netForensics Version 3.1.1.01 Update Release Notes

Copyright

Conventions Used

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 ***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 requiring user input appear between brackets in a bold italic screen font: ***<file name>***
- The **Start > Run** option represents clicking the Start button on the Windows 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

Contents

Introduction

netForensics is a Security Information Management (SIM) application that works with a heterogeneous array of security products, allowing network managers to centrally monitor, manage and administer the security of a web enabled enterprise network.

An update to netForensics is available, version 3.1.1.01, which includes software enhancements and addresses some of the known issues in version 3.1.1. netForensics can be upgraded to version 3.1.1.01 by applying an update file. These release notes highlight the features of netForensics (v3.1.1.01) and instructions for applying the update.

System Requirements

The following minimum requirements in reference to the Java™ 2 Runtime Environment are required to launch and use the 3.1.1.01 netForensics SIM Desktop:

- JRE 1.4.2_01
- Java™ WebStart

Both are available at:

http://java.sun.com/products/archive/j2se/1.4.2_01/

Update Details

The details of the nF 3.1.1.01 migration update available from CCO (Cisco.com) (see Obtaining Technical Assistance on page 14), are described in the following table:

Update Number	3.1.1.01
Release Date	05/04/2004
File Name	nFSIM-3.1.1-SFTUPD-v01.tar.gz
Minimum Disk Space Required for Install	300MB
Supported Platforms	Red Hat Linux Advanced Server 2.1, Solaris 8

Prerequisites

Before the nF 3.1.1.01 update can be applied, netForensics 3.1.1 must be installed and running. The build number for nF 3.1.1 (found in **$NF_HOME/config/system/nf.manifest.system** on UNIX,) is **20031010101010**.

Minimum Disk Space Requirement

The minimum disk space requirements for installing netForensics 3.1.1.01 is 300MB.

Warning

Please make certain that there is sufficient disk space available prior to installing the 3.1.1.01 update, otherwise the update application may fail.

Installation

Follow the steps below to apply the update:

1. Download the update file (**nFSIM-3.1.1-SFTUPD-v01.tar.gz**) from CCO (Cisco.com), (see Obtaining Technical Assistance on page 14).
2. Log in to the nF Provider server as **nf**
3. Copy the update file to the following directory on the nF Provider:

   $NF_HOME/patches

Warning

The nF Provider and Oracle Database must be running when the update file is applied. **All other** netForensics components **should be stopped** individually (i.e., without using **nfservices stop**) before the update file is applied.

Important

Please make certain that this update file is the only "tar.gz" present in this directory.

4. Apply the update using the following command:

   ```
   $ $NF_HOME/bin/installpatch
   ```

   » A log file is created in **$NF_HOME/logs/patch**

Important

Please note that the update application process may take up to 30 minutes for a medium size database. The application process is dependent on the machine capacity and database size and therefore may take longer for larger databases or slower machines.

5. Stop and start the nF Provider, then restart all other nF components. .

Important

When starting a remote component following the installation of the update file, the component will take longer than normal to start since it has to download an update from the nF Provider.

For any nF Agents installed on Windows, start the "Agent" component before the "Data" component to ensure that updates from the nF Provider are properly downloaded.

Important

During patch application, some error messages may occur within the patch.log file such as:

```
'Failed to execute SQL Insert into DEVALARMCVEMAPPING_M'
```

Errors of this type can be ignored since they are not functional and are reported because the devicetype alarms have not been updated with all the signature updates.

During the update application process, if the nF Agent for Symantec HIDS is installed the following error message is reported:

```
"Failed to download patch
preinstall_SIDS/preinstall_SIDS_DB_01.tar.gz"
```

This error can be ignored since it does not cause any functional issues.

On some lower capacity machines, where the log processing cannot be done fast enough, errors may be encountered in relation to the log cache being full. These errors can be ignored since they do not cause any functional issues.

Post-Installation

Complete the following post-installation procedures as required.

Updating Sender Information

This script updates the Sender information and Domain information in the action scripts. All the action scripts have been updated as a result of the 3.1.1.01 software update.

Warning

This post-installation procedure is mandatory.

1. Execute the following command on all machines where the nF Engine is installed.

Important

The **sender_update.sh** script must be run as the 'nf' user.

```
sh $NF_HOME/utils/sender_update.sh
```

2. Provide the 'Email User' [i.e.., "nf"], and press Enter.
3. Provide the 'Domain address' [i.e.., "netForensics.com"], and press Enter.

