



netForensics®

Quick Start Guide

Version 3.1
April 2003
78-15512-01

A **Leader** in
Security Information Management



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

netForensics Quick Start Guide

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 NON-INFRINGEMENT 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.

CCIP, CCSP, the Cisco Arrow logo, the Cisco Powered Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Net Readiness Scorecard, Networking Academy, and ScriptShare are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, LightStream, MGX, MICA, the Networkers logo, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0303R)

Copyright © 2003, Cisco Systems, Inc.

All rights reserved

Contents

1 Overview

Components	1
Engine	1
Master	1
Provider and Data Server	1
Agents	1
Report Scheduler	2
System Health Monitor	2

2 Skills Requirements

Solaris/Linux	3
Windows	3

3 System Requirements

Supported Operating Systems	4
Solaris Patches and Packages	5
Hardware and Software Requirements	5
General Requirements	10
Access Control	10
Static IP Address	10
Java™ 2 Runtime Environment and Java™ Web Start	10
NTFS Volumes (Windows only)	10
NIS-based Installations (UNIX only)	10
Automount Daemon (UNIX only)	10
Permission to Run Cron Jobs (UNIX only)	10
X Windows (UNIX only)	10

4	Installation Planning	
	Sizing Considerations	11
	Disk Partitions	11
5	Installation	
	Media	12
	Full or Custom Installation	12
	Getting Help	12
	Installation Steps	12
6	Logging In	
	netForensics Launch Window	13
	Resource Links	14
	Log in to netForensics	15
7	SIM Desktop	
	Quick Launch Icons	17
	Taskbar	18
	Virtual Desktops	19
	Current User	19
	System Resources	19
	Logging Out	19

1 Overview

netForensics is a Security Information Management (SIM) application that works with a heterogeneous array of security products. netForensics utilizes a highly distributable and scalable architecture including separate components for event normalization, filtering, aggregation, and correlation.

Components

Depending on your security network, you can distribute one or more of the following components that make up netForensics.

Engine

The Engine collects, filters, aggregates and forwards security events from nF Agents to the Data Server.

Master

The Master provides real-time cross device correlation, categorization and broadcast services to the SIM Desktop (see ["SIM Desktop"](#) on page 16).

Provider and Data Server

The Provider supplies master data services to all registered netForensics components, helping to facilitate reporting, administration, configuration, patch management and master change notification services.

The Data Server includes Oracle 9i Standard or Enterprise Edition as an industrial strength relational database management system. The Data Server stores forwarded security events used for forensics and generating reports.

Agents

netForensics Agents forward event data from security devices and applications to the netForensics Engine. The following agents are available:

• nF Agent for Arbor Peakflow	• nF Agent for Enterccept	• nF Batch Agent
• nF Agent for Check Point	• nF Agent for ISS RealSecure	• nF Batch Agent for Check Point
• nF Agent for Cisco Secure ACS	• nF Agent for ManHunt	• nF Syslog File Agent
• nF Agent for CSIDS	• nF Agent for Symantec Enterprise Firewall/VPN	• nF Universal File Agent
• nF Agent for CSIDS 4.0	• nF Agent for Sidewinder	• nF Universal RT Agent
• nF Agent for CyberGuard	• nF Agent for Snort	• nF UNIX File Agent
• nF Agent for Dragon	• nF Agent for Tripwire	• nF Windows Event Agent

Report Scheduler

A tool that launches reports, at predefined times or intervals, that have been scheduled from the netForensics Administration User Interface (nF Admin UI).

System Health Monitor

The System Health Monitor (SHM) helps manage netForensics by periodically checking the status of Server and Database components. SHM delivers email notifications, regarding the success or failure of reaching a specific component.

