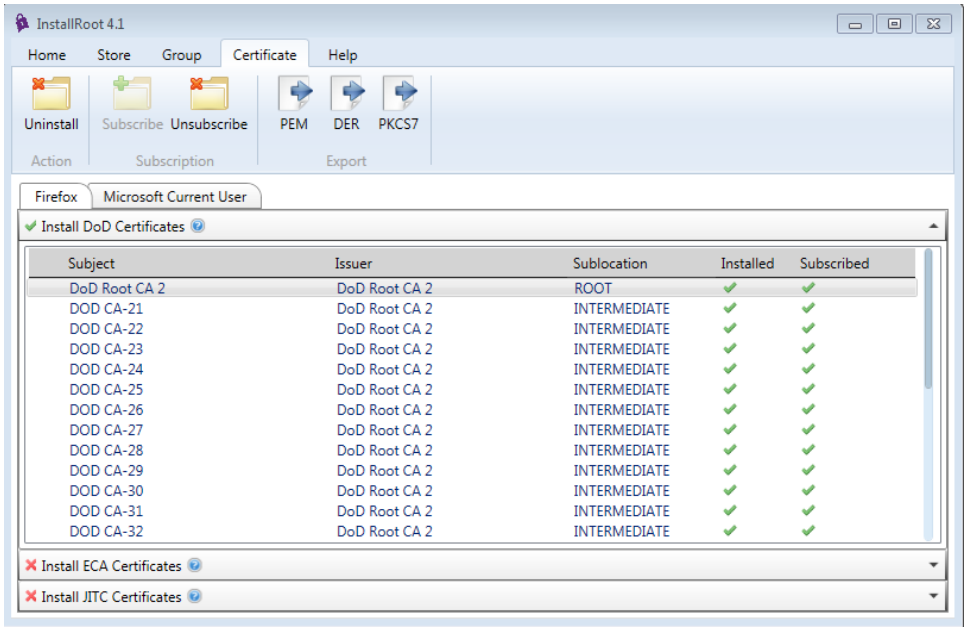
Unsubscribing from Groups

Select the desired group and click the **Unsubscribe** button.

NOTE: Unsubscribing from a group will not cause certificates in that group to be uninstalled from managed trust stores; unsubscribing will only stop any future updates from being processed for that group.

Certificate Tab

The **Certificate** tab displays actions that pertain to individual certificates, such as removing and/or exporting certificates.



Uninstalling Certificates

To uninstall individual and/or multiple certificates from a selected trust store, perform the following steps:

1) Navigate to the **Certificate** tab.
2) Select the appropriate trust store.
3) Click 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 **Ctl+A** will select all of the certificates in the group.
5) Click the **Uninstall** button in the **Certificate** tab.

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

Subscribing/Unsubscribing to Certificates Individually

Certificates can also be subscribed to and installed individually if desired. This type of fine-grained control is not commonly necessary, and it is recommended to manage subscriptions at the group level for most functions.

To subscribe to an individual certificate within a group, click the ✕ to change it to a ✔ .

To unsubscribe from an individual certificate, click the ✔ to change it to a ✕.
Subscriptions can also be managed for individual certificates using the buttons on the **Certificate** tab.

Once the desired subscriptions have been configured, navigate to the **Home** button and click **Install Certificates.** The individual certificates will be installed.

