

Getting Started with ArcSight™ ESM Appliance

ESM v4.5 SP1

August 28, 2009



Getting Started with ArcSight™ ESM Appliance

August 28, 2009

Copyright © 2009 ArcSight, Inc. All rights reserved. ArcSight, the ArcSight logo, ArcSight TRM, ArcSight NCM, ArcSight Enterprise Security Alliance, ArcSight Enterprise Security Alliance logo, ArcSight Interactive Discovery, ArcSight Pattern Discovery, ArcSight Logger, FlexConnector, SmartConnector, SmartStorage and CounterACT are trademarks of ArcSight, Inc. All other brands, products and company names used herein may be trademarks of their respective owners.

Follow this link to see a complete statement of ArcSight's copyrights, trademarks, and acknowledgements:

<http://www.arcsight.com/copyrightnotice>.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

This document is ArcSight Confidential.

Contents

- Getting Started with ArcSight™ ESM Appliance 1**
 - Installation Instructions 1
 - Installing ArcSight ESM 1
 - Preparing for Oracle Database Installation 2
 - Oracle Installation 2
- Restoring Factory Settings 3**
- Customer Support 11**

Getting Started with ArcSight™ ESM Appliance

Use this document and the *Rack Installation Guide*, included in the ArcSight ESM Appliance, to install your appliance and connect to it the first time.

The *ArcSight ESM Administrator's Guide* explains in detail how to deploy, configure and use ArcSight ESM. The guide is available:

- From the ESM Console Browse Docs page
- As a download from <https://support.arcsight.com>
- On the Server in the `/opt/arcsight/docs` directory

Installation Instructions

1. Follow the instructions in the *Rack Installation Guide* for unpacking the appliance and its accompanying accessories.
2. Securely mount the appliance in a rack and make the rear panel connections.
3. Attach a monitor, keyboard and mouse to the system.
4. Power on the system, and wait for the system to boot.

CAUTION

Read through the instructions, cautions, and warnings in the *Rack Installation Guide* carefully. Failing to do so can result in bodily injury or system malfunction.

The ArcSight ESM Appliance comes with the Oracle Enterprise Linux operating system already installed. When setting preferences for Oracle Enterprise Linux, consider the following:

- When you accept the License agreement, note that the license agreement is for Oracle Linux only. ArcSight ESM has a separate license agreement that appears when ArcSight ESM component is installed.
- If you choose to enable the firewall, you will need to open ports 8443 and 9443 for ArcSight Manager and ArcSight Web communication. You might also want to open port 22 for remote SSH access.

For more information on Oracle Enterprise Linux, see <http://www.oracle.com/linux/>.

Installing ArcSight ESM

The installation files for ArcSight ESM components are available in the `/opt/arcsight/installers` directory. Navigate to this directory and install the ESM components according to the instructions found in the *ArcSight ESM Installation and Configuration Guide*.



After installing the ArcSight Manager, download the Console installer file from the ArcSight Customer Support website and install the Console on one or more systems.



Note that the 'arcsight' user is pre-defined in the system. You do not need to create this user.

Preparing to Install the Oracle Database

Before you install the ArcSight Database, please note the following recommendations:

- There are 6 physical disks set up in a RAID 10 group that appear as a single logical disk to the Operating System. This is partitioned so that there is approximately 1 TB on `/opt/data` and 100 GB on `/`. ArcSight recommends:
 - a. Installing the ArcSight Database in the `/usr/local/arcsight/db45sp1` directory
 - b. Setting the Oracle user home and installation directory as `/home/oracle` and Oracle Home as `/home/oracle/OraHome10g`.
 - c. Storing Redo Logs and default Oracle data files (System, SysAux, etc.) under default `/home/oracle/OraHome10g/oradata/arcsight`.
 - d. Storing data files for all arcsight tablespaces (ARC_*) in `/opt/data`.
- Estimate your retention needs and whether you want to enable partition archiving or not. Contact ArcSight Support if you need help with enablement. You can completely fill the `/opt/data` directory with data files.
- Review the "Preparing a Linux System" section, steps 5-7 in the *ArcSight ESM Installation and Configuration Guide* for details on how to configure and verify that the hostname is properly set and can be pinged. The Oracle installation will fail if your host system cannot be pinged.
- When the Oracle database installation is complete, install the ArcSight Manager in the `/home/arcsight/` directory, for example `/home/arcsight/manager45sp1`.

