IA Software Installation Guide

Revision P
Version 0
January 2024
Document DOC-IA-NA-IG-P-0

Advanced Simulation Technology inc.
500A Huntmar Park Drive ▪ Herndon, Virginia 20170 USA
(703) 471-2104 ▪ asti-usa.com

Product Name: IA Software Package

IA Software Installation Guide

ASTi
500A Huntmar Park Drive
Herndon, Virginia 20170 USA

Red Hat Enterprise Linux (RHEL) Subscriptions

ASTi is an official Red Hat Embedded Partner. ASTi-provided products based on RHEL include Red Hat software integrated with ASTi's installation. ASTi includes a Red Hat subscription with every purchase of our Software and Information Assurance (SW/IA) maintenance products. Systems with active maintenance receive Red Hat software updates and support directly from ASTi.

Export Restriction

Countries other than the United States may restrict the import, use, or export of software that contains encryption technology. By installing this software, you agree that you shall be solely responsible for compliance with any such import, use, or export restrictions. For full details on Red Hat export restrictions, go to the following:

www.redhat.com/en/about/export-control-product-matrix

Revision history

Date	Revision	Version	Comments
2/12/2017	L	0	Edited content for grammar, style, and accuracy. Converted content into XML format.
8/1/2018	M	0	Changed Red Hat Network (RHN) references to Red Hat Subscription Management (RHSM). Fixed minor formatting errors throughout document. Added "Risk Management Framework (RMF) setup."
10/16/2018	M	1	Updated RHSM screenshots; updated IA installation procedure for Red Hat 7, and updated DVD label names.
11/2/2018	M	2	Fixed typo in "Password policy compliance."
12/6/2018	M	3	Streamlined mount command for Red Hat 6 and 7.
2/28/2019	M	4	Added USB License Key installation step to "Apply Red Hat Subscription Management updates."
4/30/2019	N	0	Moved USB License Key step to "Install ASTi Information Assurance software" and added mount command for Studio in Red Hat 6 and 7. Made other minor edits for clarity. In "Apply Red Hat Subscription Management updates," changed wording of Step 4, which describes how to log into the astiadmin user account as root; moved Steps 12–14 to a new section titled, "Execute the ASTi security script."
5/5/2020	O	0	Split "Password policy compliance" into two sections. Changed workflow so that users first log in as root .Instructed users to complete the IA Installation Procedure before changing passwords.
8/19/2021	O	1	Changed command in "View a password's age." Updated the title page and table styles.
7/8/2022	O	2	Made minor changes to "Execute the ASTi security script," "Install ASTi Information Assurance software," and "Apply Red Hat Subscription Management updates."
9/27/2022	O	3	Removed "license" references from the Red Hat Enterprise Linux export statement in the front matter.

Date	Revision	Version	Comments
11/28/2022	O	4	Combined content from the *IA Installation Overview* by adding "IA cold-start procedure." Further clarified instructions to mount and install IA and RHSM software on Studio in "Install ASTi Information Assurance software" and "Apply Red Hat Subscription Management updates." Removed all Red Hat 6.X references.
3/8/2023	O	5	Updated cross references to the *Voisus Cold Start Guide* in "IA cold-start procedure." Updated the Red Hat Enterprise Linux subscription and export statement in the front matter.
1/22/2024	P	0	Removed "Set up Risk Management Framework (RMF)." Updated deprecated "Target," "Remote Management System," and "ACE" terminology. Fixed broken links. Removed outdated screenshots and made minor grammar edits.

Contents

1.0 Introduction

Information Assurance (IA) software installation requires the Security Patches & Updates for Information Assurance DVD. For a comprehensive list of DVD deliverables required for the *IA Software Installation Guide*, go to the following document:

Security Patches & Updates for Information Assurance DVD/docs/ IA_Package_Overview_*xxxx*.pdf

The *IA Software Installation Guide* applies to the following ASTi systems:

- Voisus servers
- Telestra servers
- Studio development workstations
- Studio virtual machines

For Telestra and Voisus customers: before beginning, install the ASTi USB License Key with the IA license on the Telestra server or Voisus server.

