PKE

Public Key Enablement

Contract DCA200-00-D-5018

InstallRoot System Administrator Guide (SAG)

November 8, 2001

Document Control Number: 2246002-InstallRootSAG-6.4.1-01Nov08-V2.0

Prepared for:

DISA/D24
Ms. Betsy Appleby
5111 Leesburg Pike, 9th Floor
Falls Church, Virginia 22041

Prepared by:

Systems Research and Applications Corporation
a wholly owned subsidiary of SRA International, Inc.
Suite 200
5203 Leesburg Pike
Falls Church, VA 22041

TABLE OF CONTENTS

OVERVIEW

InstallRoot is a small utility use to manage DoD supported root certificates on computers. InstallRoot can be run locally, from a floppy disk, across a network, or even as a logon script.

The root certificates are important because they enable a user's system to trust, or have confidence in, any certificates issued by any of the certificate servers under each root. If a user does not have the root certificates installed and they receive a secured message from another user, they will receive an error message saying that the user is not trusted. For more information on e-mail and root certificates, refer to the Medium Grade Services (MGS) website at http://falcon3.ncr.disa.mil/html/introduction.html.

1. SYSTEM REQUIREMENTS

1.1 CLIENT REQUIREMENTS

- Windows 95, 98, ME, NT, or 2000 (Administrator or User privileges).
- Internet Explorer with 128-bit Encryption

2. RUNNING INSTALLROOT

2.1 RUNNING FROM A FLOPPY

- Insert the floppy into the floppy drive of your computer.
- Click on the Start button and click Run.
- Type "A:\InstallRoot.exe" where "A" is the letter of your floppy drive.
- Follow the on-screen prompts to complete the installation.

2.2 RUNNING OVER A NETWORK

- Using Network Neighborhood, locate the computer where the InstallRoot.exe file resides.
- Double-click on the InstallRoot.exe file and follow the on-screen prompts to complete the installation.

2.3 COMMAND LINE SWITCHES

InstallRoot accepts several command-line switches that allow the user to display, insert, and remove DoD supported root certificates. Command-line switches are also available for displaying helpful information about InstallRoot as well as creating files containing DoD supported root certificates.

InstallRoot
InstallRoot -c *filename* [**-s**
InstallRoot -d [**-f**] [**-s**
InstallRoot -h
InstallRoot -i*filename* [**-s**]
InstallRoot -l[[*filename*][,[store*name*]]]

Switch	Operation	Description
-c*filename*	Create File	Create a certificate file that contains DoD supported root certificates stored in the computer's system registries.
-d	Delete Certificates	Remove DoD supported root certificates from the computer's system store.
-f	Force Deletion	Used with the delete (-d) switch to force the deletion of certificates without confirmation by the user.
-h	Help	Displays help information.
-i*filename*	Insert Certificates	Installs DoD supported root certificates contained in a certificate file into the computer's system registries.
-l[[*filename*][,[*storename*]]]	Display Certificates	Display DoD supported root certificate information. If the file and computer system registry store names are not specified, then the certificates embedded in the program are displayed.
-s	Silent Mode	Do not display any messages. This switch is best used when automating InstallRoot to run on multiple computers at once or in a workstation's logon script

2.4 EXAMPLES

2.4.1 Display certificate information

List the certificates embedded in the InstallRoot application.

> InstallRoot -l

List the certificates stored in a file store named mystore.sto.

> InstallRoot -lmystore.sto

List the certificates stored in a Root system store.

> InstallRoot –l,root

List the certificates stored in the default certificate stores.

> InstallRoot –l,

List the certificates stored in a file store named newstore.sto and the CA system store.

> InstallRoot –lnewstore.sto,CA

2.4.2 Deleting certificates

Delete the certificates from the default certificate stores. The user will be required to confirm the deletion of each certificate.

> InstallRoot -d

Force the deletion of certificates from the default certificate stores without user confirmation.

> InstallRoot –d -f

2.4.3 Inserting certificates

Insert certificates embedded in the InstallRoot application into the default certificate stores.