New Features

This section provides information about the netForensics features and enhancements that have been included in this update.

Knowledge Base

Knowledge Base (KB) is a searchable and extendable collection of security resources provided in the form of a database. It includes industry knowledge collected by various security research institutions, netForensics security resources applicable to all users and customer-specific information collected by users.

In this release, Knowledge Base contains:

- CVE information from ICAT (CVE and candidates entries)
- nF Alarm Help
- Device Alarm Help and help from Security Device vendors
- Custom Alarm Help
- Alarm Operational Procedures
- Notes entered by a user and outside documents attached to User Notes
- CERT (advisories, vulnerability notes, guides)

Important

Device Alarm Help details are not shown for all device types. Device Alarm Help is only integrated with the following device types: Cisco Pix, Cisco VPN, Snort, Cisco IDS, Cisco IOS Firewall, Cisco IOS Access Control and Cisco IOS IDS.

Searching Knowledge Base Data

Comprehensive searching across all KB data using a literal string keyword search is provided for both normal and advanced searches. Knowledge Base is designed to return only search results that match the keyword text string completely.

The searching of user based data such as Alarm Procedures and User Notes utilizes date and time search criteria, whereas the searching of system related data such as "Device Alarm Help", does not.

Saving KB Preferences

User-based settings for the Knowledge Base main window, Alarm Help, Custom Alarm Help and Vulnerabilities can be saved using the **Save Preferences** function (found on the File Menu of each of the mentioned KB features). The **Save Preferences** function operates differently based on the KB module being used. This functionality per KB module is described below:

- Knowledge Base - saves the last criteria set for the search
- Custom Alarm - saves both the Tree Order and Device Type
- nF Alarm - saves both the Tree Order and Device Type
- Vulnerabilities - saves the Tree Order only

nF DashBoard

The nF DashBoard feature provides a centralized access point for a specific collection of reports and is launched via the "Taskbar" located on the SIM Desktop (**Apps>netForensics>nF DashBoard**).

The nF DashBoard provides nine different reports that can be viewed using Bar Chart, Pie Chart, or Report Table mode, in order to give a concise overview of what is happening within the system. These reports are also available in the Device Independent View of the Forensics Menu. (See "New Reports" on page 10.)

The nF DashBoard's view can be refreshed dynamically. A print function is also provided that enables the report data displayed within the nF DashBoard to be output to a printer.

Multi Threaded Agent

Parallel processing of messages and parsing is now provided via the Multi Thread feature at the agent level. As a result, there is substantial improvement in the number of messages processed which results in vastly increased performance if more than one processor is included in the agent hardware.

The parallel processing at the agent level is configurable via **Parser Pool Size** field located in the Boot Configuration for each agent.

Guidelines for Using the Multi Thread Agent Feature

When the number of threads for a particular agent is increased, the memory requirements for this agent will also increase requiring a manual change to the **nFLaunchers.xml** file (See "Modifying the nFLaunchers.xml file" below for more information).

The general rule for setting this parameter is 10MB plus two times the number of threads. Using this rule, the suggested minimum memory settings are shown based on the number of threads being used:

Number of Threads	Allotted Memory (in MB)
1	10
2	14
4	18
8	26

Modifying the nFLaunchers.xml file

Follow the steps below to modify the multi thread related memory settings for an agent using the multi thread feature:

1. Using a text editor, open the **nFLaunchers.xml** file located in the following directory on the agent machine:

   $NF_HOME/config/system

2. Locate the section of the file that corresponds to the agent you are using.

   The section containing the variable to be modified can be located by performing a search using the name of the agent, in association with the "serviceName" field. Once this section is located, modification of the "-Xmx" variable (discussed in the following step) must be done within the section where the Command name field is equal to "Agent".

3. Modify the number within the following parameter to adjust the allocated memory for the agent:

   ```
   -Xmx10m
   ```

   For example, increasing the default setting to 14 MB would be set as follows:

   ```
   -Xmx14m
   ```

4. Save the edits to the file and start, or restart the agent.

Admin UI Enhancements

Operational Procedure Management

The options under Operational Procedure Management (***Admin options>Alarm Management***) provide a means by which to create procedures based on Alarm Type, in conjunction with:

- nF Alarms associated with an nF Category
- Device Alarms associated with a Device Type
- Custom Alarms associated with a Custom Category

Alarm procedures include a set of predefined actions that are created and maintained via the Procedure Configuration window. The Procedure List window is also provided which displays a "view only" listing of existing alarm procedures.