Table 1: netForensics Components to Install by Device/Application

Application/Device	Version	nF Components
Third Party Apps	n/a	Universal Agent
Historical Data	See Syslog File Agent	Batch Agent
Arbor Peakflow DoS	2.1	Agent for Arbor Peakflow
Check Point FireWall-1	NG, 4.1	Agent for Check Point
Cisco IOS ACL, FW, IDS	12.2, 12.0	Syslog File Agent
Cisco Secure ACS	3.0	Agent for CSACS
Cisco Secure IDS	4.0, 3.1, 2.5, 2.2	CSIDS Agent/Syslog Agent
Cisco Secure PIX	6.2, 6.1, 6.0, 5.3, 5.2, 5.1, 5.0	Syslog File Agent
Cisco Secure PIX IDS	6.2, 6.1, 6.0, 5.3, 5.2	Syslog File Agent
Cisco VPN Concentrator	3.1, 2.5.2	Syslog File Agent
CyberGuard Firewall	5.1	Agent for CyberGuard
Dragon Sensor / Squire	5.0 / 1.3.1	Agent for Dragon
Intercept HIDS	2.5, 2.0	Agent for Intercept
ISS RealSecure HIDS / NIDS	6.5, 6.0, 5.5 / 7.0, 6.5, 6.0	Agent for ISS RealSecure
Secure Computing Sidewinder FW	5.2	Agent for Sidewinder
Snort NIDS	1.8	Agent for Snort
Symantec Enterprise FW/VPN	7.0, 6.5	Agent for Symantec Enterprise Firewall/VPN
Symantec ManHunt NIDS	2.2	Agent for ManHunt
Tripwire NIDS	3.0	Agent for Tripwire
UNIX OS Events	Solaris 8/7/6, Linux 7.2/7.1	UNIX OS File Agent
Windows Events	Win 2000 Server / Adv. Server	Windows Event Agent

2 Skills Requirements

Important



You should be familiar with the security devices that you want to monitor and be able to configure those devices to work correctly with netForensics.

Solaris/Linux

You must be familiar with basic UNIX operations. For example, you need to know how to:

- Install an operating system
- Install software packages
- Work with basic network parameters such as setting the host name, setting the DNS name, and updating DNS
- Establish NFS services and set up an NFS share
- Create disk partitions
- Run commands

If you are not sure that you can perform these tasks, please acquire these skills before you begin the installation.

Windows

You must be familiar with basic Windows 2000 operations. For example, you need to know how to:

- Navigate (using **Start > Run**) to the location of the setup program.
- Install software packages

If you are not sure that you can perform these tasks, refer to your Windows 2000 documentation or online help.

3 System Requirements

Supported Operating Systems

Table 2 lists the supported operating systems for different netForensics components.

Table 2: Quick Lookup for Supported Operating Systems

Component	Supported Operating System
nF Engine	Red Hat Linux, Solaris 8
nF Master	Red Hat Linux, Solaris 8
nF Provider/Oracle 9i Database	Red Hat Linux, Solaris 8
nF Web Server	Red Hat Linux, Solaris 8
nF Agent for Arbor Peakflow	Red Hat Linux, Solaris 8, Windows 2000
nF Agent for Check Point	Red Hat Linux, Solaris 8, Windows 2000
nF Agent for CSACS	Windows 2000
nF Agent for CSIDS	Red Hat Linux, Solaris 8
nF Agent for CSIDS 4.0	Red Hat Linux, Solaris 8, Windows 2000
nF Agent for CyberGuard	Red Hat Linux, Solaris 8, Windows 2000
nF Agent for Dragon	Red Hat Linux, Solaris 8
nF Agent for Enterecept	Windows 2000
nF Agent for ISS RealSecure	Windows 2000
nF Agent for ManHunt	Red Hat Linux, Solaris 8, Windows 2000
nF Agent for Symantec Enterprise Firewall/VPN	Solaris 8, Windows 2000
nF Agent for Sidewinder	Red Hat Linux, Solaris 8, Windows 2000
nF Agent for Snort	Red Hat Linux, Solaris 8
nF Agent for Tripwire	Red Hat Linux, Solaris 8, Windows 2000
nF Agent for Windows	Windows 2000
nF Batch Agent	Red Hat Linux, Solaris 8
nF Batch Agent for Check Point	Red Hat Linux, Solaris 8, Windows 2000
nF Syslog File Agent	Red Hat Linux, Solaris 8, Windows 2000
nF Universal Agents	Red Hat Linux, Solaris 8, Windows 2000
nF UNIX File Agent	Red Hat Linux, Solaris 8

NOTE: Red Hat Linux 7.1 (Kernel 2.4.9) or Advanced Server **only**; Windows 2000 Server/Advanced Server (SP2) **only**; Solaris on SPARC **only**

Solaris Patches and Packages

The latest patches and packages for Solaris can be obtained from:

<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

The following packages and patches should be installed – **in the order listed below** – on any server hosting a netForensics component (Tool, Server, or Agent):