Oracle Installation

For more information about Oracle installation, see the *ArcSight ESM Installation and Configuration Guide*. Refer to the *ArcSight ESM Administrator's Guide* for instructions on how to use ArcSight ESM and confirm that initialization was successful. Also, refer to the appropriate Release Notes, available on the ArcSight Customer Support site, <https://support.arcsight.com>.

When you are prompted to set the ArcSight Database Template, ArcSight recommends choosing the Extra Large template. This template will dedicate 6 GB memory for Oracle, leaving enough memory for the ArcSight Manager, operating system, and any other ArcSight components you need.

Restoring Factory Settings

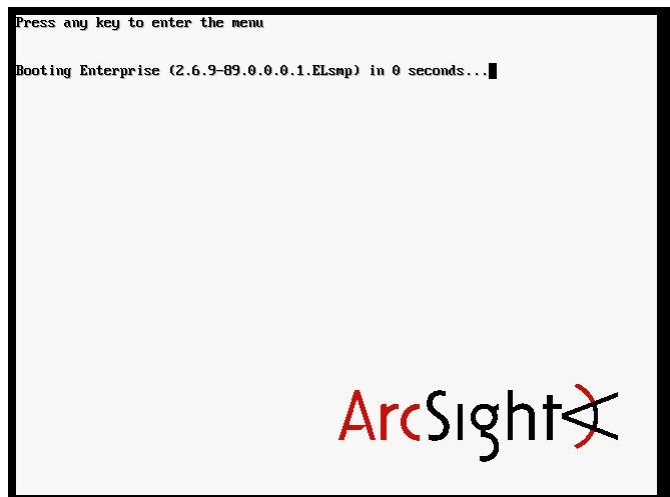
ArcSight ESM Appliance can be restored to its original factory settings using built-in Acronis True Image software.



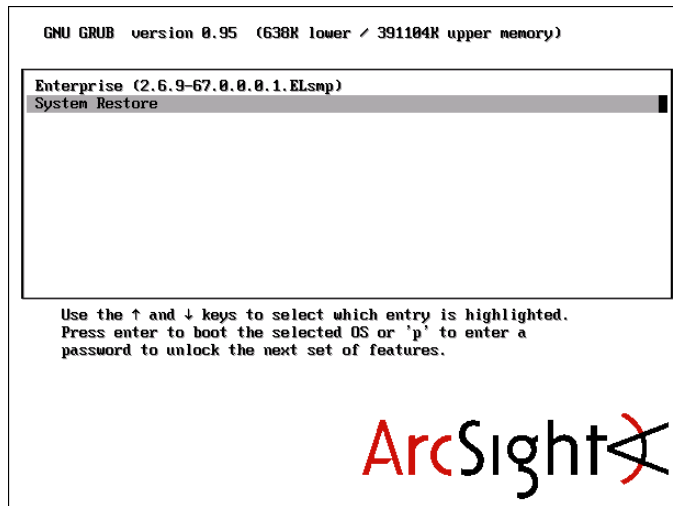
Restoring ArcSight ESM Appliance to factory settings will irrevocably delete all event data and configuration settings.

