InstallRoot 3.16 User Guide

2 June 2014

Version 3.1

DoD PKE Team

Revision History

Issue Date	Revision	Change Description
2/19/2010	2.0	Updated for v3.13 and moved to new PKE document style. Changed name to "User's Guide" from "Sys Admin Guide" based on the low level difficulty of content and intended reader of the paper.
4/25/2011	2.1	Appendix B: Known Issues and Forthcoming Changes updated
9/16/2011	2.2	Added usage instructions for command-line versions and updated information for release 3.15 of GUI.
1/5/2012	2.3	Added listing of InstallRoot-S certificates to Appendix D.
7/3/2012	2.4	Added information for InstallRoot SIPRNet Windows Installer.
11/2/2012	2.5	Updated DoD PKE support email address.
2/22/2013	2.6	Updated for 3.16
7/18/2013	2.7	Updated for 3.16 SIPR
1/8/2013	2.8	Updated Appendix D (DoD PKI NIPRNet Production Certificates) to include "type" of CA
2/13/2014	2.9	Updated Appendix D (External Certification Authority Certificates) to include IdenTrust ECA 4 certificates
4/11/2014	3.0	Updated Appendix D (External Certification Authority Certificates) to include Symantec Client ECA certificate
6/2/2014	3.1	Updated Appendix D (External Certification Authority Certificates) to include ORC ECA 5 certificates and (DoD PKI NIPRNet Production Certificates) to remove DoD PKI CAs and EMAIL CAs 19 and 20.

Contents

Table of Figures

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 validating all intermediate and root certificates in the issuance path and verifying that the root CA is trusted by the system.

For Microsoft products, trust is established by installing the CA certificate in the local system's trust store; for Mozilla NSS-based products, trust is determined by the presence and trust arguments associated with CA certificates in the system's NSS certificate database. If the issuing root CA is not trusted, all other certificates in the issuance path, including the end entity certificate, are considered untrusted.

InstallRoot is a utility which installs DoD-specific root and intermediate PKI CA certificates into trust stores on Microsoft servers and workstations, thereby establishing trust of the installed PKI CA certificates. It also provides interfaces for managing these CA certificates in the certificate stores on a system.

Both graphical user interface (GUI) and command-line versions of InstallRoot are available to suit different users' preferences and needs. Each version is distributed individually from the DoD PKE web site. The current versions include:

InstallRoot 3.16 NIPRNet Windows Installer: This package will install the InstallRoot NIPRNet GUI, providing installation and management capabilities for the DoD, External Certification Authority (ECA) and Joint Interoperability Test Command (JITC) PKI CA certificates. It provides options to manage certificates in both the Microsoft operating system and Firefox certificate stores.

InstallRoot 3.16 SIPRNet Windows Installer: This package will install the InstallRoot SIPRNet GUI, providing installation and management capabilities for the DoD Secret Internet Protocol Routing Network (SIPRNet) PKI (also known as the DoD Legacy SIPRNet PKI) and the National Security Systems (NSS) PKI root and intermediate CA certificates. It provides options to manage certificates in both the Microsoft operating system and Firefox certificate stores. This version should only be run on machines connected to Secret networks. This version is only available from the DoD PKE SIPRNet site.

InstallRoot-3.16A: This zipped archive contains an executable command-line version of InstallRoot which installs all of the DoD PKI root and intermediate CA certificates into the Microsoft operating system certificate store.

InstallRoot-3.16E: This zipped archive contains an executable command-line version of InstallRoot which installs all of the ECA root and intermediate CA certificates into the Microsoft operating system certificate store. InstallRoot-3.16E is an administrative release to keep versioning consistent.

InstallRoot-3.16J: This zipped archive contains an executable command-line version of InstallRoot which installs all of the JITC test PKI root and intermediate CA certificates into the Microsoft operating system certificate store. This version should only be run on test machines, not live assets.

InstallRoot-3.16S: This zipped archive contains an executable command-line version of InstallRoot which installs all of the DoD SIPRNet PKI and NSS PKI root and intermediate CA certificates into the Microsoft operating system certificate store. This version should only be run on machines connected to Secret networks. This version is only available from the DoD PKE SIPRNet site.

InstallRoot-3.16X: This zipped archive contains an executable command-line version of InstallRoot which installs all of the historical DoD and ECA root and intermediate CA certificates into the Microsoft operating system certificate store. These CA certificates have all expired or been decommissioned (have no outstanding valid end entity certificates) and are not necessary for operational systems.

The bulk of the instructions in this guide pertain to the InstallRoot GUI versions. Instructions for the various command-line versions are available in the Command-Line Utilities section.

System Requirements

Supported Platforms

Supported operating systems:

- Windows XP SP2 and SP3
- Windows Vista
- Windows 7
- Windows Server 2003 R2
- Windows Server 2008 and 2008 R2

Supported browsers:

- Internet Explorer 7, 8 and 9
- *Firefox 3.6 and 13

***NOTE:** FIREFOX IS SUPPORTED BY THE GUI VERSION OF THE TOOL ONLY. FIREFOX MUST BE INSTALLED PRIOR TO THE INSTALLROOT GUI FOR THE TOOL TO PROPERLY MANAGE THE FIREFOX CERTIFICATE STORE.

Java Runtime Environment (JRE)

A 32-bit Oracle JRE 1.7 is recommended for the InstallRoot Windows Installer (GUI) versions. A JRE is not required for the command-line utilities. The 32-bit JRE 1.7 can be downloaded from the Oracle/Java website.

User Privileges

Administrative privileges are required in order to install and run InstallRoot on Windows Vista, Windows 7, and Windows Server 2008. On Windows XP and Windows Server 2003, the program can be run as a non-privileged user, but in that case the tool is limited to accessing only the current user's certificate store. For a non-privileged user, note that the GUI version of the tool must be installed to a directory to which the user has write permissions.

