



CWSIMSE Migration Procedure Guide

Version 3.3

OL-8397-01

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Tel:408 526-4000
Fax:408 526-4100
<http://www.cisco.com>



Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706 USA
<http://www.cisco.com>
Phone: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

CWSIMSE Migration Procedure Guide

Revision: 121305

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Copyright © 2005, Cisco Systems, Inc.

All rights reserved

Contents

Foreword	1
1 Migration Requirements	
Migration Details	9
Migration Prerequisites and Restrictions	10
Requirements for CWSIMSE Appliance	11
Linux Operating System Requirements	11
Packages	11
Disk Partition Size	12
Staging/Production Server Requirements	13
Required CWSIMS 3.3 Software Installation Parameters	14
Allocating Proper Disk Space for Appliance Data	16
2 Migration Procedures	
Migration Methods	17
Appliance Migration Procedure	18
Using the Migration Utility	21
Back Up Appliance Configuration Data	21
Archive Security Data	22
Restore Appliance Configuration Data	23
Post-migration Procedure for CWSIMS 3.3 Solaris Systems Running the nF Unix File Agent	24
Restore Security Data	26
3 NFS Mount Information	
CWSIMSE 3.1 NFS Mount Requirements	27
Enable NFS Mounted Systems	28
NFS Mount Information for Archiving Data	28
Appliance to Staging/Production Server (Linux)	28
Appliance to Staging/Production Server (Solaris)	29
NFS Mount Information for Restoring Data	30
Staging/Production Server to CWSIMS 3.3 Production Server (Solaris)	30
Staging/Production Server to the CWSIMS 3.3 Production Server (Linux) . .	32

Foreword

netForensics is a SIM vendor with an integrated family of enterprise-class products and services that are based on the proven, repeatable nFX information security methodology. This combination empowers security organizations to combat threats more efficiently, while connecting the security organization with network operations, compliance, and risk management.

CiscoWorks SIMS (CWSIMS, also known as the nFX Open Security Platform, or nFX OSP) enables security organizations to combat, identify, and respond to threats, and mitigate risk with reduced time to remediation. CWSIMS is a completely integrated solution, combining real-time monitoring and notification with forensic analysis, reporting, and incident resolution workflow to unify remediation efforts. CWSIMS architecture can scale to deliver continuous security information management across a complex, distributed, and heterogeneous enterprise.

Who Should Read this Document?

This guide provides details about migrating from a CWSIMSE appliance to a CWSIMS 3.3 production server. It is designed for system and network administrators and others in charge of computer networks.

Document Contents

[Migration Requirements](#) - information about the requirements concerning all aspects of migrating from a CWSIMSE appliance to a CWSIMS production server are discussed with the requirements varying based on the different methods used to migrate.

[Migration Procedures](#) - includes detailed information about the different methods available for upgrading from a CWSIMSE appliance to a CWSIMS production server.

[NFS Mount Information](#) - includes detailed information about requirements and procedures for mounting NFS directories on both a CWSIMSE appliance and a CWSIMS 3.3 production server running on Solaris or Linux.

Document Conventions

The following text conventions are used in this document:

- Menu items, button names and commands appear in **bold**.
- Paths in the nF Admin tree appear in smaller, **bold italic** text.
- New or important terms and document titles appear in *italics*.
- Text that you see on the screen appears in a `screen font`.
- Variables appear between brackets in an italic screen font: *<variables>*
- Command input and file names appear in a **bold screen font**.
- Variables for which a value is required appear between brackets in a bold italic screen font: ***<file name>***
- The **Start > Run** option represents clicking the **Start** button on the Taskbar, and then clicking **Run** from the pop-up menu.
- When typing commands, you must press [**Enter**] to invoke any command, even if you are not expressly told to do so.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Cisco will continue to support documentation orders using the Ordering tool:

- Registered Cisco.com users (Cisco direct customers) can order documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- Instructions for ordering documentation using the Ordering tool are at this URL:
http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip



We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Important



Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs.