To restore ArcSight ESM Appliance to its original factory settings, perform these steps:

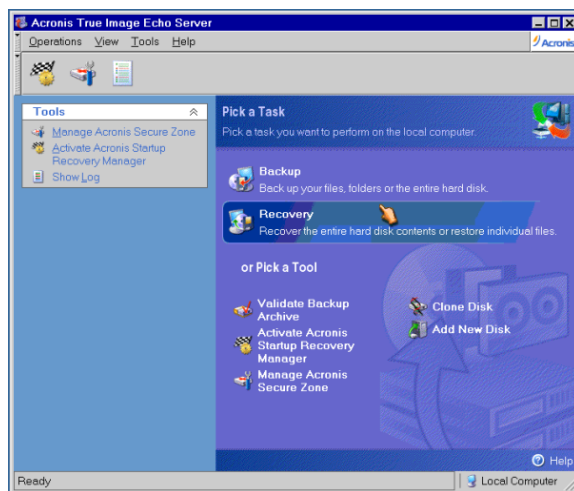
1. Attach a keyboard, monitor, and mouse directly to the ArcSight ESM Appliance system.
2. Reboot ArcSight ESM Appliance.



- When the system has started, use the mouse or arrow keys to select **System Restore** and press **Enter**.



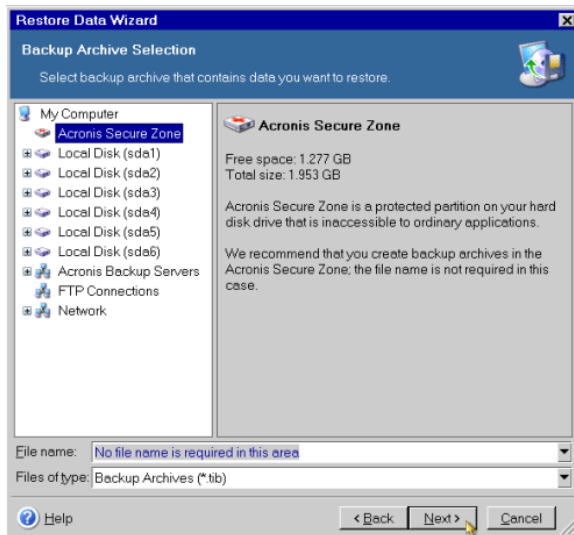
- On the Pick a Task list, choose **Recovery**.



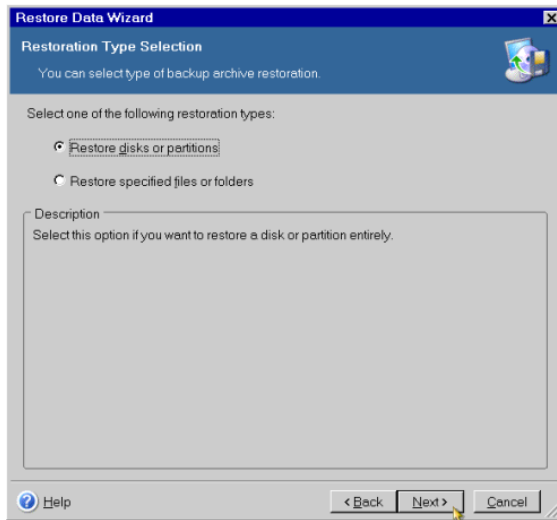
5. The Restore Data Wizard opens. Click **Next** to continue.



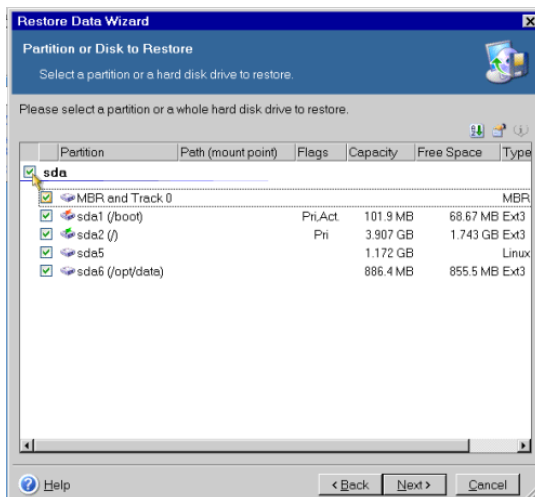
6. Select the Acronis Secure Zone and click **Next**. You will have an opportunity to review the choices you make on this page and the wizard pages that follow before initiating the restore process.



