



Advanced Simulation Technology inc.
500A Huntmar Park Drive
Herndon, Virginia 20170 USA
Tel. (703) 471-2104 • Fax. (703) 471-2108
asti-usa.com

IA Software Installation Guide

Document: DOC-IA-NA-IG-O-0

IA Software Installation Guide

© Copyright ASTi 2020

Restricted Rights: Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7015.

This material may be reproduced by or for the U.S. Government pursuant to the copyright license under the clause at DFARS 252.227-7015 (1994).

ASTi

500A Huntmar Park Drive

Herndon, Virginia 20170 USA

Red Hat® Enterprise Linux

Red Hat® Subscription

ASTi's software is designed to run on an installation of Red Hat® Enterprise Linux® client. This ensures optimal interoperability with ASTi's software, host routing software and external communications servers. As such included in the cold start DVDs is the complete installation of Red Hat® Enterprise Linux® client. This software is not activated to a current Red Hat subscription. It is the end users' responsibility to activate their subscription and connect to the Red Hat Network. The Red Hat subscription will provide the end user with support, maintenance, software and security updates. For details on Red Hat activation, go to the Red Hat web site:

www.redhat.com/apps/activate

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/licenses/export

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 "Set up Risk Management Framework (RMF)."
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 RHSM updates."
4/30/2019	N	0	Moved USB License Key step to "Install ASTi IA software" and added mount command for ACE Studio in Red Hat 6 and 7. Made other minor edits for clarity. In "Apply RHSM 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.

Contents

1.0 Introduction	1
2.0 IA software installation procedure	2
2.1 Install ASTi IA software	2
2.2 Apply RHSM updates	3
2.3 Execute the ASTi security script	5
2.4 Set up Risk Management Framework (RMF)	5
Appendix A: ASTi software package manifest	6
Appendix B: Password policy compliance	8
B-1 View a password's age	8
B-2 Update a password before expiration	8
Appendix C: IA update installation	10

1.0 Introduction

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

ASTi IA DVD/docs/ IA_Package_Overview_XXXX.pdf

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

- Voisus servers
- Telestra servers running ACE Target and ACE Studio
- Virtual machines (VMs) running ACE Studio

For Telestra and Voisus customers: before beginning, install the ASTi USB License Key or license file with ACE Security (ACE-SEC) software on the Telestra Target or Voisus server.

For SEC-TEL-0X 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 RHSM6 Security Patches & Updates DVD or RHSM7 Security Patches & Updates DVD.

2.0 IA software installation procedure

This chapter describes how to do the following:

1. Install ASTi IA software.
2. Apply Red Hat Subscription Management (RHSM) updates.
3. Execute the ASTi security script.

2.1 Install ASTi IA software

To install ASTi IA software, follow these steps:

1. Ensure an ASTi USB License Key is installed on the server. To learn about USB License Keys, go to "Licenses" in the *Voisus Quick Start Guide*.
2. Log into the system using the following default credentials:

Username	Password
root	abcd1234

3. Insert the ASTi IA DVD into the DVD drive.
4. To mount the DVD on a Target, enter **mount /dev/cdrom /media**, and press Enter. The DVD automatically mounts to a Studio; if you're using a Studio, skip to the next step.
5. Depending on your platform and operating system, enter one of the following:
 - *Target*: **sh /media/install**
 - *Studio Red Hat 7*: **sh /run/media/aceuser/DVD/install**, where *DVD* represents the DVD name
 - *Studio Red Hat 6*: **sh /media/DVD/install**

Press Enter, and wait several minutes for installation to complete.

6. To eject the DVD, enter **eject**, and press Enter. Remove the DVD from the drive.
7. Enter **reboot**, and press Enter.



Note: After reboot, you can no longer log into the system as a root user.

2.2 Apply RHSM updates



Important: ASTi does not provide Red Hat Subscription Management (RHSM) patches for SEC-TEL-0X customers. For site-specific RHSM installation instructions and patch sets, go to your IT administrator. After installing RHSM patches, skip to Section 2.3, "Execute the ASTi security script" on page 5.

To apply RHSM updates, follow these steps:

1. Open a terminal window.
2. Log into the system using one of the following:

Voisus server:

Username	Password
astiaadmin	admin

Telestra server running ACE Target:

Username	Password
admin	admin

Telestra server or virtual machine running ACE Studio:

Username	Password
aceuser	aceuser



Note: If your organization changed these default credentials, check with your IT administrator for an updated username and password.

3. 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.
4. Insert the RHSM6 Security Patches & Updates DVD or RHSM7 Security Patches & Updates DVD into the drive.
5. To mount the DVD on a Target, enter **mount /dev/cdrom /media**, and press Enter. The DVD automatically mounts to a Studio; if you're using a Studio, skip to the next step.