Alarm procedures associated with both Alarm Details Help and Device Details Help can be accessed when viewing netForensics data by:

- right-clicking result data under the nF Alarm and Device Alarm columns in generated reports and the Event Console. Additional information is supplied along with the details help including any Knowledge Base Users Notes that may have been created for the selected alarm.
- launching Alarm Details Help within Knowledge Base.

Severity Levels Enhancement

Severity Levels have been enhanced to allow for a more granular scale when setting this feature. Levels one through five are now available to provide better filtering. In general, severity levels 4 and 5 should be selected when filtering for High Severity, while Severity Levels 1, 2 and 3 should be selected when filtering for Low Severity.

This enhancement affects Event Console filters as well as severity levels associated with Report Groups and Report Options.

User Note Space

A new field that determines the size in Megabytes (MB) for the amount of data allowed to be entered into the "MyNotes" Knowledge Base related screen has been added to the **User Accounts** window (***User Options > User Management***) of the Admin UI.

IDS Device Group

A new device group called "IDS Device Group" has been added. Any device instances of type IDS (i.e., Cisco Secure PIX, Cisco Secure IDS, Dragon, Snort, ISS, etc.) will automatically be mapped to this group at the time of creation. All existing device instances of type IDS are automatically mapped to this group when the netForensics 3.1.1.01 update is applied. This system device group does not allow users to use this group or modify any mappings for the devices belonging to the group.

Asset Management

A new window has been added to Asset Management that provides a view of an enterprise's assets entitled **Asset View**. The Asset View window provides searches based on IP Address, operating system and/or networks.

Event Filters Management

Event Filters has been enhanced with the ability to set filters for specific servers using both Component Type and Component Name fields.

The location of the Event Filters Management administrative windows (including Destination Configuration, which was located under Component Options > Engine) is now under ***Component Options>Event Flow Management*** of the Admin UI.

Administration of event filters is accomplished by using the Add, Edit, and Delete functions provided. An event filter view is also provided.

Important

When adding event filters in multi-engine installations, users are prompted to save the updated information as many times as there are installed engines.

Intruder Management

The User Intruder concept has been added to aid in the tracking of users defined as intruders. When a user name is present in any of the above modules and that user is defined as an intruder, the User Intruder name is displayed along side the User Name as shown below:

```
User1 (I:Intruder Name)
```

The following areas are affected by the User Intruder modification:

- Reports
- Administration

To support the new User Intruder concept, a new window "User Intruders" (***Admin Options>Intruder Management***) has been created that allows users to be defined as an intruder and then be associated with an Intruder Group. To differentiate the new User Intruder concept, the original Intruder window which defines IP addresses as intruders has been renamed to "IP Intruder".

Enhanced Security for nF

A new field "Service Mode" has been added to the nF Provider Boot Configuration which sets the overall security level for netForensics. The available settings for netForensics security and their descriptions are as follows:

Service Mode	Description of Security Level
Partially Secure	Secures critical services only. This is the default setting for this feature.
Secure	Configures all Provider services to be secure except the installation and patch management related services. Please note that there is a performance impact when using this setting.
Non Secure	All services are not secure. This setting was the previous security level set for netForensics.

Important

When changing Service Modes, all netForensics components must be restarted including the nF Provider, all server components and the SIM Desktop.

SIM Desktop Enhancements

The following enhancements have been made for this release:

Desktop Icons

The following icons have been added to the SIM Desktop:

- **Knowledge Base** - Launches the netForensics Knowledge Base used to access Vulnerability, Resources, Alarm help, Custom Alarm help and User Notes.
- **My Notes** - Launches the My Notes (Knowledge Base related feature) used to create security related information associated with various types of Knowledge Base data.

Taskbar Enhancement

The netForensics Taskbar has been enhanced to provide access to both the nF DashBoard and Knowledge Base feature.

Save Session and Knowledge Base

Saving session information from the SIM Desktop enables each application running in each virtual desktop to be relaunched upon the subsequent session. Saving session preferences from the SIM Desktop now encompasses the Knowledge Base feature. The Session function is located at the right side of the SIM Desktop Taskbar. To save current session information, select the **Session** button , then click **OK** to confirm the save operation. Please refer to the *netForensics User Guide* for more information on using this feature.

Drop Down List Sorting

All drop down lists where ever there is potential for large number of entries are sorted (Admin, Event Query, Event Console). All nFAlarm drop downs are sorted by nFCategory and nF Alarm Description. All nF Severity displays are sorted by severity level with the most critical (5) being displayed first at the top of the list.