For TL-SW-IA-M customers: ASTi does not provide Red Hat Subscription Management (RHSM) patches. It is your responsibility to obtain RHSM patches and maintain a valid RHSM account.

For active IA Maintenance customers: ASTi provides RHSM patches on the RHSM7 Security Patches & Updates DVD or RHSM8 Security Patches & Updates DVD.

2.0 IA cold-start procedure

On the Security Patches & Updates for Information Assurance DVD, go to the following document section for a comprehensive list of DVD requirements: **Docs folder/ IA_Package_Overview_*XXXX*.doc/ DVD Deliverables**

Before installing Information Assurance (IA) on an ASTi system, follow these steps:

1. If you're using a Studio virtual machine (VM), follow the instructions in the *Studio VM Quick Start Guide* to install and configure VMware Workstation Player.
2. Back up your system to avoid losing data during the cold-start procedure, which completely erases your system's hard drive.
   - *Voisus server:* go to "System backups" in the *Voisus Cold Start Guide*.
   - *Telestra server:* go to "Backup" in the *Telestra Cold Start Guide*.
   - *Studio development workstation or VM:* save any important files (e.g., previous backups, text files) to external media.
3. Follow the applicable cold-start procedure to install ASTi software on your system:
   - *Voisus server:* go to "Cold-start procedure for IA Software Package 7.X or 8.X" in the *Voisus Cold Start Guide*.
   - *Telestra server:* go to "Telestra server cold-start procedure for Telestra 7.X and 8.X" in the *Telestra Cold Start Guide*.
   - *Studio development workstation or VM:* go to "Studio cold-start procedure for IA Software Package 7.X and 8.X" in the *Telestra Cold Start Guide*.
4. Restore the backup you created in Step 1.
   - *Voisus server:* go to "System restoration" in the *Voisus Cold Start Guide*.
   - *Telestra server, Studio development workstation, and Studio VM:* go to "Restore" in the *Telestra Cold Start Guide*.
5. Proceed to Section 3.0, "Information Assurance software installation procedure" on the facing page.

3.0 Information Assurance software installation procedure

This chapter describes how to:

- Install ASTi Information Assurance software
- Apply Red Hat Subscription Management updates
- Execute the ASTi security script

3.1 Install ASTi Information Assurance software

To install ASTi Information Assurance (IA) software, follow these steps:

1. Ensure an ASTi USB License Key is inserted into the system's USB drive. To learn about USB License Keys, go to "Licenses" in the *Voisus Quick Start Guide* or *Telestra Web Interface User Guide*.
2. Insert the Security Patches & Updates for Information Assurance DVD into the DVD drive.
3. To mount and install IA software on a Telestra server or Voisus server, do the following:
   a. Log into the system using the following default credentials:

Username	Password
root	abcd1234

   b. To mount the DVD, run **mount /dev/cdrom /media**.
   c. Run **sh /media/install**, and wait several minutes for installation to complete.

   To mount and install IA software on a Studio, do the following:

   a. Log into Studio using the following default credentials:

Username	Password
aceuser	aceuser

   b. From the desktop, right-click and select **Open Terminal**, or go to **Applications** > **System Tools** > **Terminal**.

c. To switch to the root user account, run **su**, and enter the root password (i.e., **abcd1234** by default).

d. Studio mounts the DVD automatically. Run **sh /run/media/aceuser/***DVD***/install**, where *DVD* represents the DVD name (e.g., ASTi_IA_DVD_*YYYYQN*, where *YYYY* is the year and *N* is the quarterly release number). Wait several minutes for installation to complete.