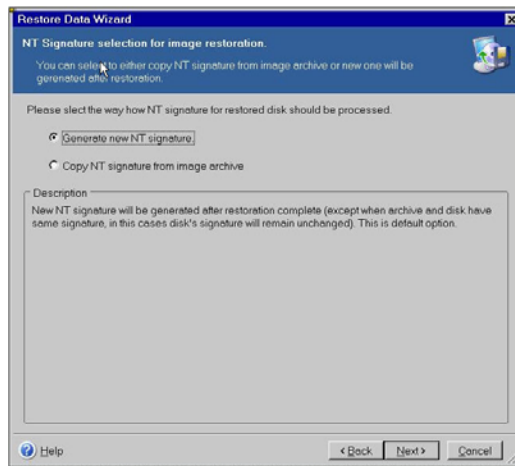
7. Select **Restore disks or partitions**, and then click **Next**. Only choose other options if specifically directed to do so by ArcSight Customer Support.



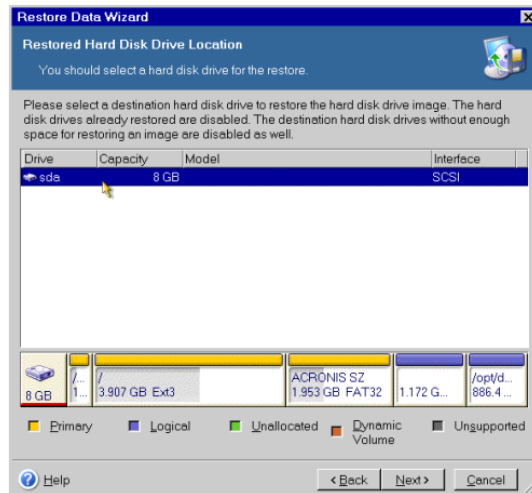
8. Select the entire drive, labeled 'sda' in the figure below. Click **Next** to continue.



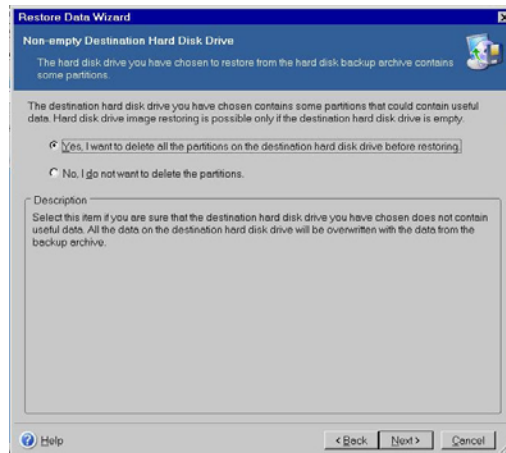
9. Select **Generate new NT signature**, and then click **Next**.



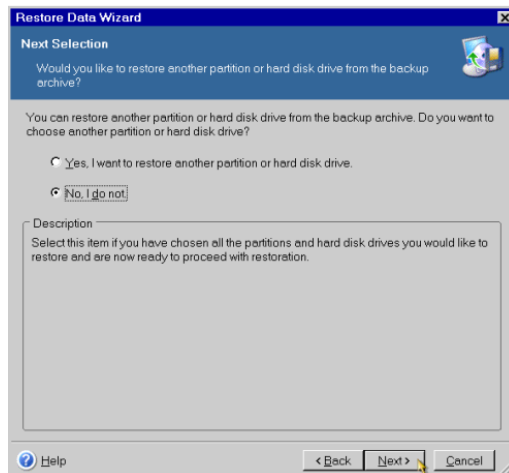
10. Choose the drive to restore ('sda'), and then click **Next**.