The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting show command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
or view the digital edition at this URL:
<http://ciscoiq.texterity.com/ciscoiq/sample/>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

Migration Requirements

1

Review the following information before you start data migration from a CWSIMSE appliance to the CWSIMS 3.3 production server. The method of migration that you use determines which requirements apply to you. This chapter includes the following sections:

- [Migration Details](#)
- [Migration Prerequisites and Restrictions](#)
- [Requirements for CWSIMSE Appliance](#)
- [Staging/Production Server Requirements](#)
- [Allocating Proper Disk Space for Appliance Data](#)

Migration Details

The details of the migration utility are described in the following table:

Release Date	08/08/2005
File Name	nFMigration.sh
Supported Platforms for Backing up Data	CWSIMSE Appliance version 3.1 (migrated to 3.1.1.01) or CWSIMSE Appliance version 3.1.2
Supported Platforms for Restoring Data	Red Hat Linux Advanced Server 2.1, Red Hat Linux Advanced Server 3.0, Solaris 8, Solaris 9

Migration Prerequisites and Restrictions

The following table contains critical information in reference to using the migration utility to migrate your data to a CWSIMS 3.3 production server:

Archiving data and backing up configuration	<p>The migration utility requires CWSIMSE Appliance version 3.1 (migrated to CWSIMSE 3.1.1.01) or 3.1.2 to be installed to archive security data and/or backup existing configuration settings.</p> <p>Please refer to Cisco.com. See Obtaining Additional Publications and Information on page 7 for access to release notes associated with updating to 3.1.1.01.</p>
Restoring security data and configuration parameters	<p>For the migration utility to be able to restore existing event data and/or configuration parameters, you must have CWSIMS software version 3.3 installed in conjunction with Point Update 49455.</p> <p>Please refer to <i>CiscoWorks SIMS 3.3 Release Notes</i> for information about installing this version of the software. Refer to <i>CWSIMSE Migration Release Notes</i> for information on applying the 49455 Point Update.</p>
Migration restrictions	<ul style="list-style-type: none">• Configuration data for components installed on machines remotely connected to the appliance, will not be migrated.• Migration of all components is expected to be done only once.• If a Unix agent was active on the appliance, the Unix messages logged by this agent will be migrated as they are (using the appliance's hostname).• Configuration information related to external engines (Engine to Engine forwarding) will not be migrated.• The backup and restore of scheduled reports is not supported by the migration utility.• The backup and restore of security data (.dat) files that have been archived previous to using the migration utility will not be migrated automatically. These files must be copied to the new CWSIMS 3.3 production server manually. Their location upon restore is then declared within nF Restore Utility's Archive Data Directory field.

Requirements for CWSIMSE Appliance

If you plan to install CWSIMS 3.3 software using the CWSIMSE appliance hardware, you must rebuild the operating system on the appliance prior to installing CWSIMS. Rebuilding the operating system using the requirements listed below ensures that the appliance hardware is configured to properly handle the memory constraints associated with the CWSIMS 3.3 software.

The following requirements and guidelines must be followed when configuring your appliance to run CWSIMS 3.3.

- [Linux Operating System Requirements](#)
- [Disk Partition Size](#)

Important



Disk partition size suggested is based on the size of the appliance hardware.

Linux Operating System Requirements

The following are the packages to be selected while installing Red Hat AS 3.0

- X Windows System
- Software Development
- Kernel Development

Important



Do not install Legacy Support packages as this will interfere with Oracle installation.

Packages

The following packages are required for the successful installation of Oracle. Before starting the CWSIMS and Oracle installation, copy these from the CD and install them on the appliance.

- Compat-db-4.0.14-4
- Compat-gcc-c++-7.3-2.96.122
- Compat-gcc-7.3-2.96.122

- Compat-libstdc++-7.3-2.96.122
- Compat-libstdc++-devel-7.3-2.96.122
- Openmotif21-2.1.30-8
- Setarch-1.3-1
- Pmake-1.45-10

Please refer to the *CiscoWorks SIMS Version 3.3 Release Notes* and the *nFX OSP Unix and Windows Installation Guide* for details concerning system configuration and installation procedures for installing CWSIMS.

Disk Partition Size

The following is the suggested disk partitioning for an appliance:

/var	2 G
/usr	2 G
swap	2 G
/tmp	1 G
/tftpboot	596 M
/opt	600 M
/boot	99 M
/	1 G
/adata	10 G
/rptschedule	5.7 G
/home	111 G - Though 111G should be available, 6 G does not show up and so only 105 G is available. After the CWSIMS and Oracle installation, out of the 105 G, only 101 G is left. Out of the 101G, reserve 4 G for /home/nf and use 97 G for Oracle.
/home/nf	4 G
/home/oracle	97 G

Staging/Production Server Requirements

If a staging server is being used to hold only the backed up appliance data, and will not be used as the new CWSIMS installation, the requirements are governed by the size of data being backed up. To determine the size of the files generated by the appliance backup see [“Allocating Proper Disk Space for Appliance Data” on page 16](#).