- SUNWarc, SUNWarcx, SUNWcsl, SUNWcslx, SUNWcscr, SUNWcstl, SUNWcstlx, SUNWcstx, SUNWcscu, SUNWcscux, SUNWdplx, SUNWdtbax, SUNWdtwm, SUNWhea, SUNWi1cs, SUNWiimr, SUNWiimu, SUNWmdb, SUNWmfrun, SUNWxi18n, SUNWxi18x, SUNWxim, SUNWximx, SUNWxwaxm, SUNWxwfa, SUNWxwfnt, SUNWxwice, SUNWxwicx, SUNWxwinc, SUNWxwman, SUNWxwpld, SUNWxwplx, SUNWxwpmn, SUNWxwslb
- Solaris 8 Recommended Cluster Patch
- J2SE for Solaris 8 Cluster Patch
- <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/J2SE>
- The following packages are also required on the netForensics **Provider**: SUNWbtool, SUNWlibm, SUNWlibms, SUNWsprt, SUNWtoo

Hardware and Software Requirements

Warning



Memory recommendations assume that current system memory is sufficient for supporting existing operating system and applications.

Full Install

Table 3: Minimum System Requirements for Full Install

Component	Requirement
Operating System	See " Supported Operating Systems " on page 4
Processor	Linux: Dual Intel Pentium 4 1.5 GHz (Server class) Solaris: Dual UltraSPARC-III 444 MHz (Server class)
Memory	4 GB total system memory
Free disk space	18 GB (see " Disk Partitions " on page 11 for more information)
Storage Device	CD-ROM
Software Packages	Linux: Anonymous FTP Server, Development Libraries, Kernel Development Solaris 8: See " Solaris Patches and Packages "

Provider and Oracle Database

Table 4: Minimum System Requirements for Database

Component	Requirement
Operating System	See " Supported Operating Systems " on page 4
Processor	Linux: Dual Intel Pentium 4 1.5 GHz (Server class) Solaris: UltraSPARC-III 444 MHz (Server class)
Memory	System memory + 1 GB for Provider and Oracle Database (1536 MB minimum recommended)
Free hard disk space	18 GB (see " Disk Partitions " on page 11 for more information)
Storage Device	CD-ROM
Software Packages	Linux: Anonymous FTP Server, Development Libraries, Kernel Development Solaris 8: See " Solaris Patches and Packages "

WebServer

Table 5: Minimum System Requirements for WebServer

Component	Requirement
Operating System	See " Supported Operating Systems " on page 4
Processor	Linux: Intel Pentium 4 1.0 GHz (Server class) Solaris: UltraSPARC-III 444 MHz (Server class)
Memory	System memory + 64 MB for WebServer (384 MB minimum recommended)
Free hard disk space	1 GB
Storage Device	CD-ROM
Software Packages	Linux: Anonymous FTP Server, Development Libraries, Kernel Development Solaris 8: See " Solaris Patches and Packages "

Engine

Table 6: Minimum System Requirements for Engine

Component	Requirement
Operating System	See " Supported Operating Systems " on page 4
Processor	Linux: Intel Pentium 4 1.0 GHz (Server class) Solaris: UltraSPARC-III 444 MHz (Server class)
Memory	System memory + 256 MB for Engine
Free hard disk space	1 GB
Storage Device	CD-ROM
Software Packages	Linux: Anonymous FTP Server, Development Libraries, Kernel Development Solaris 8: See " Solaris Patches and Packages "

Master

Table 7: Minimum System Requirements for Master

Component	Requirement
Operating System	See " Supported Operating Systems " on page 4
Processor	Linux: Dual Intel Pentium 4 1.5 GHz (Server class) Solaris: UltraSPARC-III 444 MHz (Server class)
Memory	System memory + 256 MB for Master
Free hard disk space	1 GB
Storage Device	CD-ROM
Software Packages	Linux: Anonymous FTP Server, Development Libraries, Kernel Development Solaris 8: See " Solaris Patches and Packages "

netForensics Agents

Table 8 lists the general system requirements for installing an individual agent.