> InstallRoot

Insert certificates contained in a file store named “newcerts.sto” into the default certificate stores.

> InstallRoot –inewcerts.sto

2.4.4 Creating a file store

Insert certificates embedded in the InstallRoot application into a file store named “savecerts.sto”.

> InstallRoot -csavecerts.sto

2.4.5 Invoking help

Show the InstallRoot application help information.

> InstallRoot -h

2.4.6 Using the silent mode option

The silent mode switch, -s, could be used with the create (-c), delete (-d), and insert (-i) switches to prevent the application from displaying the results of its operation.

3. INSTALLED ROOTS

3.1 WINDOWS NT USER PRIVILEGES

When a user with Administrative privileges runs InstallRoot, the program will install the root certificates into the Local Machine branch of the system registry. This makes the root certificates visible to and usable by all accounts on that computer. However, if the user running InstallRoot does not have Administrative privileges, the root certificates will be installed under the Current User branch of the system registry, making them available to that user only.

3.2 TRUSTED ROOTS

- DoD CLASS 3 Root CA
- DoD PKI Med Root CA
- DST IECA-2
- General Dynamics IECA Root CA
- Onsite2-188 (VeriSign IECA)
- ORC IECA.

3.3 INTERMEDIATE ROOTS

- DOD CLASS 3 CA-3
- DOD CLASS 3 CA-4
- DOD CLASS 3 CAC CA
- DOD CLASS 3 CAC EMAIL CA
- DOD CLASS 3 EMAIL CA-3
- DOD CLASS 3 EMAIL CA-4
- Med CA-1
- Med CA-2
- Med Email CA-1
- Med Email CA-2.

4. KNOWN ISSUES

4.1 RUNNING INSTALLROOT AS A LOGON SCRIPT UNDER WINDOWS 9X

a. Error: “Bad command or file name.”

   Explanation: This issue arises if you do not specify the full Universal Naming Convention (UNC) path for the filename when the silent switch (-s) is specified (an example of a UNC pathname is \\SRA\NETLOGON for the NETLOGON folder on the SRA computer). Unfortunately, the server does not allow UNC pathnames in the logon

script setup. We recommend creating a batch file that executes InstallRoot with the UNC pathname, and subsequently setting that batch file to run in the logon script.

b. Program crash:

Explanation: This issue arises if you run without the silent switch in a logon script under Windows 9X. We recommend using the silent switch in all logon scripts.

Note: Running any program as a logon script forces that program to be executed each time a user logs in to the computer. InstallRoot has been tested in this environment and is safe to run in a logon script.

4.2 RUNNING INSTALLROOT AS A LOGON SCRIPT UNDER WINDOWS 9X, ME

Problem: InstallRoot logon script gets run when user logs on but certificates are not visible on the Certificate Manager window.

Explanation: This problem occurs when client machine has user profile set up for that logon user and the Primary Network Logon is anything except "Microsoft Family Logon". Solution to this problem is as follows:

1. On the client machine, log off from the domain.
2. The "Enter Network Password" window appears.
3. Click the "Cancel" button so you will not log on to the domain
4. Access the "Users" window from the "Control Panel" window. To get to the "Control Panel" window, click on "Start", "Settings", and then "Control Panel".
5. On the "Users" window, remove the user profile of the user who needs to run the InstallRoot logon script.
6. Log off.
7. On the "Enter Network Password" window, enter logon information and click "OK" button.
8. Verify that InstallRoot logon script is run and that the certificates are visible on the "Certificate Manager" window.

4.3 RUNNING UNDER WINDOWS WITHOUT ADMINISTRATIVE RIGHTS

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

.

5. TECHNICAL SUPPORT

- Daniel S. Falcone, Programmer, dan_falcone@sra.com, 703-824-5313
- Ronald Spitz, Engineer, ronald_spitz@sra.com, 703-824-5315
- Doug Colligan, Engineer, doug_colligan@sra.com, 703-824-5382
- Kevin Heald, Engineer, kevin_heald@sra.com, 703-824-5365
- Tyron Meadows, Programmer, tyron_meadows@sra.com, 703-824-5337