If a new machine is being used as the production server and will be used to run CWSIMS 3.3, then the system configuration must adhere to the minimum requirements in the *nFX OSP Unix and Windows Installation Guide*.

For procedural information on migrating to CWSIMS 3.3 see [“Appliance Migration Procedure” on page 18](#).

Required CWSIMS 3.3 Software Installation Parameters

When installing CWSIMS3.3 during the migration process the following parameters should be followed:

1. Under "Install Netforensics Components", select the box "NetForensics", then select the home directory as "/home/nf" for NF, and "/home/oracle" for Oracle.
2. When prompted for Oracle Server Path, Data Path, Index Path and Rollback & Temp Path, select the appropriate directory based on the requirements outlined in the section, "Disk Partition Size" on page 12.

The following table displays an example of some possible values (subdirectories) the installation program will create and append to "/home/oracle":

Parameter	Value entered and Created
Oracle Server Path	/home/oracle/software
Data Path	/home/oracle/data
Index Path	/home/oracle/index
Rollback & Temp Path	/home/oracle/rbs

3. For Oracle "SGA" Calculator, choose "Custom", using the following values:

DB Recycle Cache	890.0
DB_Cache_Size	400.0
shared_pool_size	85.0
pga_aggregate_size	1000.0

Important



The above values for the Oracle SGA Calculator should only be used for appliances (previously running CWSIMSE). For information on establishing these values for CWSIMS 3.3 installations that use a production/staging server, please refer to the *nFX OSP Unix and Windows Installation Guide*.

4. Select the "Standard" license.

Important



Enterprise License is not supported.

5. Enter the number of messages the appliance is currently receiving when prompted for the "Number of Messages".
6. You must select "UTC" as the time zone because this is the standard time zone used for all appliance and agent installations. Selecting time zones other than UTC will result in incorrect timestamps being applied to the restored security events.

Important



When installing CWSIMS 3.3 software on the appliance, you must make certain that:

- The operating system must be re-installed when selecting the original appliance as the new CWSIMS 3.3 installation using "UTC" as the timezone.
- The newly installed 3.3 version should not be used before the migration is complete in order to avoid any data being overwritten.
- Point Update 49455 must be applied in conjunction with CWSIMS 3.3.
- All agents must be installed on the new system running at the 3.3 level.

Please refer to the *nFX OSP Unix and Windows Installation Guide* for a complete description of the installation process.

Allocating Proper Disk Space for Appliance Data

When installing the operating system on the production server you must take into account the disk space required for the data backed up from the appliance, particularly the file sizes associated with the backed up security event data. In order to allocate the correct amount of disk space for your backed up appliance data, follow the steps below:

1. Run the following command from an SQLplus prompt:

```
select sum(blocks) from user_tables where table_name in  
( 'HIGHSEVERITYEVENTS', 'LOWSEVERITYEVENTS', 'RELATEDEVENTS',  
'EVENTINFO' );
```

- » The query returns the current size used for event data in blocks which is then used to determine the total amount (in MB) of event data.

For example:

If our query returns 150 blocks we can use the following calculation knowing the constant of 8192 bytes per block:

$$(150 * 8192) / 1024 / 1024 = 1.17$$

The total space used/required by the events for this system is 1.17MB

Migration Procedures

2

This chapter discusses the different methods that can be employed for upgrading from a CWSIMSE appliance to a CWSIMS 3.3 production server. When selecting the migration method best suited for your enterprise, please take into account the prerequisites for both hardware and software which are listed in the ["Migration Requirements" on page 9](#).

Migration Methods

The two methods discussed for upgrading a CWSIMSE appliance to a CWSIMS 3.3 production server are:

- **Method 1 - Installation of CWSIMS 3.3 software on the existing CWSIMSE appliance**

This method includes the use of a staging server which is used to hold data backed up from the appliance. Once the data is stored, the appliance is rebuilt with a newly installed operating system and CWSIMS 3.3. The appliance data is then restored from the staging server using the migration utility and the restore utility that exists in the CWSIMS software.

In addition, there are certain limitations that must be accounted for and planned when using an appliance to run the full version of CWSIMS. Please refer to ["Requirements for CWSIMSE Appliance" on page 11](#) for more information.

- **Method 2 - Installation of CWSIMS 3.3 software on a new production server**

This method includes preparing an additional production server to run the CWSIMS 3.3 application. The migration utility is used to archive appliance data on the production server and then restore that data using the restore utility that exists in the CWSIMS software.

Both methods for migration are taken into account within the steps described in the ["Appliance Migration Procedure" on page 18](#).