When Windows XP and Windows 2003 users with administrative privileges run InstallRoot, the program manages the LOCAL_MACHINE branch of the system registry or certificate store. It installs ONLY authorized DoD root and intermediate CA certificates. This makes these certificates visible and usable by all accounts on that computer. In Windows Vista, Windows 7 and Windows 2008 the program has to be right-clicked "run as" administrator to be installed into LOCAL_MACHINE EVEN if logged on with administrative privileges

If the user running InstallRoot does not have administrative privileges, it will manage the CURRENT_USER branch, where it will install authorized DoD root and intermediate certificates, making them available only to that user.

Verifying the Digital Signature on the Utility

Before proceeding with this installation, verify that the utility executable (MSI or EXE) you are about to run has been digitally signed by DoD PKE Engineering Support. Follow these steps to verify the digital signature on the executable:

1. In Windows Explorer, navigate to the directory containing the executable package.
2. Right-click on the executable and select **Properties** from the pop-up menu.
3. The Properties window opens. Click the Digital Signatures tab.
4. Select the certificate and click **Details**. The Digital Signature Details window opens. The message "This digital signature is OK" will display when checking the signature on a machine with the DoD production PKI certificates installed. If the DoD production PKI certificates aren't installed (e.g. because InstallRoot has never been run on the machine before), the message "This signature is untrusted." will display.
5. Click **View Certificate** and select the **Certification Path** tab to verify the certification path. The certification path should read "DoD Root CA 2 > DoD CA-21 > CS.DoD PKE Engineering.DoDPKE60002."

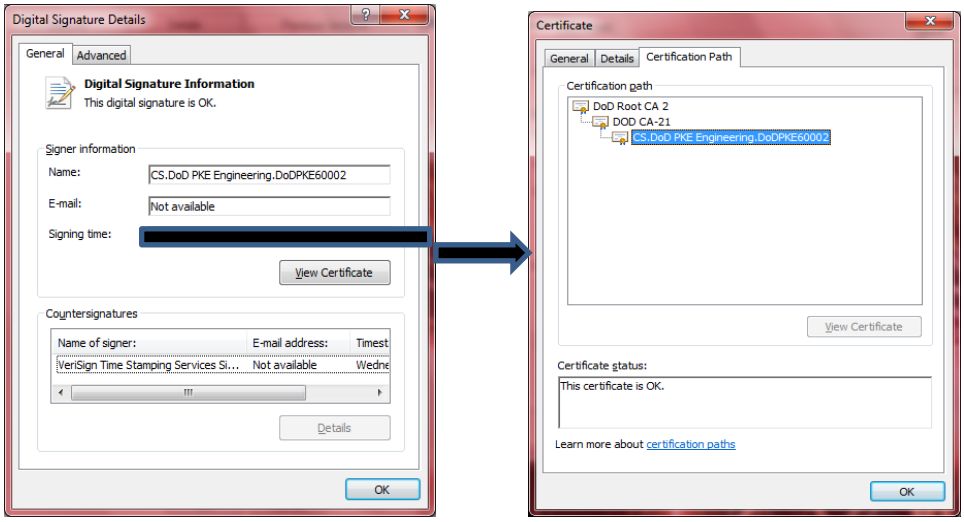


Figure 1: Verifying Digital Signature

6. If this is the first time the DoD production PKI certificates are being installed on the machine (as indicated by receipt of the "This signature is untrusted" message in step 4), perform the following additional steps to verify that the signature should be trusted:

a. On the Certificate Path tab, select DoD Root CA 2 and click **View Certificate**.
b. Select the DoD Root CA 2 certificate's **Details** tab and scroll to the bottom of the window to view the thumbprint.

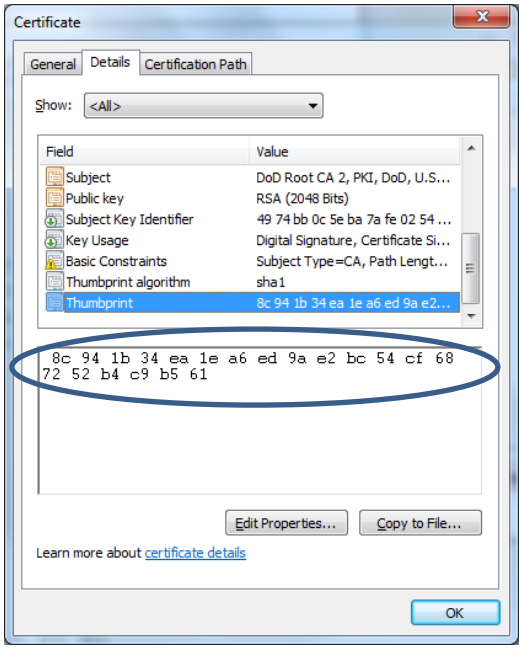


Figure 2: DoD Root CA 2 Thumbprint

c. Call the **DoD PKI Help Desk** at **(800) 490-1643** or **DSN 339-5600** to verify that the displayed thumbprint matches the thumbprint of record for DoD Root CA 2.

Installing and Running the InstallRoot GUI

Please uninstall any currently installed versions of InstallRoot before proceeding. Choose the appropriate installer for the classification level of your device – NIPRNet for unclassified environments and SIPRNet for secret environments.

Running the InstallRoot Windows Installer

1) After verifying the digital signature on the InstallRoot Windows Installer (MSI) file as described in the Verifying the Digital Signature on the Utility section of this guide, double-click the InstallRoot MSI to launch the installation wizard.
2) On the **Welcome** screen of the wizard, click **Next.**
3) On the **Configure Shortcuts** screen of the wizard, uncheck the boxes for any shortcuts which should not be created and click **Next.**
4) On the **Select Installation Folder** screen of the wizard, enter the desired installation location for the tool and click **Next**. The default path is C:\Program Files\DoD-PKE\InstallRoot 3.x.x\. On 64-bit operating systems, the x86 program files directory will be used by default.