Table 8: Minimum System Requirements for netForensics Agents

Component	Requirement
Operating System	See " Supported Operating Systems " on page 4
Processor	Linux/Windows: Intel Pentium 4 1.0 GHz (Server class) Solaris: UltraSPARC-III 444 MHz (Server class)
Memory	System memory + 64 MB per agent
Free hard disk space	100 MB
Storage Device	CD-ROM
Software Packages	Linux: Anonymous FTP Server, Development Libraries, Kernel Development Solaris 8: See " Solaris Patches and Packages "

Report Scheduler

Table 9: Minimum System Requirements for Report Scheduler

Component	Requirement
Operating System	See " Supported Operating Systems " on page 4
Processor	Linux: Intel Pentium 4 1.0 GHz (Server class) Solaris: UltraSPARC-III 444 MHz (Server class)
Memory	System memory + 128 MB for Report Scheduler
Free hard disk space	1 GB
Storage Device	CD-ROM
Software Packages	Linux: Anonymous FTP Server, Development Libraries, Kernel Development Solaris 8: See " Solaris Patches and Packages "

System Health Monitor

Table 10: Minimum System Requirements for System Health Monitor

Component	Requirement
Operating System	See " Supported Operating Systems " on page 4
Processor	Linux: Intel Pentium 4 1.0 GHz (Server class) Solaris: UltraSPARC-III 444 MHz (Server class)
Memory	System memory + 128 MB for System Health Monitor
Free hard disk space	10 MB
Storage Device	CD-ROM
Software Packages	Linux: Anonymous FTP Server, Development Libraries, Kernel Development Solaris 8: See " Solaris Patches and Packages "

General Requirements

This section provides general system requirements for installing netForensics.

Access Control

Several ports are used by netForensics components (see the *netForensics Installation Guide* for details). Before starting, ensure that communications on these ports is permitted (i.e., via access control lists) throughout the network.

Static IP Address

The netForensics components should be installed on a computer having a static IP address. The computer cannot use a system, such as Dynamic Host Configuration Protocol (DHCP), that dynamically assigns IP addresses.

Java™ 2 Runtime Environment and Java™ Web Start

netForensics requires J2RE Standard Edition 1.4.1 (1.4.1_02 recommended) and Java™ Web Start 1.2. Both are bundled together and available at:

<http://java.sun.com/j2se/1.4.1/download.html>

NTFS Volumes (Windows only)

Windows volumes (hard disks) where netForensics Agents are to be installed should be formatted as NTFS.

NIS-based Installations (UNIX only)

NIS-based installations are not currently supported.

Automount Daemon (UNIX only)

To ensure that CDs are automatically mounted during the installation, make sure **automountd** is running before starting.

Permission to Run Cron Jobs (UNIX only)

The **nf** user should be granted permission to run cron jobs on the netForensics Data Server. Check local policies (`cron.allow` and `cron.deny` files) to ensure these permissions exist.

X Windows (UNIX only)

The installation requires X Windows on the server where the netForensics Database is to be installed. Ensure X Windows is installed before you begin.

4 Installation Planning

Sizing Considerations

The following guidelines should be noted for allocating space to the home partition of the **nf** user for a full install:

- The database should be sized according to the volume of security events and the local retention policy. For more information, log in to the **Support** area of the netForensics website and download the "Database Sizing" document.
- Raw data from Syslog File Agent is stored in \$NF_HOME. A single Syslog File Agent data file (10MB) holds ~62,500 PIX messages (this amount varies and depends on the nature and rate of traffic).
- A typical archive of one million records consumes ~270 MB. When zipped, this same archive consumes ~14 MB. Ensure you have allocated sufficient disk space for \$NF_HOME on the database server.
- The size of scheduled reports can vary greatly. A considerable amount of disk space should be allocated for them (a 425-page PDF report is ~800KB in size). Ensure you have allocated sufficient disk space for \$NF_HOME/reports on the Report Scheduler server.

If you have already installed netForensics and feel that you have not allocated sufficient disk space for \$NF_HOME, create a directory in a partition having sufficient free space and create symbolic links to the original directory.

Disk Partitions

netForensics recommends four disk partitions – u01, u02, u03, u04 – to install Oracle 9i. Partition u01 must be at least 3.5 GB. The netForensics installation also supports the installation of the above components on a single disk partition.

5 Installation

Media

The Installation Kit includes six CDs:

- *CiscoWorks Security Information Manager Documentation*
- *CiscoWorks Security Information Manager Server Installation*
- *CiscoWorks Security Information Manager Agent Installation*
- *CiscoWorks Security Information Manager Database* (Disc 1, 2, 3) - Oracle 9i Standard and Enterprise

Full or Custom Installation

The netForensics installation wizards for **Servers** and **Agents** provide two options: **Full Installation** or **Custom Installation**. The **Full** option installs all listed components on the same server. If you prefer, however, you can distribute any or all of the components across two or more servers with the **Custom** option.

Getting Help

If you need additional information during the installation, click **Help** in the lower-right corner of the installation screens.

Installation Steps

See the *netForensics Installation Guide* for details about installing on your specific operating system.