Appliance Migration Procedure

Important



We recommend that you use a Cisco-certified MCS Server as your production server. For more information, go to:

<http://www.cisco.com/go/sims>

From that location, read the Q&A to obtain the part number of a suitable HP MCS server.

The following steps outline the procedure for migrating from a CWSIMSE appliance (using the existing appliance hardware) to a CWSIMS 3.3 production server.

1. Verify that the CWSIMSE appliance is running the correct version level for migration.

Important



The CWSIMSE appliance must be running either 3.1.1.01 or 3.1.2. Please refer to ["Migration Prerequisites and Restrictions" on page 10](#) for more information.

2. Prepare the staging server to store backed-up data from the appliance. Perform the following task(s) based on your migration scenario:
 - If the staging server will also be used as the new CWSIMS 3.3 production server, install CWSIMS 3.3 on the staging server.
 - If the staging server is only being used to store the archived appliance data, refer to ["Staging/Production Server Requirements" on page 13](#) for more information.

Whether you are using a staging server or a production server to store the backed-up appliance data, you must take into account the disk space requirement for the stored appliance data. See ["Allocating Proper Disk Space for Appliance Data" on page 16](#) for detailed information on configuring your hardware to account for these restrictions.

3. [Enable NFS Mounted Systems](#) on both the appliance and the staging/CWSIMS production server being used for the migration.

The procedures for enabling NFS mounted systems on appliances and staging/production servers differs according to the operating systems they run.

[NFS Mount Information for Archiving Data \(page 28\)](#), includes the appropriate procedure for every relevant operating system:

- ["Appliance to Staging/Production Server \(Linux\)" on page 28](#)
- ["Appliance to Staging/Production Server \(Solaris\)" on page 29](#)

Important



The listed procedures assume the use of similar operating systems. If this is not true for your migration scenario, select the appropriate procedure based on the operating system running on each particular machine as outlined below:

- [Staging/Production Server Running Linux \(page 28\)](#)
- [Appliance Running Linux \(page 29\)](#)
- [Staging/Production Server Running Solaris \(page 29\)](#)
- [Appliance Running Linux \(page 30\)](#)

Please refer to [“CWSIMSE 3.1 NFS Mount Requirements” on page 27](#) for systems running this version of the appliance software.

4. Share the external drive on the staging or production server so it can be mounted from a CWSIMSE appliance. See [“Enable NFS Mounted Systems” on page 28](#) for more information.

Important



Ensure that the drive has the proper write permissions that will provide access for the migration utility.

5. Mount the shared drive created on the staging/production server as a local partition on the appliance. See [“Enable NFS Mounted Systems” on page 28](#) for more information.
6. On the appliance, log in as **nf**.
7. Download the migration utility file (`nFXMigration.tar`) from the CWSIMS product download page (<http://www.cisco.com/go/sims>), and copy the file to a temporary directory.

For example:

```
/tmp
```

8. Extract the `nFXMigration.tar` file as shown below:

```
tar -xvf nFXMigration.tar
```

- The migration utility (`nFMigration.sh`) is extracted to the “nFXMigration” subdirectory which is created under the directory where the tar file resides. For example:

/tmp/nFXMigration

9. Use the migration utility to backup the appliance configuration data on the staging/production machine using the procedure outlined in the [Back Up Appliance Configuration Data \(page 21\)](#) section.
10. Use the migration utility to backup the appliance event data on the staging/production server using the procedure outlined in the [Archive Security Data \(page 22\)](#) section.
11. If you are using the appliance hardware to run CWSIMS 3.3, install CWSIMS 3.3 on the appliance machine. Please refer to "[Requirements for CWSIMSE Appliance](#)" on [page 11](#) for details on completing this task.

Important



You must [Enable NFS Mounted Systems](#) if you are using the appliance hardware to run CWSIMS 3.3. (See [Step 3](#) earlier in this procedure for more information).

12. Run the migration utility to restore the appliance configuration data to the system running CWSIMS 3.3. Please refer to "[Restore Appliance Configuration Data](#)" on [page 23](#) for details on completing this task.

Important



If your new CWSIMS system configuration includes running the Unix Agent on the Solaris platform, you must complete the post migration procedure. See "[Post-migration Procedure for CWSIMS 3.3 Solaris Systems Running the nF Unix File Agent](#)" on [page 24](#).

13. Restore the archived event data on the system running CWSIMS 3.3. Please refer to "[Restore Security Data](#)" on [page 26](#) for details on completing this task.

Using the Migration Utility

The migration utility is a command line interface that allows users to migrate the configuration and security event data from the CWSIMSE appliance to a CWSIMS 3.3 production server.