   NOTE: IF THE TOOL IS BEING INSTALLED BY A NON-PRIVILEGED USER, ENSURE THAT A DIRECTORY TO WHICH THE USER HAS WRITE PERMISSIONS IS SELECTED IN THIS STEP.
5) On the **Ready to Install** screen, click **Install** to install the program.
6) When the wizard completes installation, click **Finish**

Running the Tool

1) Using the Windows Start Menu, navigate to All Programs > DOD-PKE > InstallRoot > InstallRoot 3.x.

   NOTE: IF A JAVA JRE NOT FOUND ERROR IS DISPLAYED, PLEASE INSTALL AN APPROPRIATE JRE (SEE **JAVA RUNTIME ENVIRONMENT** IN THE **SYSTEM REQUIREMENTS** SECTION FOR THE RECOMMENDED JRE VERSION).
2) InstallRoot 3.x.x will launch, displaying the Standard Mode screen. For instructions on using the tool in Standard and Advanced modes, see the following sections.

Standard Mode

InstallRoot 3 standard mode allows the user to select both certificate group(s) to install and a trust store in which to install them.

Selecting Certificates to be Installed

1) After launching **InstallRoot 3.x.x**, the screen in Figure 3 or Figure 4 below will display.
2) Select the certificate group(s) to be installed by checking the appropriate boxes:

Unclassified/NIPRNet systems

- Install DoD NIPRNet Certificates on systems using the operational DoD PKI
- Install JITC and O&M Certificates on **non-operational or test systems ONLY**
- Install External Certification Authority (ECA) Certificates on systems that need to accept ECA certificates from DoD partners who do not have Common Access Cards (CACs) or other DoD PKI certificates

Secret/SIPRNet systems

- Install NSS SIPRNet Certificates on systems using the NSS PKI; typically all secret systems will rely on the NSS PKI for SIPRNet token support and new device (e.g. web site) certificates
- Install SIPR Pilot Certificates on systems using the Legacy SIPRNet PKI for interaction with older device certificates and user software certificates

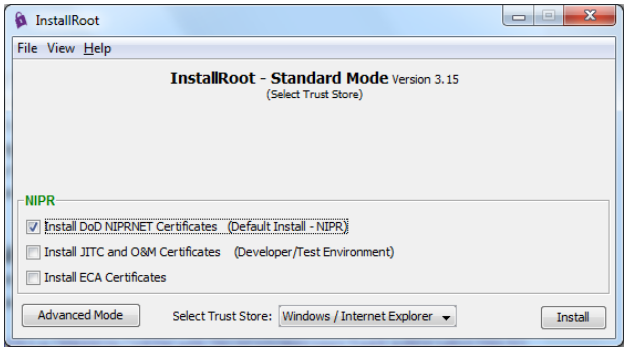


Figure 3: IntallRoot NIPRNet GUI Standard Mode

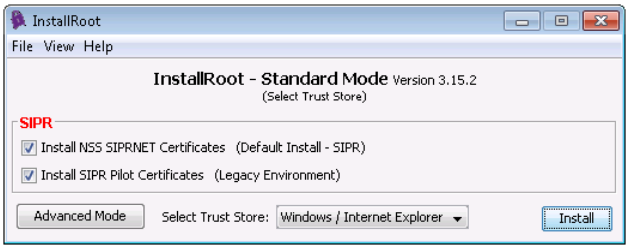


Figure 4: InstallRoot SIPRNet GUI Standard Mode

Selecting the Trust Store for Certificate Installation

1) In the **Select Trust Store** pick list in the bottom center of the window, select the trust store to which the certificates will be installed: **Windows / Internet Explorer** or **Firefox / Mozilla / Netscape.**

NOTE: TO INSTALL CERTIFICATES IN BOTH THE WINDOWS AND FIREFOX TRUST STORES, RUN THE TOOL TWICE, ONCE SELECTING THE WINDOWS/INTERNET EXPLORER STORE, AND ONCE SELECTING THE FIREFOX/MOZILLA/NETSCAPE STORE.

2) When selecting the **Firefox / Mozilla / Netscape** trust store, a prompt will display asking the user to select from a list of Firefox user trust stores found on your system. Please allow InstallRoot a few minutes to identify and locate user trust stores on the system in order to display the list. Select the desired user trust store and click **OK** when prompted.

Installing Certificates

1) Once the appropriate certificate group(s) and trust store are selected, click **Install** to install the certificates.

   NOTE: THE MOZILLA/FIREFOX/NETSCAPE TRUST STORES MAY TAKE A FEW MINUTES TO INSTALL

2) Upon completion of the installation, a notification pop-up will display indicating the number of certificates that were successfully installed to the selected trust store.

Advanced Mode

Advanced mode allows the user to manage individual certificates in the Windows and Firefox certificate stores. Specific certificates can also be selected and exported to disk as .cer files.

Switching Between Standard and Advanced Modes

Advanced mode can be reached from the Standard mode screen by clicking the **Advanced Mode** button in the lower left of the window or by selecting **View > Advanced Mode** from the menu bar. To return to Standard mode from Advanced mode, click the **Standard Mode** button in the upper left of the Advanced Mode window or select **View > Standard Mode** from the menu bar.

Selecting a Trust Store

To select the trust store for which to manage certificates:

1) In the **Select Trust Store** picklist in the upper right corner of the window, select the trust store for which to manage certificates: **Windows / Internet Explorer** or **Firefox / Mozilla / Netscape.**
2) When selecting the **Firefox / Mozilla / Netscape** trust store, a prompt will display asking the user to select from a list of Firefox user trust stores found on the system. Please allow InstallRoot a few minutes to identify and locate user trust stores on your system in order to display the list. Select the desired user trust store and click **OK** when prompted.