6 Logging In

The monitoring and reporting tools of netForensics are made available from the SIM Desktop, a Java application that works like the graphical desktop environment of most operating systems. SIM Desktop details are provided in Section 7.

The SIM Desktop is launched with Java™ Web Start, which gives you the power to launch full-featured applications with a single click from your Web browser. Java Web Start is bundled with J2SE™ 1.4.1 (1.4.1_02 recommended), which is required for running netForensics. See the *netForensics User's Guide* for further details about JRE plug-ins and Java Web Start, or go to:

<http://java.sun.com/products/javawebstart/>

To start netForensics, point your browser to the host machine on which the netForensics Web Server has been installed (e.g., <http://myweb.mycompany.com>).

netForensics Launch Window

After browsing to your netForensics WebServer, the netForensics launch window opens.



Figure 1: netForensics Launch Window

The launch window contains:

- Links to additional information and support resources (see Figure 2)
- Link for launching the netForensics SIM Desktop
- Link to the Java Web Start Application Manager and Java Web Start status
- Link to information about cryptography related compliance requirements

Resource Links

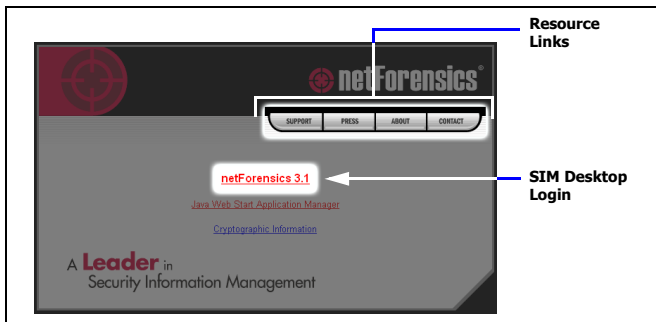


Figure 2: Links to Information and Support Resources

The login window provides links to these topics:

- **Support** - information about netForensics technical support, its hours of operation, and contact methods
- **Press** - netForensics news and events
- **About** - general information about netForensics
- **Contact** - information about contacting netForensics, including office addresses and directions

Important



The resource links in the netForensics launch window are available on the Cisco web site. To use these links, your web server must have access to the Internet.

Important

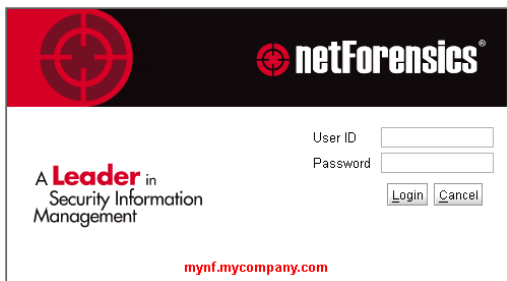


Once the SIM Desktop has been launched, the user can create a shortcut to it on the operating system desktop.

Log in to netForensics

To log in to netForensics:

1. Click the [\[netForensics\]](#) link
 - » The Java Web Start application is launched and the required files are downloaded from the netForensics server
 - » The netForensics Login dialog appears



A Leader in
Security Information
Management

User ID

Password

mynf.mycompany.com

2. Type your user ID and password in the fields provided

Important



User IDs and passwords are case-sensitive, and must be typed exactly as they were created.

Warning



Use admin as the user ID and password to log into netForensics as the default Administrator.

3. Click **Login**
 - » The netForensics SIM Desktop is displayed, indicating that you have successfully logged in.

7 SIM Desktop

The SIM Desktop is an extensible Java application that provides an interactive console that centralizes the control and configuration of netForensics and the real-time monitoring and analysis of security events that are taking place in the network.