The procedure for migrating appliance data is outlined in ["Appliance Migration Procedure" on page 18](#). This section describes the following functions of the migration utility.

- [Back Up Appliance Configuration Data \(page 21\)](#)
- [Archive Security Data \(page 22\)](#)
- [Restore Appliance Configuration Data \(page 23\)](#)
- [Post-migration Procedure for CWSIMS 3.3 Solaris Systems Running the nF Unix File Agent \(page 24\)](#)
- [Restore Security Data \(page 26\)](#)

Back Up Appliance Configuration Data

The migration utility's backup function enables your existing appliance configuration to be saved and restored on your CWSIMS 3.3 production server. The naming convention used for the files that store appliance configuration data is as follows:

```
nFMigrate<YYYYMMDDHHMMSS>.zip
```

the variable <YYYYMMDDHHMMSS> designates the year, month, day, hour, minutes and seconds. For example:

```
nFMigrate20050803113004.zip
```

Important



Please note that this file is used when you ["Restore Appliance Configuration Data"](#).

Follow the steps below to back up configuration data:

1. Log in as **nf** on the appliance.
2. Run the migration utility using one of the following methods:
 - From the same directory where the migration utility resides:

```
$ ./nFMigration.sh
```

- From any directory:
\$ /<path to migration utility>/nFMigration.sh
3. Select option [2] from the menu and press **Enter**.
 - You are prompted for the destination directory to use for the backup file.
 4. Enter the absolute path to the directory where the backup file will be stored and then press **Enter**.
 - This directory location can either be either a local directory on the appliance or an NFS mounted directory.

Archive Security Data

The security data on your appliance is backed up using the standard CWSIMS format. An example of the files created by the archive function is shown below:

```
HIGHSEVERITYEVENTS1.dat.gz
LOWSEVERITYEVENTS1.dat.gz
LOWSEVERITYEVENTS2.dat.gz
RELATEDEVENTS1.dat.gz

nF_1_FULLEVENTSBACKUP_20030123231717_20050811200009.ach
```

Important



The number of archived data files created will be based on the amount of data in your organization's database. When additional data files are created, an incremental numeric counter is used to create the filename as shown (for the low severity events) in the example above.

The syntax of the header filename (.ach) reflects the date range of the backed up security data:

```
nF_1_FULLEVENTSBACKUP_<BEGINDATE OF DATA>_<ENDDATE OF DATA>.ach
```

It is this header file that is used when restoring your event data via the migration tool's restore function.

Follow the steps below to archive security data:

1. Log in as **nf** on the CWSIMSE appliance.
2. Run the migration utility using one of the following methods:
 - From the directory where the migration utility resides:
\$./nFMigration.sh

- From any directory:
\$ /<path to migration utility>/nFMigration.sh
3. Select option [1] from the menu and press **Enter**.
 - You are prompted for the destination storage directory to use for files created when archiving the event data.
 4. Enter the absolute path to the storage directory for archived files, then press **Enter**.

Important



The storage directory can be either a local directory on the CWSIMSE appliance or an NFS mounted directory.

To restore the archived data, this storage directory must be declared in the nF Restore boot configuration section. See ["Restore Security Data" on page 26](#) for more information.

Restore Appliance Configuration Data

The migration tool's Restore Appliance Configuration function enables your existing appliance configuration to be restored on your CWSIMS 3.3 production server. The restore function utilizes the files created when using the migration utility to [Back Up Appliance Configuration Data](#).

Important



CWSIMS 3.3 software must be installed on the production server prior to restoring data. Please refer to the ["Migration Procedures" on page 17](#) prior to restoring your data.

Follow the steps below to restore configuration data:

1. Log in as **nf** on the CWSIMS 3.3 production server.
2. Run the migration utility using one of the following methods:
 - From the directory where the migration utility resides:
\$./nFMigration.sh
 - From any directory:
\$ /<path to migration utility>/nFMigration.sh
3. Select option [3] from the menu and press **Enter**.
 - You are prompted for the directory and filename of the backed up configuration file.

4. Enter the absolute path including the zip filename for the backed up configuration, then press **Enter**.

Important



Whenever a restore is initiated on a CWSIMS 3.3 production server, the migration utility backs up the entire database, in addition to the system's configuration files. These files are used to restore an existing configuration in the event that the restored configuration is not successful.

Please refer to ["Post-migration Procedure for CWSIMS 3.3 Solaris Systems Running the nF Unix File Agent"](#) for detailed information about restoring existing data.