Selecting Certificate Groups for Display

In Advanced mode, the user can select a certificate group or groups to display a table of all certificates contained in the group(s) as shown in Figure 5 and Figure 6 below. To select a certificate group, click on its name in the left column. Selected groups will display as blue-highlighted cells, as the DoD NIPRNet and SIPRNet Certificates group in Figure 5 and Figure 6 is shown. Multiple groups may be selected simultaneously. To deselect a group, click on its name again.

The certificate group options are:

Unclassified/NIPRNet systems

- **DoD NIPRNet Certificates:** Contains DoD PKI production CA certificates
- **JITC and O&M Certificates:** Contains DoD test PKI CA certificates
- **ECA Certificates:** Contains certificates from the DoD-sponsored ECA PKI serving DoD partners who are not eligible for CACs or DoD PKI certificates

Secret/SIPRNet systems

- **NSS SIPRNet Certificates:** Contains NSS PKI production CA certificates
- **SIPR Pilot Certificates:** Contains DoD Legacy SIPRNet PKI CA certificates

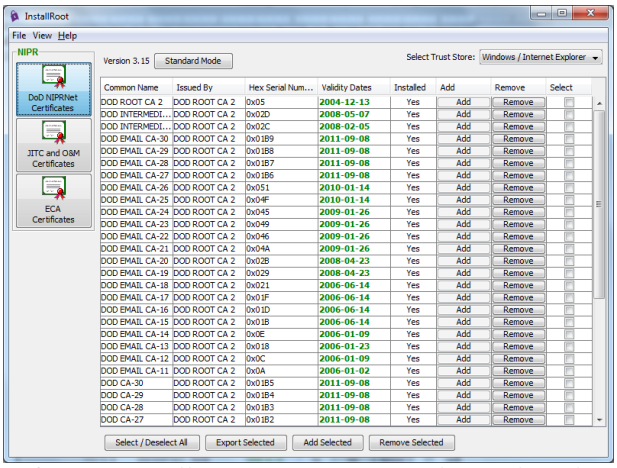


Figure 5: InstallRoot NIPRNet GUI Advanced Mode

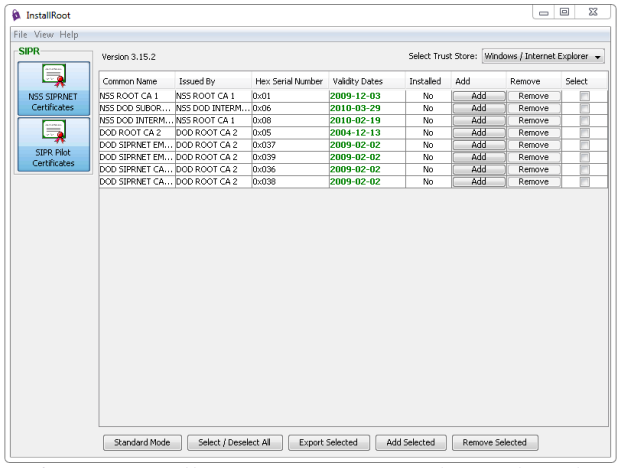


Figure 6: InstallRoot SIPRNet GUI Advanced Mode

Once a certificate group or groups has been selected, all of the certificates within that group will display in the certificates table. For each listed certificate, the table displays the following:

- **Common Name:** The certificate subject common name (CN)
- **Issued By:** The certificate issuer CN
- **Hex Serial Number:** The certificate serial number expressed as a hexadecimal
- **Validity Dates:**
  - For time-valid certificates, the certificate issuance date – expiration date (in green text)
  - For expired certificates, the text "Expired as of [certificate expiration date]" (in red text)

  NOTE: TO VIEW THE FULL RANGE OF INFORMATION IN THIS COLUMN, EXPAND THE WINDOW AND/OR VALIDITY DATES COLUMN.
- **Installed:** The certificate's installation status in the selected trust store (Yes or No)
- **Add button:** Clicking this button adds the certificate in the button's row to the selected trust store
- **Remove button:** Clicking this button removes the certificate in the button's row from the selected trust store
- **Select checkbox:** Checking this box indicates that the certificate in the checkbox's row will be included in any bulk actions performed by clicking the buttons at the bottom of the window (Export Selected, Add Selected or Remove Selected)

Adding and Removing Certificates

To add or remove individual certificates from the selected trust store:

Click the **Add** or **Remove** button (depending on the desired action) in the row of the certificate to be added or removed. Verify that the **Installed** column has been updated to reflect the desired certificate status in the trust store (**Yes** for an **Add** action or **No** for a **Remove** action).

To add or remove multiple certificates from the selected trust store:

1) Check the boxes in the **Select** column for each certificate to be added or removed.

   NOTE: THE **SELECT/DESELECT ALL** BUTTON IN THE BOTTOM BUTTON ROW IS A TOGGLE THAT WHEN CLICKED WILL CHECK ALL OF THE BOXES IN THE SELECT COLUMN; WHEN CLICKED AGAIN, IT WILL UNCHECK ALL OF THE BOXES.

2) Click the **Export Selected** button in the bottom button row. Verify that the **Installed** column has been updated to reflect the desired certificate statuses in the trust store (**Yes** for an **Add** action or **No** for a **Remove** action).

Exporting Certificates

To export certificates to disk:

1) Check the boxes in the **Select** column for each certificate to be exported.

   NOTE: THE **SELECT/DESELECT ALL** BUTTON IN THE BOTTOM BUTTON ROW IS A TOGGLE THAT WHEN CLICKED WILL CHECK ALL OF THE BOXES IN THE SELECT COLUMN; WHEN CLICKED AGAIN, IT WILL UNCHECK ALL OF THE BOXES.

2) Click the **Export Selected** button in the bottom button row.
3) In the **Open** window, navigate to the directory to which you would like to export the selected certificates.
4) In the **File Name** field, ensure that the path to the export directory is displayed. Do not enter a specific file name.
5) Press enter or click **Open** to export the certificates to the selected directory. Individual certificates will be exported with the file naming convention Subject_CN__Serial_Number__Issuer_CN.cer.

