



## NetIntercept 4.0 Quick Start

### Hardware Requirements

- Appropriate climate-controlled (78°F/25°C) space for the system: 2U of 19" rack space to a depth of 26 inches (the 3TB system uses 3U of rack space).
- Alternating current electrical power (110V 60 cycle 15 Amp grounded outlet for machines shipped to North American destinations). Although not required, a surge protector, or better yet an Uninterruptible Power Supply, is strongly recommended.
- 10/100/1000 Base-T copper Ethernet connection to the network hub or switch "span" port that is to be monitored. See Chapter 3 of the *NetIntercept User Manual* for recommended monitoring topologies.
- PC peripherals for initial setup and test (connected to the NetIntercept system directly or via a KVM switch): VGA-compatible video monitor, PC-type 102-key keyboard with PS-2 compatible connector, and 2- or 3-button mouse with PS-2 compatible connector.
- If you will be working with captured audio files from the NetIntercept console, you will need to obtain a USB sound adapter and speakers to allow audio playback.
- If the NetIntercept system will be remotely accessed via the control port, you will also need to provide:
  - 10/100/1000 Base-T copper Ethernet connection for the control port. See Chapter 3 of the *NetIntercept User Manual* for recommended security considerations.
  - Remote client system with software, configuration and network access to allow it to connect to the NetIntercept system, including: Secure Shell (ssh) version 2 configured to allow X11 port forwarding, and X Window System server software configured to accept connections via SSH port forwarding. See Sandstorm's web site for a list of tested SSH clients and X Window System servers.

### Before You Begin

- Ensure that the hardware requirements listed above have been provided.
- Decide on a location for the NetIntercept machine on your network. Chapter 3 of the *NetIntercept User Manual* contains further information on recommended monitoring topologies.
- Devise secure passwords for the three accounts on the machine: **root**, **ni**, and **niadmin**.
- (*If you will be using NetIntercept remotely*) Obtain the correct network address information (hostname, IP address, router IP address, subnet mask, and domain name) for the NetIntercept system's control interface. Alternatively, ensure that there is an available DHCP server which will provide the necessary configuration. You may also provide a DNS server IP address and NTP Time Server IP address for the control interface, but these items are optional.

### Attaching Cables and Peripherals

- Attach the hardware license management device (KeyLok) to the USB or parallel port.
- Attach network cables – one for the monitored network (labeled "CAPTURE"), and one for the control network (if you will be running the machine remotely).
- (*For DR1510 and DR3010 systems*) These systems have numbered hot-swappable hard drives, which are packaged separately. Please insert each drive into the front of the machine in the corresponding numbered slot. Properly seated drives are flush with the front of the machine, allowing the front panel to be closed easily.
- Attach all other peripherals and plug the machine in. The NetIntercept software is pre-installed on the machine in the `/usr/ni` directory.



## Configuring NetIntercept

**Note:** For the initial configuration process, you must attach a monitor, keyboard, and mouse to the system, even if you will be running the machine remotely.

- Turn on the machine. It will boot and display an X Window System login prompt.
- Press [**Ctrl+Alt+F2**] to access a console login prompt, and log in as **root** (no password needed).
- Run the NetIntercept configuration script ( **/root/modrconf.sh** ). You will be prompted to enter:
  - (if you will be accessing the machine remotely via a static IP address) the hostname, IP address, gateway, name server, subnet mask, and domain name for the control network interface
  - which interface to use as the control network,
  - (optional) the NTP time server for the control network interface,
  - (optional) SNMP configuration information for SNMP v3 (and optionally for SNMP v1 & v2c as well),
  - your organization's name,
  - whether or not to regenerate NetIntercept's private-key encryption key,
  - timezone information (initially configured to Greenwich Mean Time),
  - new passwords for the three accounts on the machine.
- After running the script, reboot the machine using the **shutdown -r now** command.
- If you will only be accessing the machine remotely (*i.e.*, over the network) confirm that remote access works. Then remove the monitor, keyboard, and mouse from the machine, if desired.

## Logging In and Using NetIntercept

Wait for the machine to finish rebooting (if you have configured NetIntercept according to the instructions above). Upon restart, NetIntercept will detect a monitoring interface and begin capturing network traffic. An X Window System login prompt should display. Log in as user **ni** (lowercase), using the password you chose during configuration. The NetIntercept user interface will start automatically. The Traffic tab in the user interface should display a graph of captured traffic.

**Getting help:** The user manual is available via the user interface, by pressing the [**F1**] key or choosing *Help...* from the *Help* menu. Optional configuration information can be found in Chapter 3 of the manual. Release Notes for the current release are in the **/usr/ni/docs** directory on the NetIntercept machine. Technical support contact numbers and links to NetIntercept support information are available at <http://sandstorm.net/support/>.

## Building a Database

We strongly recommend that you create a test database using captured traffic after installing NetIntercept to familiarize yourself with the way it analyzes your data.

Many of NetIntercept's user interface elements have online help. Press the *What's this?* button on the toolbar, then click on a part of the interface, such as a column, button, or tab, to pop up a short description of that element.

1. **Sweep traffic.** From the user interface, choose the Traffic tab. Highlight a time range on the graph of captured traffic by clicking and dragging the mouse across the graph. Note that the number of packets and bytes in the selection is displayed at the top of the tab. For your first database, we recommend selecting 1GB or less of traffic.
2. **Create a database.** Once a highlighted area appears on the graph, press the *New* button on the toolbar at the bottom of the Traffic tab. When prompted, enter a database name (or accept the default), and press *OK*. NI will parse the traffic and create a database. Depending on the amount of traffic chosen, this process can take anywhere from a few seconds to an hour or more.
3. **Explore the data.** Once NI has created and loaded the new database, the remainder of the interface can be used to explore the data. We recommend the Summary tab (to view overall database information), the Views tab (to view host information, captured images and web pages), and the Forensics tab (to search the database).

### Contact us at:

Sandstorm Enterprises, Inc.  
14 Summer Street • Malden, MA 02148-3986  
P: +1 781-333-3200 • F: +1 270-964-0394 • E: [sales@sandstorm.net](mailto:sales@sandstorm.net)