Post-migration Procedure for CWSIMS 3.3 Solaris Systems Running the nF Unix File Agent

If your CWSIMS 3.3 production server is Solaris-based and runs the nF Unix File Agent, you must use the post-migration script, `postNFMigrate.sh`. The post-migration script is saved to the `/nFXMigration` subdirectory by default when you extract the `nFXMigration.tar` file.

After you use the post-migration script, you must start nFX Administration and correct the value associated with the physical location of the agent's message file. This parameter value is accessed via the nF Unix File Agent boot configuration section. Complete both procedures associated with this installation scenario:

To run the post-migration script

1. Log in as **nf** on the CWSIMS 3.3 production server.
2. Run the migration utility using one of the two following methods:
 - From the directory where the migration utility resides:

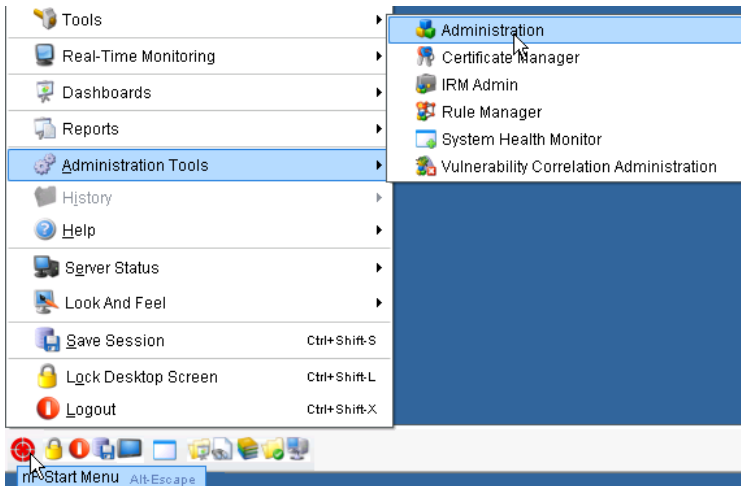
```
$ ./postNFMigrate.sh
```
 - From any directory:

```
$ /<path to post-migration script>/postNFMigrate.sh
```

To Modify the message file location for the Unix Agent

1. Log in to the CWSIMS desktop using a user profile with proper nF Administration access and modify permissions.

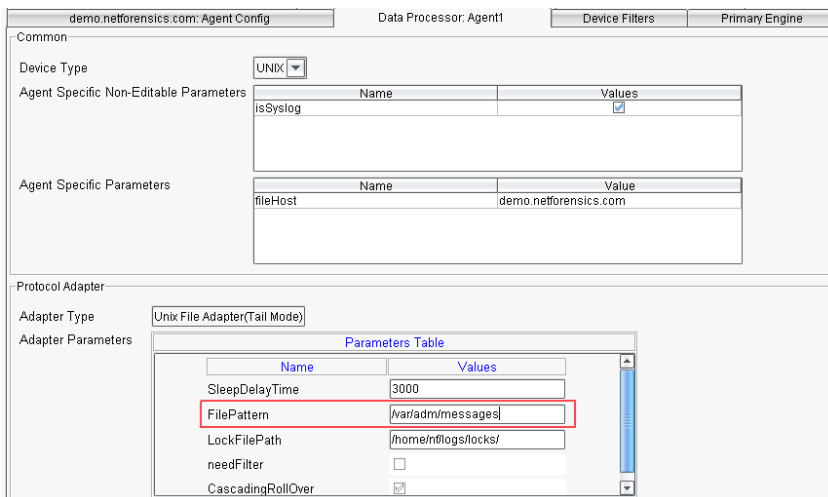
2. Launch nF Administration via the nF Start Menu.



3. Navigate to the nF Unix File Agent boot configuration section (**Component Options>Boot Configuration > [server name] > nF Agent Unix File Agent**).

4. Click the Advanced radio button to display all available configuration options/tabs.

5. Select the Data Processor:Data 1 tab as shown below:



6. Change the message file location to:

`/var/adm/messages`

Restore Security Data

The CWSIMS 3.3 restore utility can be run to restore archived security data associated with the CWSIMSE appliance.

Warning



In order for the migration utility to be able to restore existing event data and/or configuration parameters, you must have CWSIMS 3.3 installed in conjunction with Point Update 49455.

Please refer to *CiscoWorks SIMS 3.3 Release Notes* and/or the *CWSIMSE Migration Release Notes* for detailed information about each release.