Exporting Certificates

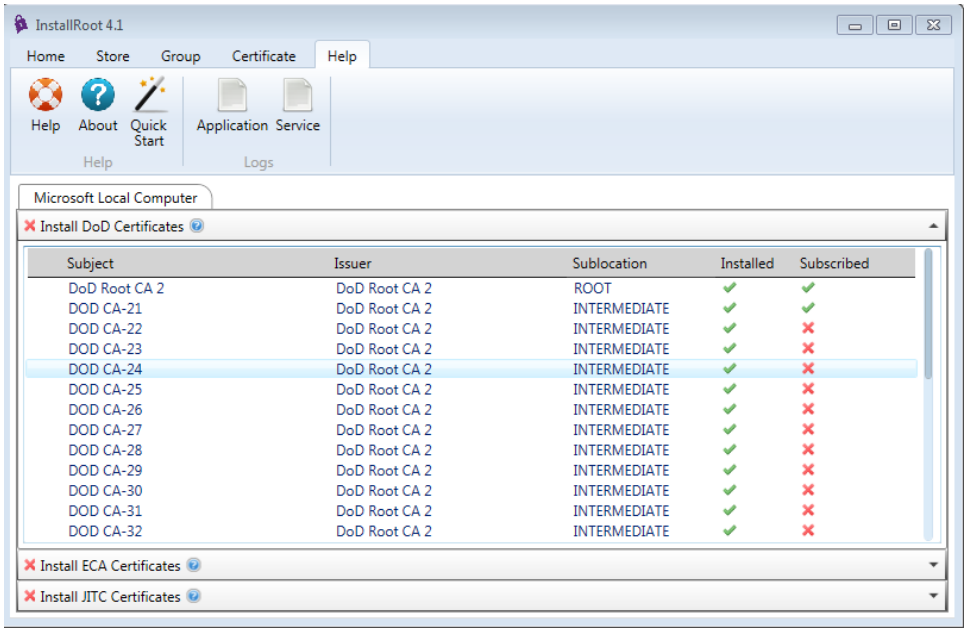
To export certificates to disk:

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 Export.p7b.
5) Click **Save**.

Help Tab

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



Help: Displays a PDF version of this user guide.

About: Displays the version number, the web site for DoD PKE information, and the email address for the DoD PKE group.

Quick Start: Restarts the Quick Start guide that is presented at first use.

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: NTAuth Trust Store and Log Information**.

Uninstalling InstallRoot

When updating InstallRoot versions, the best practice is to first uninstall any currently installed InstallRoot versions.

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

To uninstall InstallRoot:

1) Using the **Windows Start Menu**, navigate to InstallRoot. The default path is **All Programs > DoD-PKE > InstallRoot**.
2) Select **Uninstall InstallRoot 4**.
3) When prompted to confirm the uninstall, click **Yes.**

Alternative method 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**.

Command-Line Utility

The command-line utility can be run locally, from portable media, or even as a logon script. **Command Line Interface Exit Codes** are provided in Appendix B to facilitate using the utility in batch scripts.

Preparation

The command-line utility comes packaged within the .msi file.

If the utility was not pre-installed by an MSI package, verify the digital signature on the command-line executable file (.exe) by following the instructions in the **Verifying the Digital Signature on the Utility** section of this document.