Event Query Enhancements

Support for Asset, Intruder, Asset Group, Intruder Group, and Source User Name in Event Query has been added. The Event Query inputs are changed to accept Asset, IP Intruder, User Intruder, Asset Group, and Intruder Group by providing a list of these values from master data.

Support for Port Ranges and Individual Numbers to Event Query

These logic based changes are effective for all integer fields of Event Query Inputs. (i.e. Source Port, Destination Port, Device Severity).

1. To input a single value, specify a number.
2. To input a range, specify it as "beginning of range – end of range".

   Examples:

   a. 20 – 30 to select between 20 and 30.
   b. –20 to select 20 or less than 20.
   c. 30- to select 30 or greater than 30.

Event Console Enhancements

Support for Source User Name, Source MAC Address, Destination MAC Address, Type and Device Group has been added for Event Console. To include data associated with any of these columns within the Event Console's display, click the Customize button in the top right corner of the Event Console window.

For additional Event Console enhancements see the following topics

- "Operational Procedure Management" on page 6
- "Severity Levels Enhancement" on page 7

Report Enhancements

The following enhancements have been made to the Report module:

Report Performance Improvements

The netForensics report framework has been modified to enhance the report performance by using more optimized and efficient queries.

Report Scheduler

The Report Scheduler screen (***Report Scheduling>Manage Report Schedule***) now has an additional field titled, "Email from" that allows reports to be mailed displaying a user defined sender email address.

Additional Report Improvements

Other enhancements made for this release include:

- Allowing users to select the severity for the reports.
- Adding a new section in the Drilldown screen to show the context that will be carried over for the Drilldown reports. The user can select/deselect the context fields.
- "Summarized by" in Report Options now shows all the possible breakdown periods instead of only two.

New Reports

The following new reports have been added to the Device Independent View tab of the netForensics reporting subsystem.

The following reports have been added under Security>Network Category:

1. Activity Targets by Business Unit
2. Activity Originators by Business Unit
3. Selective Activity Summary by Business Unit
4. Selective Activity by Business Unit

The following Drilldown reports are associated with the "Activity Targets by Business Unit" report:

1. Activity Networks by Business Unit
2. Affected Hosts

The following Drilldown reports are associated with the "Activity Originators by Business Unit" report:

1. Originating Networks by Business Unit
2. Originating Hosts

The following nF DashBoard related reports have been added under "Dashboard Reports":

1. Risk Score
2. Threat Score
3. Event Summary
4. Top Attacking Sources
5. Top Attacking Destinations

6. Top nF Alarms
7. nF Severity Summary
8. nF Category Summary
9. Top Device Alarms

Event Schema Changes

The database table schema has been modified for the "highseverityevents" and "lowseverityevents" tables to support feature enhancements. As a result, the **event.xml** has been changed, which in turn has created changes in the action scripts. In addition, the archive and restore procedures have been modified to support the schema changes.

Migrating Archived Data Files

Archived data files generated in 3.1.1 need to be migrated with schema changes when restore is necessary after the nF 3.1.1.01 update is applied.

Important

This archive data file migration procedure is only required for systems that are utilizing restore capabilities in reference to 3.1.1 archived data.

The script **nFArchivedFilesMigration.sh** (for the Unix platform), and **nFArchivedFilesMigration.bat** (for the Windows platform) are designed to update the nF database schema to handle changes in the low/high severity events table. The nF 3.1.1.01 patch places the platform specific migration script in the following directory:

UNIX:

```
$NF_HOME/archives/nFArchivedFilesMigration.sh
```

Windows:

```
%NF_HOME%\archives\nFArchivedFilesMigration.bat
```

To update archived data files execute the following command on the nF Provider machine:

UNIX:

```
sh nFArchivedFilesMigration.sh <path location of 3.1.1 archived data files>
```

For example

```
sh nFArchivedFilesMigration.sh /home/nf/archives
```

Windows:

```
nFArchivedFilesMigration.bat <path location of 3.1.1 archived data files>
```

For example:

```
nFArchivedFilesMigration.bat C:\home\nf\archives
```

Issues Fixed

The following issues have been fixed in the netForensics 3.1.1.01 release:

1. The Logout Time displayed in the User Login-Logout Activity Report is earlier than the login time. (CSCea52146)
2. Cold backup reports "Space not available" on destination directory when destination is an NFS mounted file system. (CSCsa20749)
3. Reports fail when run through the Report Scheduler for report names that include a slash '/' because the report scheduler interpret the slash as a directory separator. (CSCsa20751)
4. User gets SQL Exception error when attempting to setup event notification for some CSIDS alarms. (CSCsa20752)
5. The Source and Destination IP addresses are showing up as PIX firewall IPs for PIX alarms 305012 and 106023. (CSCsa20753)
6. Contents of the nFAlarms description is showing up in two cells within the Most Frequent Events report. (CSCsa20755)
7. System Health Monitor Report runs slow. (CSCsa20757)
8. nFSeverity Override by Device window's Device field, does not show all devices preventing the override of alarms for hidden devices. (CSCsa20758)
9. Purge jobs are slow and occupy large table space. (CSCsa20759)
10. Cannot set the Report Period (on the Report Options tab) if exported directly without generating report first. Defaults to last 10 minutes period. (CSCsa20762)
11. When multiple Event Consoles are running and the desktop session is saved and the session is brought back, all the Event Consoles are launched with the same filter as the last saved preferences. The individual filters are not remembered across the sessions in spite of saving the session. Not all event consoles are re-launched after the save session. (CSCsa20761)
12. Lack of support for Context buffer information for IDS Version 4 sensors. (CSCsa20763)
13. Signature updates fail if a custom alarm has already been added in netForensics due to Signature Update being present in Signature Management is there in signature updates. (CSCsa20764)
14. Event Console time not in sync with message time. (CSCsa20765)
15. nF Provider hangs when the number of notification threads increase. (CSCsa20766)
16. The nF Syslog File Agent Java lists the time in 12 hour format in the syslog datasource file. (CSCsa20767)
17. Incorrect parsing of VPN messages. (CSCsa20769)
18. Line Charts summarized by hour fails. (CSCsa20770)
19. When multiple firewalls send messages to the same Syslog File agent, firewall messages are mapped to the incorrect Firewall IP. (CSCsa20771)

Known Issues

This section lists known issues in the netForensics 3.1.1.01 release.

1. Distributed webserver installation where the webserver is remote to the nF provider displays a fatal error at installation:

   "`Failed to create pre-install archive for patch 3.1.1.01 in file 3.1.1.01_FW_01.tar.gz. Failed to apply patch 3.1.1.01 component patch 3.1.1.01_FW_01. nfweb started`".

   This is a false messages that only appears when the Webserver is remote to the provider. This message can be ignored since this behavior is not related to any functional problems. (35534)

2. Names assigned to user notes via the My Notes feature allows for the duplication of the text string. Each unique note is then displayed with the duplicate name within the Knowledge Base User Note window. (35369)

3. Any attached text file within Knowledge Base when launched within the browser will not format properly. (34525)

4. The following nF Agent for Tripwire reports do not show correct data due to missing the appropriate SQL action check. (36939)

   - Unique Reports>Files Added
   - Unique Reports>Files Remove
   - Unique Reports>Files Modified

5. Cisco - Vendor Summary - Shows Device Types twice. (36961)

6. Any period selected in Forensics will be changed after the nF DashBoard report refreshes to 'Last One Hour'. (36875)

7. When creating report groups through Report Scheduler, if no severity is selected, the group is not saved on selection of the Save button. No pop up error message is seen. (36852)

8. Asset as Destination Drilldown is showing data for destinations other than the ones in Assets. (36784)

9. When you create a filter through Event Filter Management and then add an additional filter, the screen does not refresh automatically when attempting to edit the filter. Also, if you add two filters one "Forward" and the other "Block", and then delete the Forward filter, it gets deleted but the filter set to Block becomes Forward. (36614)

   Work Around: Relaunch the screen.

10. Two remote components on the same box are unable to start at the same time. Locking keeps the late starting component from starting the download. (36160)

    Work Around: Restart the component that failed to start.

11. Users (with Admin privileges) mapped to nF Super User group do not see Knowledge Base on the SIM Desktop until a save operation is performed. (35600)

    Work Around: Perform a save for that user via the User Account window in the Admin UI (**User Options>User Management**) in order for Knowledge Base to become available from the SIM Desktop.

12. The Resources link under Knowledge Base for providing Security Device Vendor help connects to the Provider and this may require the Provider port 9000 to be open. If this port cannot be opened up, then the Security Device Vendor Help will show an error "Page cannot be displayed". (36197)

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) Website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Cisco TAC Website

You can use the Cisco TAC website to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/en/US/support/index.html

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.