Important



Make certain that the archived data files created via the migration utility's [Archive Security Data](#) function are in the directory declared in the nF Restore boot configuration section. See the "nF Restorer" boot configuration section of the *nFX OSP Administration and Configuration Guide* for more information.

Follow the steps below to restore archived files:

1. Log in as **nf** on the machine running the nF Database Server.
2. Change to the `$NF_HOME/bin` directory.
3. Run the restore utility:

```
$ ./nfrestorectl start
```

Important



To restore archived data successfully, the data files must reside within the directory declared in the nF Restore boot configuration section.

See the "nF Restorer" boot configuration section of the *nFX OSP Administration and Configuration Guide* for more information.

If the restore operation fails, refer to **nfrestore.log+timestamp**, **nfrestore_err.log** and **nfrestore_out.log** for further information. These logs can be found in:

`$NF_HOME/logs/tools`

For more information on archiving data see the "Archive and Purge Jobs" section of the *nFX OSP Administration and Configuration Guide*.

NFS Mount Information

3

CWSIMSE 3.1 NFS Mount Requirements

In order to enable NFS clients for systems running CWSIMSE 3.1, the following two additional RPMs (Red Hat Package Management) are required for installation:

- portmap-4.0-41.i386.rpm
- nfs-utils-0.3.3-5.i386.rpm

The above RPMs are included in the `nFXMigration.tar` file. When the `nFXMigration.tar` file is extracted, the above RPMs are copied to the following subdirectory (created under the directory where the tar file resides). For example:

```
/tmp/nFXMigration/rpm
```

Important



The RPMs listed above only required for systems running CWSIMSE 3.1 and are not required for systems running CWSIMSE 3.1.2.

To install the required RPMs on your CWSIMSE 3.1 system:

1. Transfer the RPMs to the CWSIMSE 3.1 appliance.
2. Login as **root**.

```
mount -o remount,rw /usr
```

3. Change to the directory that contains the RPMs.
4. Run the following command to install both RPMs:

```
rpm -Uvh nfs-utils-0.3.3-5.i386.rpm portmap-4.0-41.i386.rpm
```

Enable NFS Mounted Systems

Important



All mount procedures must be performed as the "root" user.

This sections covers

- [NFS Mount Information for Archiving Data](#)
- [NFS Mount Information for Restoring Data](#)

NFS Mount Information for Archiving Data

The following section describes the process for enabling NFS mounted systems on appliances and staging/production servers with respect to archiving appliance data. Sections for Solaris and Linux are included.

Appliance to Staging/Production Server (Linux)

Staging/Production Server Running Linux

Perform the following steps on the staging/production server (where the archived data will be placed).

1. Make a directory for storing the archived files:

```
mkdir <LOCAL DIRECTORY FOR STORING ARCHIVED FILES>
```

2. Change the mode of the created directory.

```
chmod -R 777 <LOCAL DIRECTORY FOR STORING ARCHIVED FILES>
```

3. Make an entry into the exports file ("/etc/exports") as shown below:

```
<LOCAL DIRECTORY FOR STORING ARCHIVED FILES> <IPADDRESS of APPLIANCE>(rw)
```

For example:

```
/tmp/foo cwsimse.foo.com(rw)
```

or

```
/tmp/foo 10.1.11.12(rw)
```

4. Run the following commands:

```
/etc/init.d/nfs restart
```

```
/etc/init.d/portmap restart
```

Appliance Running Linux

Perform the following steps on the appliance (where the CWSIMSE migration tool will be executed):

1. Run the following commands:

```
/etc/init.d/ipchains stop
/etc/init.d/nfs restart
/etc/init.d/portmap restart
```

2. Run the following command:

```
mount <Machine-1 IPADDRESS>:<ARCHIVED DATA LOCATION on MACHINE-1> <LOCAL MOUNT POINT>
```

For example:

```
mount 172.16.110.154:/tmp/foo /home/ghost
```

Appliance to Staging/Production Server (Solaris)

Staging/Production Server Running Solaris

Perform the following steps on the staging server (where the archived data will be placed).