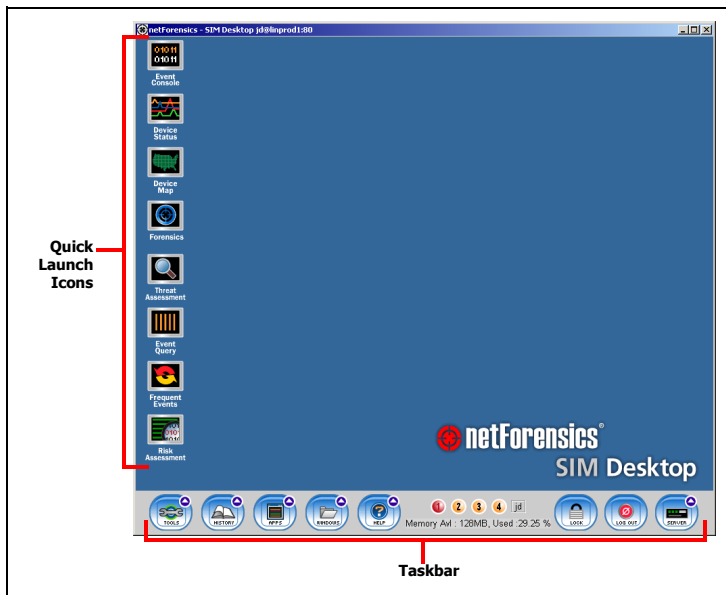










Figure 3: netForensics SIM Desktop

Quick Launch Icons

These icons provide rapid access to the netForensics monitoring and reporting tools and the most frequently used reports. Click any of the following icons to launch the corresponding tool or report:

Icon	Name	Description
	Event Console	A scrolling event viewer that displays details about real-time security events according to user-defined filters: <ul style="list-style-type: none">• Multiple console windows can be displayed• Filters are based on business units, device type, device, severity, alarm, protocol, and source and destination IP• Detailed report, application message, or charts, launched for any event
	Device Status	Displays aggregated, severity-based scores for security devices: <ul style="list-style-type: none">• Displays count for all device types, devices and alarm categories• Displays event count for all devices in the installation• Users can launch charts or event console for specific levels in the tree
	Device Map	Displays business units and devices in a graphical format based on their geographical location: <ul style="list-style-type: none">• Displays aggregated event count for the business units or device instances defined for the current user according to category or severity• Displays event categories as dynamic bar charts• Displays information according to business unit or device• Charts are created dynamically and updated in real time• Displays charts based on category and severity
	Forensics	Launches the netForensics report tree for generating device-independent or vendor-specific reports
	Threat Assessment	Launches the Threat Assessment report, showing the likelihood of specific assets that may come under attack
	Event Query	Launches the Event Query report which shows statistics according to user-defined filters
	Frequent Events	Launches the Frequent Events report which displays the most frequent events, sorted by count for all five severities
	Risk Assessment	Launches the Risk Assessment report which displays the risk of attack for your assets

Taskbar

The taskbar appears at the bottom of your screen. The taskbar contains several buttons, which you can use to launch additional tools, quickly access recent reports, arrange open windows, access help, switch between virtual desktops, lock the SIM Desktop, view the status of netForensics servers, and log out of your current session.

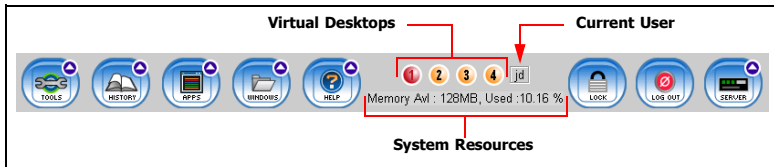










Figure 4: netForensics Taskbar

The icons and buttons on the taskbar are described below:

Icon	Name	Feature
	Tools	Provides access to the Secure Certificate Manager, Administration, Device List, and System Health Monitor console
	History	Provides single-click access to the last 20 reports visited
	Apps	Provides access to Forensics (reports), Event Console, Device Status, Device Map
	Windows	Provides tools for arranging windows and lets users jump quickly to another window in any virtual desktop
	Help	Provides further information about the SIM Desktop and general information about netForensics
	Lock	Locks the current desktop session and activates a screen saver
	Log Out	Closes the current user session
	Server	Shows the status of all connected netForensics servers

Virtual Desktops

The netForensics SIM Desktop provides four different workspaces, or virtual desktops, where users can view reports or run any of the other netForensics monitoring tools. The use of virtual desktops provides users with more options for viewing and organizing information. Each virtual desktop operates independently from all others, and any open window in a virtual desktop can be quickly accessed from the Window icon on the taskbar.

When the SIM Desktop is launched, virtual desktop 1 is displayed. To switch to a different virtual desktop, click its number on the taskbar. The number of the active (i.e., the one currently displayed) virtual desktop is highlighted in red.

Current User

The login ID of the current user is displayed in the taskbar next to the virtual desktop icons.

System Resources

The amount of available system memory and the percentage of that memory currently in use by the SIM Desktop are displayed on the taskbar, below the virtual desktop icons.

Logging Out

To log out of netForensics, click the **Log Out** button on the right side of the toolbar at the bottom of the SIM Desktop.



Figure 5: Log Out Button