4. To eject the DVD, run **eject**. Remove the DVD from the drive.

***Note**: On Studio VM, right-click and select **eject**.*

5. Run **reboot**.

3.2 Apply Red Hat Subscription Management updates

***Important**: ASTi does not provide Red Hat Subscription Management (RHSM) patches for TL-SW-IA-M customers. For site-specific RHSM installation instructions and patch sets, go to your IT administrator. After installing RHSM patches, skip to Section 3.3, "Execute the ASTi security script" on the facing page.*

To apply RHSM updates, follow these steps:

1. Insert the RHSM7 Security Patches & Updates DVD or RHSM8 Security Patches & Updates DVD into the DVD drive.

2. To mount and install RHSM updates on a Telestra server or Voisus server, do the following:

   a. From the terminal prompt, log into the system using one of the following credentials:

   Voisus server:

Username	Password
astiadmin	admin

   Telestra server:

Username	Password
admin	admin

   b. To switch to the root user account, run **su**, and enter the root password (i.e., **abcd1234** by default).

c. To mount the DVD, run **mount /dev/cdrom /media**.

d. At the prompt, run **sh /media/install**.

To mount and install RHSM updates on a Studio, do the following:

a. Log into Studio using the following default credentials:

Username	Password
aceuser	aceuser

b. From the desktop, right-click and select **Open Terminal**, or go to **Applications** > **System Tools** > **Terminal**.

c. To switch to the root user account, run **su**, and enter the root password (i.e., **abcd1234** by default).

d. Studio mounts the DVD automatically. Run **sh /run/media/aceuser/***DVD***/install**, where *DVD* represents the DVD name (i.e., RHSM-8-X64).

3. On **Product Install**, press Tab to select **Ok**, and then press Enter.
4. On **Install RHSM-*N*-X64**, select **Yes**, and press Enter.

***Note**: The DVD name depicted above may vary depending on the quarterly release version.*

5. Wait several minutes for installation to complete, and run **eject**.
6. Remove the DVD from the drive.

3.3 Execute the ASTi security script

To execute the security script, follow these steps:

1. At the prompt, run **secure_telestra.sh**.
2. To verify that the system is set according to the current manifest, run **ace-package-report -C**.

```
[root@telestra-57-98-1D ~]# ace-package-report -C
Loading manifest from ace-target-2011Q4.txt:
Manifest Checksum:      PASS
Package Manifest:       PASS
[root@telestra-57-98-1D ~]# _
```

Figure 1: Telestra package report

3. To finalize changes, run **reboot**.

Appendix A: ASTi software package manifest

The **ace-package-report** command generates the system software package manifest. See the specific syntax shown below:

ace-package-report -h

usage: ace-package-report *options*

where *options* is one of the command options in Table 1, "Command options" below.

Command Options	Details	Description
-h	--help	Show this help message and exit
-a	-asti	List ASTi packages
-b	--baseos	List Base OS packages
-c	--commercial	List Commercial packages
-C	--checksum	Check current system against previously installed manifest file
- C MANIFEST *(Optional)*	--checksum = MANIFEST	Check current system against MANIFEST
-f OUTPUT	--outfile=OUTPUT	Output Filename
-m	--manifest	Generate Package Manifest
-n	--names	List names of installed packages
-o	--opensource	List Open Source packages
-u	--unknown	List unknown vendor packages
-v	--verbose	Enable debug output
-d VENDOR DATA	--vendordata =VENDORDATA	Vendor data file

Table 1: Command options

To verify that the system you are installing matches the manifest that ASTi or another IA entity provided, run **ace-package-report -C**. If the system matches the manifest exactly, you will see the following:

```
Manifest Checksum: PASS
Package Manifest: PASS
```

When the system does not match the manifest exactly, the output varies based on the differences between the manifest and the system you are verifying. For example, if the system you are checking has a newer version of Network File System (NFS), you might see the following:

```
# ace-package-report -C
Manifest Checksum: PASS
Package Manifest: FAIL
Package Details:
NEW: nfs-utils-1.0.9-40.el5(nfs-utils-1.0.8-40.el5)
```

However, if the manifest file itself was corrupted, the following might display:

```
# ace-package-report -C
Manifest Checksum: PASS
Package Manifest: FAIL
Package Details:
NEW: nfs-utils-1.0.9-40.el5(nfs-utils-1.0.8-40.el5)
```

Various other findings such as new, old, removed and added packages also display, as applicable.