Uninstalling InstallRoot

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

To uninstall InstallRoot:

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

Command-Line Utilities

The command-line utilities can be run locally, from portable media, or even as logon scripts.

Preparation

The command-line utilities come packaged within zip archives. No installation beyond extraction of the archive and validation of its contents is necessary.

1) Extract the contents of the .zip archive by right-clicking on the archive, selecting "**Extract All…**" from the pick list, entering the desired extraction location in the pop-up window and clicking **Extract**.
2) Verify the digital signature on the command-line executable file (.exe) that was extracted from the .zip archive by following the instructions in Verifying the Digital Signature on the Utility.

Running the Tool

To run the utility locally or from portable media

1) In a command prompt, navigate to the directory containing the command-line executable.
2) Enter the desired command (see Options section for available arguments) to run the tool.

NOTE: ON WINDOWS VISTA, 7, AND SERVER 2008, RUN THE COMMAND PROMPT AS AN ADMINISTRATOR TO ENSURE THAT ALL TOOL OUTPUT IS VISIBLE. IF THE COMMAND PROMPT IS NOT OPEN WITH ADMINISTRATIVE PRIVILEGES, ENTERED COMMANDS WILL SPAWN A NEW WINDOW WHICH WILL CLOSE IMMEDIATELY UPON COMPLETION OF EXECUTION OF THE COMMAND, RESULTING IN THE USER NOT BEING ABLE TO VIEW THE TOOL OUTPUT.

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

Usage

There are four core commands available with the InstallRoot command-line utilities: Install certificates (the default behavior), delete certificates (executed using –d), list certificates (executed using –l), and view tool help (executed using –h). This section shows the optional arguments that may be used in combination with each core command. See **Options** for a description of the behavior of each core command and optional argument. Replace <num_letter> with the release number and version letter

included at the end of the executable name you wish to run; for example, InstallRoot_v3.16A. Optional arguments are displayed in square [ ] brackets.

To install certificates: InstallRoot_v<num_letter> [-s]
To delete certificates: InstallRoot_v<num_letter> -d [-f] [-s]
To list certificates: InstallRoot_v<num_letter> -l
To view tool help: InstallRoot_v<num_letter> -h

Options

Arguments shown in angle <> brackets are mandatory; arguments in square [ ] brackets are optional.

-d

This option deletes certificates from the default system store.

Usage:
```
-d
```

Example:
```
InstallRoot_v3.16A -d
```

-f

This option is used with the delete (-d) option to force the deletion of certificates without confirmation from the user.

Usage:
```
-d -f
```

Example:
```
InstallRoot_v3.16A -d -f
```

-h

This option displays help information for the tool.

Usage:
```
-h
```

Example:
```
InstallRoot_v3.16A -h
```

-l

This option lists the certificate information contained in a file store.

Usage:

```
-l
```

Examples:

```
InstallRoot_v3.16A -l
```

-s

This option can be used in combination with the install and delete options to run the commands in silent mode, so that status and results of the program are not output.

Usage:

```
-s
```

Examples:

```
InstallRoot_v3.16A –s
InstallRoot_v3.16A –d -s
```

Appendix A: Supplemental Information

Please use the links below for additional information 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 technical support through the email address below.
dodpke@mail.mil

Appendix B: Known Issues

If errors are encountered while using InstallRoot, please contact technical support at dodpke@mail.mil. In addition, please collect log files for troubleshooting purposes. InstallRoot log files are located at **<InstallRoot Installed Parent Directory>\DoD-PKE\InstallRoot\error.log** and **<InstallRoot Installed Parent Directory>\DoD-PKE\InstallRoot\output.log**

"Insufficient Privileges" Error Message During Installation

Administrative privileges are not required to install and run InstallRoot on Windows XP and Server 2003; however, it must be installed to a directory to which the current user has write privileges. Attempting to install InstallRoot to an area without write privileges will result in error message stating "insufficient privileges". Select **Cancel** to exit the installation.

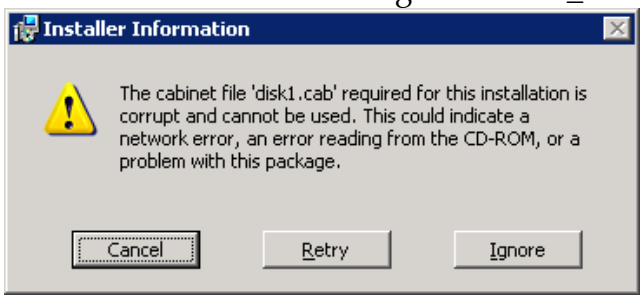
Running in Windows XP/2003 without Administrative Rights

Because of Windows security features, users without administrative rights may see a Root Certificate Store dialog box appear briefly, and then vanish for each trusted root certificate inserted to or deleted from the computer's root system registry

Unsuccessful InstallRoot Download

If InstallRoot did not completely download, the following error may display when installing the application:

Error received when running Installroot_3.13.msi



Attempt to download InstallRoot again, if the problem persists please contact technical support at dodpke@mail.mil.

Menu Incorrectly Displayed

Due to a mismatch on the frame size, the main menu will display the "InstallRoot - Standard Mode" name incorrectly when viewing the application in Windows XP Style appearance in Windows XP. This bug does not affect the functionality of the application.

Appendix C: New in Release 3.16

The following features are new in version 3.16:

- Added new NIPRNet CA certificates for CA-31, CA-32, Email CA-31, and Email CA-32.
- Added new SIPRNet NSS CA-2 certificate.

The following features are new in version 3.16.2:

- Added new IdenTrust ECA 4 certificate.

Appendix D: Included Certificates

The following certificates are included in release 3.16 of the InstallRoot tools. Highlighted rows denote new certificates in this release. Certificates removed in this release are noted separately.