Running InstallRoot

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\InstallRoot4\
```

2) Enter the desired command (see **Usage** section for available arguments) to run InstallRoot.

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 at http://iase.disa.mil/pki-pke under **PKE A-Z > Guides**.

Usage

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 online help within the CLI use: **InstallRoot.exe --help**

InstallRoot.exe: Installs 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 –-group: The command is not run on its own; instead it is used to identify targets for other commands. Multiple groups can be specified by separating groups with commas. For example: **InstallRoot.Exe --delete ECA,DoD,JITC** or **InstallRoot.exe --insert --group JITC**

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 --nssdb %APPDATA%\Roaming\Mozilla\Firefox\Profiles\vvof92ga.default**

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. The only difference between the two is that 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 --nssdb %APPDATA%\Roaming\Mozilla\Firefox\Profiles\vvof92ga.default**

  NOTE: If the NSS database is password-protected, InstallRoot will prompt for the password. To automate the password input use the --password parameter followed by the password.
- To delete all certificates from the appropriate Microsoft certificate store: **InstallRoot.exe --delete --group ECA,DoD,JITC**

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 --store: Used to identify one or more Microsoft certificate stores against which to perform an operation. This command is not run on its own; instead, it is used to identify targets for other commands. If the utility is run as an administrator, the allowable options for this are **MSCAPI_CU** and **MSCAPI_LC**. Otherwise, **MSCAPI_CU** is the only available option. If running InstallRoot as a Domain Administrator on a domain-joined machine, **NT_AUTH** is also an allowable option.

InstallRoot.exe --liststores: Lists all of the stores that can be used as inputs for the **--store** command. The available stores are **MSCAPI_LC**, **MSCAPI_CU**, and **NT_AUTH**.

InstallRoot.exe –-nssdb: Used to identify the path of an NSS store against which to perform an operation. This command is not run on its own; instead, it is used to identify targets for other commands. For example: **InstallRoot.exe –-insert –-group DoD,JITC --nssdb %APPDATA%\Roaming\Mozilla\Firefox\Profiles\vvof92ga.default**

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 --nssdb %APPDATA%\Roaming\Mozilla\Firefox\Profiles\vvof92ga.default**

InstallRoot.exe -- listkeys: Used to list the public keys for all certificates. The listkey command 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**

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

InstallRoot.exe --clearcache: Used to clear the InstallRoot cache folder located at %LOCALAPPDATA%/DoD-PKE/InstallRoot/4.1/cache

InstallRoot.exe --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: Used to define the path to the log file. Can be used with the **--level** command to define different logging levels. 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**

InstallRoot.exe -- certs: 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 -- 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: Specifies the format type to be used when exporting certificates.

InstallRoot.exe -- uri: Used to define an alternate location for a TAMP message. This location will override the defaults.

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

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

Windows Service

The Windows Service is used by InstallRoot to handle periodic update checks for certificate bundles. The service will automatically install and delete certificates according to the configured Certificate Group subscriptions.

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

When running, the service will check for updated InstallRoot TAMP messages at the interval that is specified by the **Perform online check after** interval in **Preferences**. It will do this by comparing the current date/time to the last time the service, or a user running the GUI as an administrator, initiated an update check. 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.

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

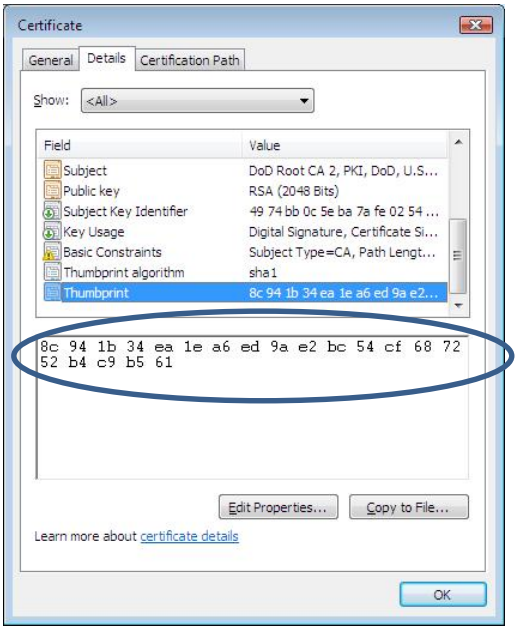
CA	Certification Authority
CN	Common Name
CLI	Command-Line Interface
DER	Distinguished Encoding Rules
DoD	Department of Defense
GUI	User Interface
MSI	Microsoft installer
NSS	National Security Systems (PKI) Network Security Service (Mozilla)
PEM	Privacy Enhanced Email
PKCS7	Public Key Cryptographic Standard 7
PKE	Public Key Enablement
PKI	Public Key Infrastructure
SIPRNet	Secret Internet Protocol Router Network
TAMP	Trust Anchor Management Protocol

Appendix B: NTAuth Trust Store and Log Information

Initializing the NTAuth Trust Store

InstallRoot can manage the NTAuth store, but only after the store has been initialized. The steps below will initialize the NTAuth store by installing the DoD Root CA 2 into the NTAuth store using `certutil`.

1) Log onto a domain controller with domain admin rights.
2) Install InstallRoot (if not already installed).
3) Navigate to the **Certificate** tab.
4) Expand the **Install DoD Certificates** group by clicking ▼.
5) Highlight the top certificate (**DoD Root CA 2**).
6) Click the **DER Export** button and select a directory to store the exported certificate.
7) Verify the thumbprint of the exported certificate:
    a. Open the certificate and select the **Details** tab.
    b. Scroll to the bottom of the window to view the thumbprint.
    c. Verify the DoD Root CA 2 thumbprint by calling the DoD PKI Help Desk at (800) 490-1643 or DSN 339-5600



8) Open an elevated command prompt using **Run as Administrator**, and navigate to the directory where the certificate was stored in the previous step.

9) Run this command:

```
certutil -dspublish -f
"DoD_Root_CA_2__05__DoD_Root_CA_2.cer" NTAuthCA
```

A message should display indicating that the certificate was added to the DS store and the dspublish command completed successfully.

InstallRoot Error Logging

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

- Service logs (by default):

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

- GUI logs:

  `%LOCALAPPDATA%\DoD-PKE\InstallRoot\4.1\InstallRoot.log`

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\4.1\`

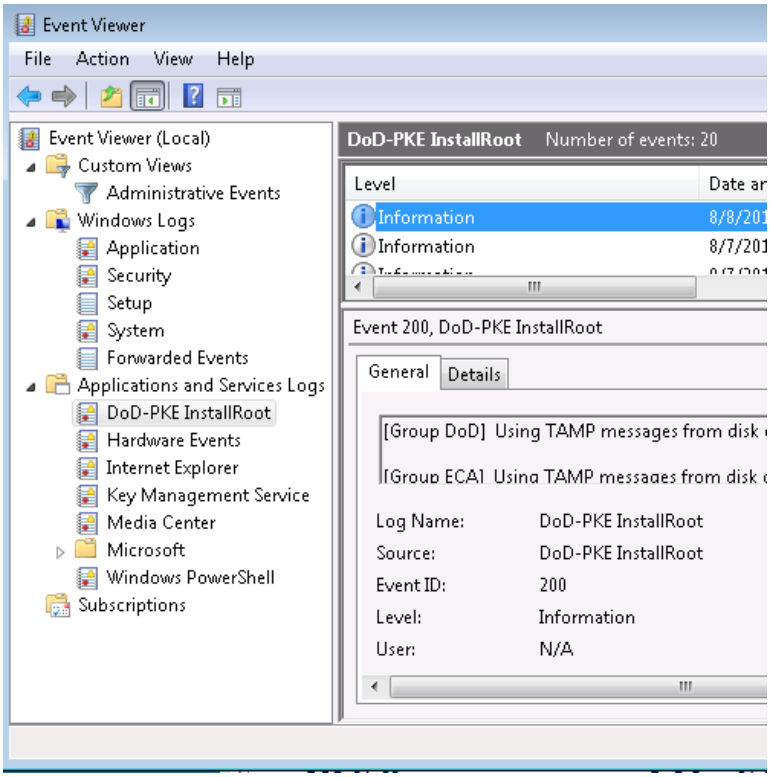
   To set the **DebugMode** flag for the user GUI events navigate to:

   `HKEY_CURRENT_USER\Software\DoD-PKE\InstallRoot\4.1`

   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.

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 command argument
2	Initialization error • 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 error • Export format option used without Export option error • No cache option used without Update option error • Unsupported group
4	Permissions error • Request update of MSCAPI Local Computer store without adequate permissions error. • Request update of NTAuth store without adequate permissions error. • Request update of NTAuth 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: Signature Verification Failure(SIGVERFAILURE)
7	Certificate Database Processor error: Signer Revoked (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 NTAuth 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 while creating the export directory - PathTooLongException, IOException, SecurityException, Generic Exception
18	Error while 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	Running NSS processes identified that will conflict with the importing and removal of certificates

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 4.1.

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
Untrusted	DoD Root CA 2	DoD Interoperability Root CA 1
Untrusted	DoD Root CA 2	US DoD CCEB Interoperability Root CA 1
Intermediate	DoD CA-25	DoD Root CA 2
Intermediate	DoD CA-26	DoD Root CA 2
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-25	DoD Root CA 2
Intermediate	DoD EMAIL CA-26	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 Root CA 2	US DoD CCEB Interoperability Root CA 1
Intermediate	**DoD Root CA 2	DoD Interoperability Root CA 1

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

External Certification Authority (ECA) PKI Certificates

Target CA Store	Subject CN	Issuer CN
Root	ECA Root CA 2	ECA Root CA 2
Intermediate	IdenTrust ECA CA 3	ECA Root CA 2
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
Untrusted	ECA Root CA 2	DoD Interoperability Root CA 1
Untrusted	ECA Root CA 2	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-26	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-26	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	DoD 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	** DoD JITC Root CA 2	US DoD CCEB JITC Interoperability Root CA 1
Intermediate	** DoD JITC Root CA 2	DoD Interoperability Root CA 1
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