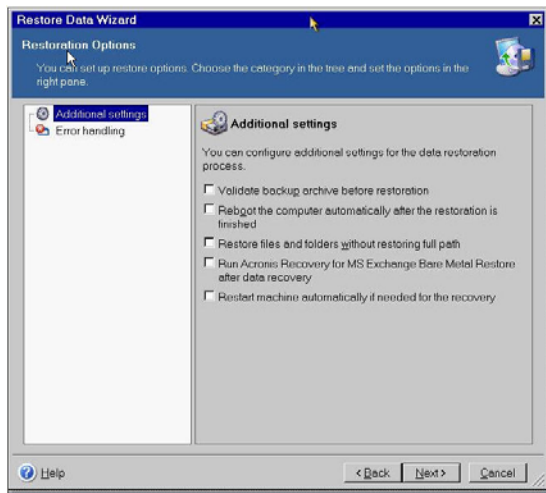
11. Choose **Yes, I want to delete all the partitions on the destination hard disk drive before restoring**, and then click **Next**.



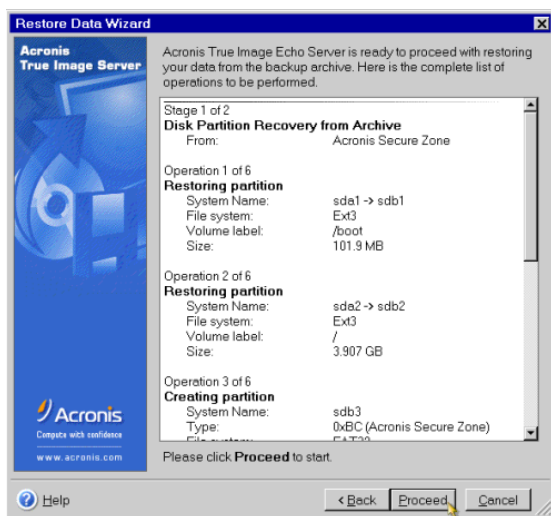
12. Because there are no other partitions or disks to restore, choose **No, I do not**, and then click **Next**.



13. Select **Restart machine automatically if needed for recovery**, and then click **Next**.

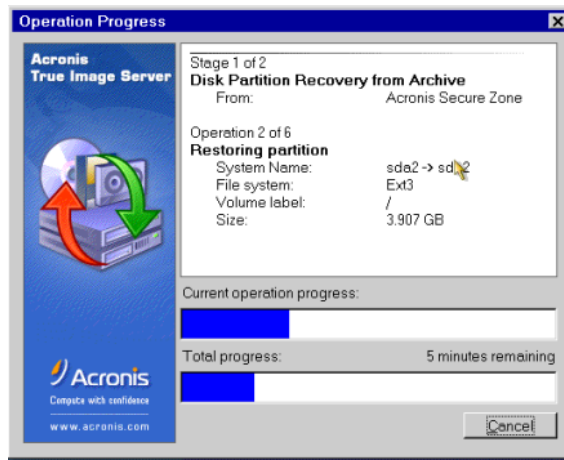


14. Review the checklist of operations to be performed and click **Proceed** to begin the restore process, or click **Back** to revisit previous wizard pages.



Do not interrupt or power-down ArcSight ESM Appliance during the restore process. Interrupting the restore process may force the system into a state from which it cannot be recovered.

15. The progress bars shown in the figure below display the status of the current and total operations. When the restoration is complete, an alert is displayed that says "Data was successfully restored." Click **OK**.



16. Close the Acronis True Image Server window to reboot ArcSight ESM Appliance.

Customer Support

To answer any questions, contact ArcSight Customer Support:

Phone: 1-866-535-3285 (North America)

+44 (0)870 141 7487 (EMEA)

E-mail: support@arcsight.com

Web: <https://support.arcsight.com>