DoD PKI NIPRNet Production Certificates

Applicable InstallRoot Versions: InstallRoot 3.16 GUI, InstallRoot-3.16A

Target CA Store	Subject CN	Type	Issuer CN	Not Before (GMT)	Not After (GMT)
Root	DoD Root CA 2	N/A	DoD Root CA 2	12/13/2004 15:00	12/5/2029 15:00
Intermediate	DoD Intermediate CA-1	N/A	DoD Root CA 2	2/5/2008 15:36	2/4/2018 14:36
Intermediate	DoD Intermediate CA-2	N/A	DoD Root CA 2	5/7/2008 14:44	5/7/2018 13:44
Intermediate	DoD CA-21	Software	DoD Root CA 2	1/26/2009 16:35	1/25/2015 16:35
Intermediate	DoD CA-22	Software	DoD Root CA 2	1/26/2009 20:18	1/25/2015 20:18
Intermediate	DoD CA-23	Hardware	DoD Root CA 2	1/26/2009 16:38	1/25/2015 16:38
Intermediate	DoD CA-24	Hardware	DoD Root CA 2	1/26/2009 20:23	1/25/2015 20:23
Intermediate	DoD CA-25	Hardware	DoD Root CA 2	1/14/2010 17:33	1/14/2016 17:33
Intermediate	DoD CA-26	Hardware	DoD Root CA 2	1/14/2010 17:38	1/14/2016 17:38
Intermediate	DoD CA-27	Software	DoD Root CA 2	9/8/2011 15:50	9/8/2017 15:50
Intermediate	DoD CA-28	Software	DoD Root CA 2	9/8/2011 15:57	9/8/2017 15:57
Intermediate	DoD CA-29	Hardware	DoD Root CA 2	9/8/2011 15:58	9/8/2017 15:58
Intermediate	DoD CA-30	Hardware	DoD Root CA 2	9/8/2011 15:59	9/8/2017 15:59
Intermediate	DoD CA-31	Hardware	DoD Root CA 2	1/16/2013 14:49	01/16/2019 14:49
Intermediate	DoD CA-32	Hardware	DoD Root CA 2	2/04/2013 20:44	02/04/2019 20:44
Intermediate	DoD EMAIL CA-21	Software	DoD Root CA 2	1/26/2009 16:41	1/25/2015 16:41
Intermediate	DoD EMAIL CA-22	Software	DoD Root CA 2	1/26/2009 20:25	1/25/2015 20:25
Intermediate	DoD EMAIL CA-23	Hardware	DoD Root CA 2	1/26/2009 16:43	1/25/2015 16:43
Intermediate	DoD EMAIL CA-24	Hardware	DoD Root CA 2	1/26/2009 20:26	1/25/2015 20:26
Intermediate	DoD EMAIL CA-25	Hardware	DoD Root CA 2	1/14/2010 17:36	1/14/2016 17:36
Intermediate	DoD EMAIL CA-26	Hardware	DoD Root CA 2	1/14/2010 17:39	1/14/2016 17:39
Intermediate	DoD EMAIL CA-27	Software	DoD Root CA 2	9/8/2011 16:00	9/8/2017 16:00
Intermediate	DoD EMAIL CA-28	Software	DoD Root CA 2	9/8/2011 16:01	9/8/2017 16:01
Intermediate	DoD EMAIL CA-29	Hardware	DoD Root CA 2	9/8/2011 16:02	9/8/2017 16:02
Intermediate	DoD EMAIL CA-30	Hardware	DoD Root CA 2	9/8/2011 16:03	9/8/2017 16:03
Intermediate	DoD EMAIL CA-31	Hardware	DoD Root CA 2	1/16/2013 14:52	01/16/2019 14:52
Intermediate	DoD EMAIL CA-32	Hardware	DoD Root CA 2	2/04/2013 20:48	02/04/2019 20:48

Removed in 3.16

Target CA Store	Subject CN	Issuer CN	Not Before (GMT)	Not After (GMT)
Intermediate	DoD CA-11	DoD Root CA 2	1/2/2006 16:24	1/1/2012 16:24
Intermediate	DoD CA-12	DoD Root CA 2	1/9/2006 13:47	1/8/2012 13:47
Intermediate	DoD CA-13	DoD Root CA 2	1/23/2006 16:49	1/22/2012 16:49
Intermediate	DoD CA-14	DoD Root CA 2	1/9/2006 13:57	1/8/2012 13:57
Intermediate	DoD CA-15	DoD Root CA 2	6/14/2006 15:22	6/13/2012 23:00
Intermediate	DoD CA-16	DoD Root CA 2	6/14/2006 16:58	6/14/2012 15:58
Intermediate	DoD CA-17	DoD Root CA 2	6/14/2006 17:09	6/14/2012 16:09
Intermediate	DoD CA-18	DoD Root CA 2	6/14/2006 17:16	6/14/2012 16:16
Intermediate	DoD CA-19	DoD Root CA 2	4/23/2008 20:57	4/23/2014 19:57
Intermediate	DoD CA-20	DoD Root CA 2	4/23/2008 21:05	4/23/2014 20:05
Intermediate	DoD EMAIL CA-11	DoD Root CA 2	1/2/2006 16:45	1/1/2012 16:45
Intermediate	DoD EMAIL CA-12	DoD Root CA 2	1/9/2006 13:54	1/8/2012 13:54
Intermediate	DoD EMAIL CA-13	DoD Root CA 2	1/23/2006 16:54	1/22/2012 16:54
Intermediate	DoD EMAIL CA-14	DoD Root CA 2	1/9/2006 14:00	1/8/2012 14:00
Intermediate	DoD EMAIL CA-15	DoD Root CA 2	6/14/2006 16:38	6/14/2012 15:38
Intermediate	DoD EMAIL CA-16	DoD Root CA 2	6/14/2006 17:04	6/14/2012 16:04
Intermediate	DoD EMAIL CA-17	DoD Root CA 2	6/14/2006 17:13	6/14/2012 16:13
Intermediate	DoD EMAIL CA-18	DoD Root CA 2	6/14/2006 17:20	6/14/2012 16:20
Intermediate	DoD EMAIL CA-19	DoD Root CA 2	4/23/2008 21:03	4/23/2014 20:03
Intermediate	DoD EMAIL CA-20	DoD Root CA 2	4/23/2008 21:08	4/23/2014 20:08