Appendix B: Password policy compliance

After completing Section 3.0, "Information Assurance software installation procedure" on page 3, you will need to update your ASTi system's default password, which does not comply with stringent password rules required by government security regulations. Passwords expire every 60 days on a hardened system, forcing you to enter a new password during your next login via an automated dialog. This process enforces the stringent rules for the new password.

This chapter discusses how to:

- View a password's age
- Update a password before expiration

B-1 View a password's age

To view the current password age information, follow these steps:

1. Log into the server using the following credentials:

Username	Password
astiadmin	admin

2. At the prompt, run **chage -i astiadmin**. The current password age information displays.

B-2 Update a password before expiration

To change the default password before the 60 days has passed, follow these steps:

1. Log into the server using the following credentials:

Username	Password
astiadmin	admin

2. To switch to the root user account, do the following:
   a. Enter **su**, and press Enter.
   b. Enter the root password (i.e., **abcd1234** by default), and press Enter.
3. At the prompt, run **chage -d 0 astiadmin**.
4. Run **chage -d 0 root**.
5. To log out of root, run **exit**. Repeat this step to log out of **astiadmin** as well.

6. When you log back in, the system prompts you for a new password. Enter a password for the **astiadmin** account, and press Enter.
7. At the prompt, elevate to root again:

Username	Password
su	abcd1234

8. At the prompt, enter a new password for the root user. Your system passwords are now compliant.

Appendix C: IA update installation

In addition to quarterly IA updates, some sites may also receive periodic updates. These electronic updates can be applied to an existing system and do not require a cold start. Before installing patches, ASTi recommends that you back up your system.

ASTi only provides an IA .ISO update if an information assurance vulnerability alert (IAVA) affects an ASTi system. In this context, critical IAVAs are those defined and published by the Defense Information System Agency (DISA).

ASTi delivers these patch sets electronically via secure download to a single point of contact for each IA Maintenance contract. You are responsible for generating a DVD from the .iso file provided.

To install an IA update, follow these steps:

1. Create a DVD from the .ISO file that ASTi delivered electronically.

   

   ***Note**: An .ISO file, also called an image, is a single file that is a copy of an entire data CD or DVD. When you burn a CD or DVD from an .ISO file, the new hard drive has the same folders, files, and properties as the original.*

2. Open a terminal window.
3. Log into your system using one of the following credentials:

   Voisus server:

Username	Password
astiadmin	admin

   Telestra server:

Username	Password
admin	admin

4. Insert the DVD that you created in Step 1.
5. To mount the DVD, run **mount /dev/cdrom /media**.
6. Run **sh /media/install**.
7. Select **Ok**, and press Enter.

8. Select **Yes**, and press Enter.

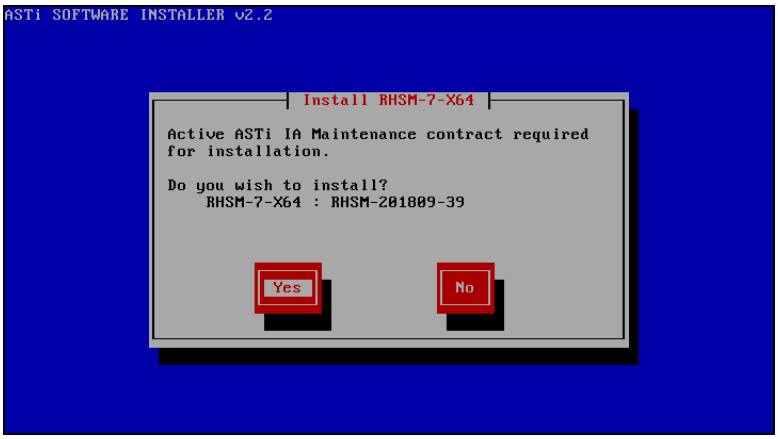

Figure 2: Install the RHSM DVD

9. After the installation is complete, run **eject**.
10. Run **secure_telestra.sh**.
11. To reboot the system, run **reboot**.