1. Make a directory for storing the archived files:

```
mkdir <LOCAL DIRECTORY FOR STORING ARCHIVED FILES>
```

2. Change the mode of the created directory.

```
chmod -R 777 <LOCAL DIRECTORY FOR STORING ARCHIVED FILES>
```

3. Run the following commands:

```
update /etc/dfs/dfstab
```

```
share -F nfs -o rw=<IPADDRESS OF MACHINE-2> -d "<identifier text>" <LOCAL DIRECTORY FOR STORING ARCHIVED FILES>
```

For example:

```
share -F nfs -o rw=172.16.100.163 -d "restorer dir" /tmp/foo
```

4. Run the following commands:

```
/etc/init.d/nfs.server stop
/etc/init.d/nfs.server start
```

Appliance Running Linux

Perform the following steps on the appliance (where the CWSIMSE migration utility will be executed). Run the following commands:

```
/etc/init.d/ipchains stop
/etc/init.d/nfs restart
/etc/init.d/portmap restart
```

```
mount <Machine-1 IPADDRESS>:<ARCHIVED DATA LOCATION on MACHINE-1> <LOCAL MOUNT POINT>
```

For example:

```
mount 172.16.110.154:/tmp/foo /home/ghost
```

Important



For systems running Solaris 9.0, the host name (of the machine sharing the archived data directory) must be used instead of the machine's IP address. In order for this method of lookup to work properly, the host name used must be present in the system's "/etc/hosts" file.

NFS Mount Information for Restoring Data

The following section describes the process for enabling NFS mounted systems on appliances and staging/production servers, with respect to restoring archived appliance data. Sections for Solaris and Linux are included.

Staging/Production Server to CWSIMS 3.3 Production Server (Solaris)

Staging/Production Server Running Solaris

Perform the following steps on the staging server (where the archived data has been placed).

1. Run the following commands:

```
mkdir <LOCAL DIRECTORY FOR STORING ARCHIVED FILES>
```

2. Change the mode of the created directory.

```
chmod -R 777 <LOCAL DIRECTORY FOR STORING ARCHIVED FILES>
```

3. Run the following commands:

```
update /etc/dfs/dfstab
```

4. Share the drive holding the archived data:

```
share -F nfs -o rw=<IPADDRESS OF MACHINE-2> -d "<identifier text>" <LOCAL  
DIRECTORY FOR STORING ARCHIVED FILES>
```

For example:

```
share -F nfs -o rw=172.16.100.163 -d "restorer dir" /tmp/foo
```

5. Run the following commands:

```
/etc/init.d/nfs.server stop
```

```
/etc/init.d/nfs.server start
```

CWSIMS 3.3 Production Server Running Solaris

Perform the following steps on the CWSIMS 3.3 production server where the Restore Utility (`nfrestorect1`) will be executed:

1. Run the following command:

```
update /etc/vfstab
```

```
<IPADDRESS OF Machine 1>:<LOCATION of the ARCHIVED FILES MACHINE-1> - <MOUNTPOINT  
ON MACHINE-2> nfs - yes rw,hard
```

For Example:

```
172.16.110.154:/tmp/foo - /home/ghost nfs - yes rw,hard
```

2. Run the following command:

```
umask 022
```

3. Mount the machine and directory where the archived files are stored:

```
mount <Machine-1 IPADDRESS>:<LOCATION of the ARCHIVED FILES MACHINE-1>  
<LOCAL MOUNT POINT>
```

For example:

```
mount 172.16.110.154:/tmp/foo /home/ghost
```

Please refer to the ["Restore Security Data" on page 26](#) for information on running the restore utility.

Staging/Production Server to the CWSIMS 3.3 Production Server (Linux)

Staging Server Running Linux

Perform the following steps on the staging server (where the archived data has been placed).

1. Make a directory for storing the archived files:

```
mkdir <LOCAL DIRECTORY FOR STORING ARCHIVED FILES>
```

2. Change the mode of the created directory.

```
chmod -R 777 <LOCAL DIRECTORY FOR STORING ARCHIVED FILES>
```

3. Make an entry into the exports file ("/etc/exports") as shown below:

```
<LOCAL DIRECTORY FOR STORING ARCHIVED FILES> <IPADDRESS of APPLIANCE>(rw)
```

For example:

```
/tmp/foo cwsimse.foo.com(rw)
```

or

```
/tmp/foo 10.1.11.12(rw)
```

4. Run the following commands:

```
/etc/init.d/nfs restart
```

```
/etc/init.d/portmap restart
```

CWSIMS 3.3 Production Server Running Linux

Perform the following commands on the CWSIMS production server where the nfrestorectl will be executed:

```
/etc/init.d/ipchains stop
```

```
/etc/init.d/nfs restart
```

```
/etc/init.d/portmap restart
```

```
umask 022
```

```
mount <Machine-1 IPADDRESS>:<ARCHIVED DATA LOCATION on MACHINE-1> <LOCAL MOUNT POINT>
```

For example:

```
mount 172.16.110.154:/tmp/foo /home/ghost
```

Please refer to the ["Restore Security Data" on page 26](#) for information on running the restore utility.