NSS PKI Certificates

Applicable InstallRoot Version: InstallRoot-3.16S, IntallRoot-3.16 SIPRNet GUI

Target CA Store	Subject CN	Issuer CN	Not Before (GMT)	Not After (GMT)
Root	NSS Root CA 1	NSS Root CA 1	12/03/2009 22:06	11/28/2029 22:06
Intermediate	NSS DoD Intermediate CA 1	NSS Root CA 1	02/19/2010 16:31	11/28/2029 22:06
Intermediate	NSS DoD Subordinate CA 1	NSS DoD Intermediate CA 1	03/29/2010 16:25	03/26/2020 16:25
Intermediate	NSS CA-2	NSS DoD Intermediate CA 1	06/06/2013 06:28	06/04/2023 06:36

DoD Legacy SIPRNet PKI Certificates

Applicable InstallRoot Version: InstallRoot-3.16S, IntallRoot-3.16 SIPRNet GUI

Target CA Store	Subject CN	Issuer CN	Not Before (GMT)	Not After (GMT)
Root	DoD Root CA 2	DoD Root CA 2	12/13/2004 15:00	12/05/2029 15:00
Intermediate	DOD SIPRNet CA-21	DoD Root CA 2	02/02/2009 20:44	02/01/2015 20:44
Intermediate	DOD SIPRNet CA-22	DoD Root CA 2	02/02/2009 18:58	02/01/2015 18:58

Intermediate	DOD SIPRNet EMAIL CA-21	DoD Root CA 2	02/02/2009 20:49	02/01/2015 20:49
Intermediate	DOD SIPRNet EMAIL CA-22	DoD Root CA 2	02/02/2009 19:39	02/01/2015 19:39

Removed in 3.16 SIPRNet GUI Version

Target CA Store	Subject CN	Issuer CN	Not Before (GMT)	Not After (GMT)

DoD Test PKI (JITC and O&M) Certificates

Applicable InstallRoot Versions: InstallRoot 3.16 GUI, InstallRoot-3.16J

Target CA Store	Subject CN	Issuer CN	Not Before (GMT)	Not After (GMT)
Root	DoD JITC Root CA 2	DoD JITC Root CA 2	7/15/2005 3:31	7/4/2030 3:31
Intermediate	DOD JITC CA-21	DoD JITC Root CA 2	12/30/2008 18:09	12/29/2014 18:09
Intermediate	DOD JITC CA-23	DoD JITC Root CA 2	1/16/2009 20:29	1/15/2015 20:29
Intermediate	DOD JITC CA-25	DoD JITC Root CA 2	12/24/2009 20:17	12/24/2015 20:17
Intermediate	DOD JITC CA-27	DoD JITC Root CA 2	3/16/2011 0:00	3/16/2017 0:00
Intermediate	DOD JITC CA-29	DoD JITC Root CA 2	2/14/2011 0:00	2/14/2017 0:00
Intermediate	DOD JITC CA-31	DoD JITC Root CA 2	10/30/2012 00:00	10/30/2018 00:00
Intermediate	DOD JITC EMAIL CA-21	DoD JITC Root CA 2	1/22/2009 15:48	1/21/2015 15:48
Intermediate	DOD JITC EMAIL CA-23	DoD JITC Root CA 2	1/21/2009 22:56	1/20/2015 22:56
Intermediate	DOD JITC EMAIL CA-25	DoD JITC Root CA 2	12/29/2009 19:44	12/29/2015 19:44
Intermediate	DOD JITC EMAIL CA-27	DoD JITC Root CA 2	2/18/2011 0:00	2/15/2017 0:00
Intermediate	DOD JITC EMAIL CA-29	DoD JITC Root CA 2	3/11/2011 0:00	3/11/2017 0:00
Intermediate	DOD JITC EMAIL CA-31	DoD JITC Root CA 2	10/30/2012 00:00	10/30/2018 00:00
Intermediate	DOD OM CA-22	DoD JITC Root CA 2	12/10/2008 15:21	12/9/2014 15:21
Intermediate	DOD OM CA-24	DoD JITC Root CA 2	12/10/2008 15:27	12/9/2014 15:27
Intermediate	DOD OM CA-26	DoD JITC Root CA 2	11/13/2009 10:49	11/13/2015 10:49
Intermediate	DOD OM CA-28	DoD JITC Root CA 2	10/18/2010 16:44	10/18/2016 16:44
Intermediate	DOD OM CA-30	DoD JITC Root CA 2	10/21/2010 0:00	10/21/2016 0:00
Intermediate	DOD OM CA-32	DoD JITC Root CA 2	11/15/2012 00:00	11/15/2018 00:00
Intermediate	DOD OM EMAIL CA-20	DoD JITC Root CA 2	8/2/2007 11:33	7/31/2013 11:32
Intermediate	DOD OM EMAIL CA-22	DoD JITC Root CA 2	12/10/2008 15:24	12/9/2014 15:24
Intermediate	DOD OM EMAIL CA-24	DoD JITC Root CA 2	12/10/2008 15:28	12/9/2014 15:28
Intermediate	DOD OM EMAIL	DoD JITC Root CA 2	11/5/2009 13:46	11/5/2015 13:46