6. Depending on your platform and operating system, enter one of the following:
 - *Target*: **sh /media/install**
 - *Studio Red Hat 7*: **sh /run/media/aceuser/DVD/install**, where *DVD* represents the DVD name (e.g., RHSM-7-X64)
 - *Studio Red Hat 6*: **sh /media/DVD/install**

Press Enter.

7. On **ACE Product Install**, press Tab to select **Ok**, and then press Enter.



Figure 1: ACE Product Install

8. On **Install ACE-RHSM**, select **Yes**, and press Enter.

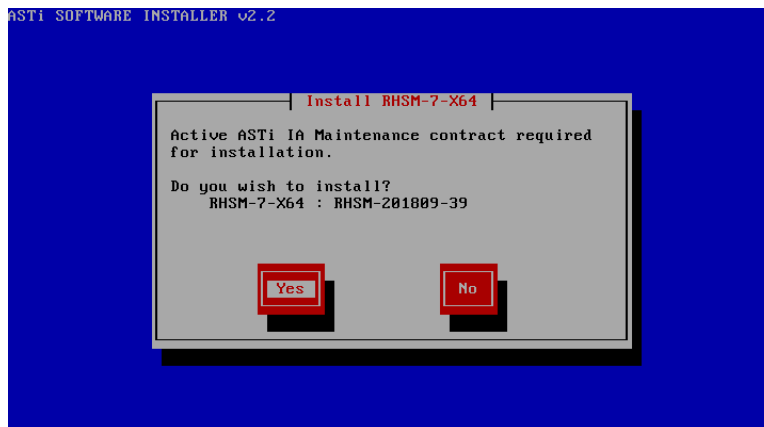


Figure 2: Install ACE-RHSM

9. Wait several minutes for installation to complete. Enter **eject**, and press Enter.
10. Remove the DVD from the drive.

2.3 Execute the ASTi security script

To execute the security script, follow these steps:

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

```
[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 3: ACE package report

3. To reboot the server, enter **reboot**, and press Enter.

2.4 Set up Risk Management Framework (RMF)

If your server requires RMF for Authority to Operate (ATO) compliance, go to the associated ATO's System Security Plan (SSP) and RMF package. For anti-virus, Advanced Intrusion Detection Environment (AIDE), remote logging, and **firewalld** setup instructions, go to *ASTi IA Post Installation RMF Setup Procedures*. This document is located in the **/docs/ato** folder on the quarterly ASTi IA DVD.

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, enter **ace-package-report -C**, and press Enter. 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.e15(nfs-utils-1.0.8-40.e15)
```

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.e15(nfs-utils-1.0.8-40.e15)
```

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

Appendix B: Password policy compliance

After completing Section 2.0, "IA software installation procedure" on page 2, 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
astiaadmin	admin



Note: If your organization changed these default credentials, check with your IT administrator for an updated username and password.

2. At the prompt, enter **chage -1 astiaadmin**, and press Enter. 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
astiaadmin	admin



Note: If your organization changed these default credentials, check with your IT administrator for an updated username and password.

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, enter **chage -d 0 astiadmin**, and press Enter.
4. Enter **chage -d 0 root**, and press Enter.
5. To log out of root, enter **exit**, and press Enter. Repeat this step to log out of **astiadmin** as well.
6. When you log back in, the system will prompt 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 a disk 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 disk has the same folders, files, and properties as the original disk.

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

Voisus server:

Username	Password
astiaadmin	admin

Telestra server running ACE Target:

Username	Password
admin	admin

Telestra server or virtual machine running ACE Studio:

Username	Password
aceuser	aceuser



Note: If your organization changed these default credentials, check with your IT administrator for an updated username and password.

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



Figure 4: ACE Product Install

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

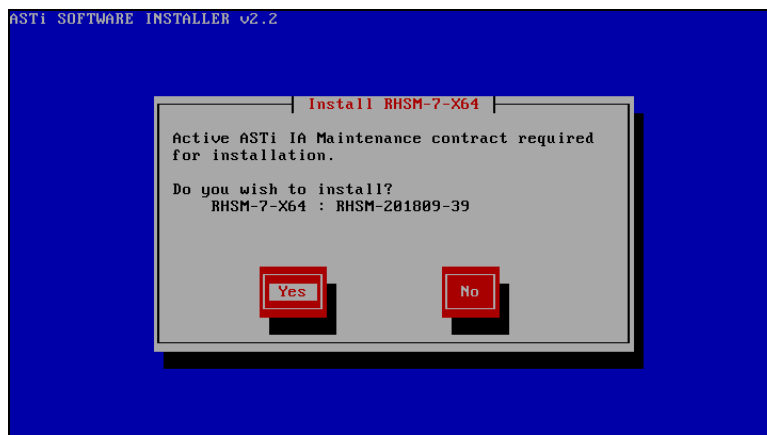


Figure 5: Install ACE-RHSM

10. After the installation is complete, enter **eject**, and press Enter.
11. Enter **secure_telestra.sh**, and press Enter.
12. To reboot the system, enter **reboot**, and press Enter.