	CA-26			
Intermediate	DOD OM EMAIL CA-28	DoD JITC Root CA 2	10/19/2010 18:02	10/19/2016 18:02
Intermediate	DOD OM EMAIL CA-30	DoD JITC Root CA 2	10/21/2010 0:00	10/21/2016 0:00
Intermediate	DOD OM EMAIL CA-32	DoD JITC Root CA 2	11/15/2012 00:00	11/15/2018 00:00
Intermediate	DoD JITC Intermediate CA-1	DoD JITC Root CA 2	2/12/2009 19:18	2/10/2019 19:18
Intermediate	DoD OM Intermediate CA-2	DoD JITC Root CA 2	2/12/2009 17:36	2/10/2019 17:36
Intermediate	DOD TEST SHA-256 CA-22	DoD JITC Root CA 2	9/28/2010 20:28	9/28/2016 20:28
Intermediate	DOD TEST SHA-256 CA-26	DoD JITC Root CA 2	9/27/2010 21:03	9/27/2016 21:03
Intermediate	DOD TEST SHA-256 EMAIL CA-22	DoD JITC Root CA 2	9/27/2010 21:03	9/27/2016 21:03
Intermediate	DOD TEST SHA-256 EMAIL CA-26	DoD JITC Root CA 2	9/27/2010 21:03	9/27/2016 21:03
Root	NSS JITC Root CA 1	NSS JITC Root CA 1	11/25/2009 16:19	11/20/2029 16:19
Intermediate	NSS DoD JITC Intermediate CA 1	NSS JITC Root CA 1	2/16/2010 0:00	11/20/2029 16:19
Intermediate	NSS DoD JITC Subordinate CA 1	NSS DoD JITC Intermediate CA 1	4/19/2010 0:00	4/16/2020 0:00
Intermediate	NSS DoD OM Subordinate CA 2	NSS DoD JITC Intermediate CA 1	4/26/2010 0:00	4/23/2020 0:00

Removed in 3.16

Target CA Store	Subject CN	Issuer CN	Not Before (GMT)	Not After (GMT)
Intermediate	DOD JITC CA-11	DoD JITC Root CA 2	12/13/2005 22:39	12/12/2011 22:39
Intermediate	DOD JITC CA-13	DoD JITC Root CA 2	1/26/2006 2:56	1/25/2012 2:56
Intermediate	DOD JITC CA-15	DoD JITC Root CA 2	6/28/2006 2:24	6/27/2012 2:24
Intermediate	DOD JITC CA-17	DoD JITC Root CA 2	6/28/2006 2:51	6/27/2012 2:51
Intermediate	DOD JITC CA-19	DoD JITC Root CA 2	11/27/2007 21:07	11/27/2013 21:07
Intermediate	DOD JITC EMAIL CA-11	DoD JITC Root CA 2	12/14/2005 2:34	12/13/2011 2:34
Intermediate	DOD JITC EMAIL CA-13	DoD JITC Root CA 2	1/26/2006 3:28	1/25/2012 3:28
Intermediate	DOD JITC EMAIL CA-15	DoD JITC Root CA 2	6/28/2006 2:37	6/27/2012 2:37
Intermediate	DOD JITC EMAIL CA-17	DoD JITC Root CA 2	6/28/2006 3:06	6/27/2012 3:06
Intermediate	DOD JITC EMAIL CA-19	DoD JITC Root CA 2	11/27/2007 21:11	11/26/2013 21:11
Intermediate	DOD OM CA-14	DoD JITC Root CA 2	3/11/2006 5:50	3/10/2012 5:50
Intermediate	DOD OM CA-16	DoD JITC Root CA 2	7/13/2006 18:22	7/12/2012 18:22
Intermediate	DOD OM CA-18	DoD JITC Root CA 2	6/28/2006 20:00	6/27/2012 20:00
Intermediate	DOD OM CA-20	DoD JITC Root CA 2	8/3/2007 16:27	8/1/2013 16:26

Intermediate	DOD OM EMAIL CA-14	DoD JITC Root CA 2	3/11/2006 5:45	3/10/2012 5:45
Intermediate	DOD OM EMAIL CA-16	DoD JITC Root CA 2	6/28/2006 22:00	6/27/2012 22:00
Intermediate	DOD OM EMAIL CA-18	DoD JITC Root CA 2	6/28/2006 19:55	6/27/2012 19:55

External Certification Authority Certificates

Applicable InstallRoot Versions: InstallRoot 3.16.4 GUI, InstallRoot-3.16.4E

Target CA Store	Subject CN	Issuer CN	Not Before (GMT)	Not After (GMT)
Root	ECA Root CA 2	ECA Root CA 2	4/4/2008 14:24	3/30/2028 14:24
Intermediate	IdenTrust ECA 3	ECA Root CA 2	3/30/2011 13:39	3/28/2017 13:39
Intermediate	IdenTrust ECA 4	ECA Root CA 2	1/16/2014 14:35	1/16/2020 14:35
Intermediate	ORC ECA HW 3	ECA Root CA 2	6/11/2008 13:43	6/10/2014 13:43
Intermediate	ORC ECA HW 4	ECA Root CA 2	6/1/2011 13:41	5/30/2017 13:41
Intermediate	ORC ECA SW 3	ECA Root CA 2	5/7/2008 15:43	5/6/2014 15:43
Intermediate	ORC ECA SW 4	ECA Root CA 2	6/1/2011 13:43	5/30/2017 13:43
Intermediate	VeriSign Client External Certification Authority – G2	ECA Root CA 2	7/2/2008 14:41	7/1/2014 14:41
Intermediate	VeriSign Client External Certification Authority - G3	ECA Root CA 2	7/6/2011 14:05	7/4/2017 14:05
Intermediate	Symantec Client External Certification Authority	ECA Root CA 2	3/20/2014 14:24	3/19/2020 08:24
Intermediate	ORC ECA HW 5	ECA Root CA 2	5/19/2014 06:45	5/18/2020 06:45
Intermediate	ORC ECA SW 5	ECA Root CA 2	5/19/2014 06:33	5/18/2020 06:33