Network Navigator™

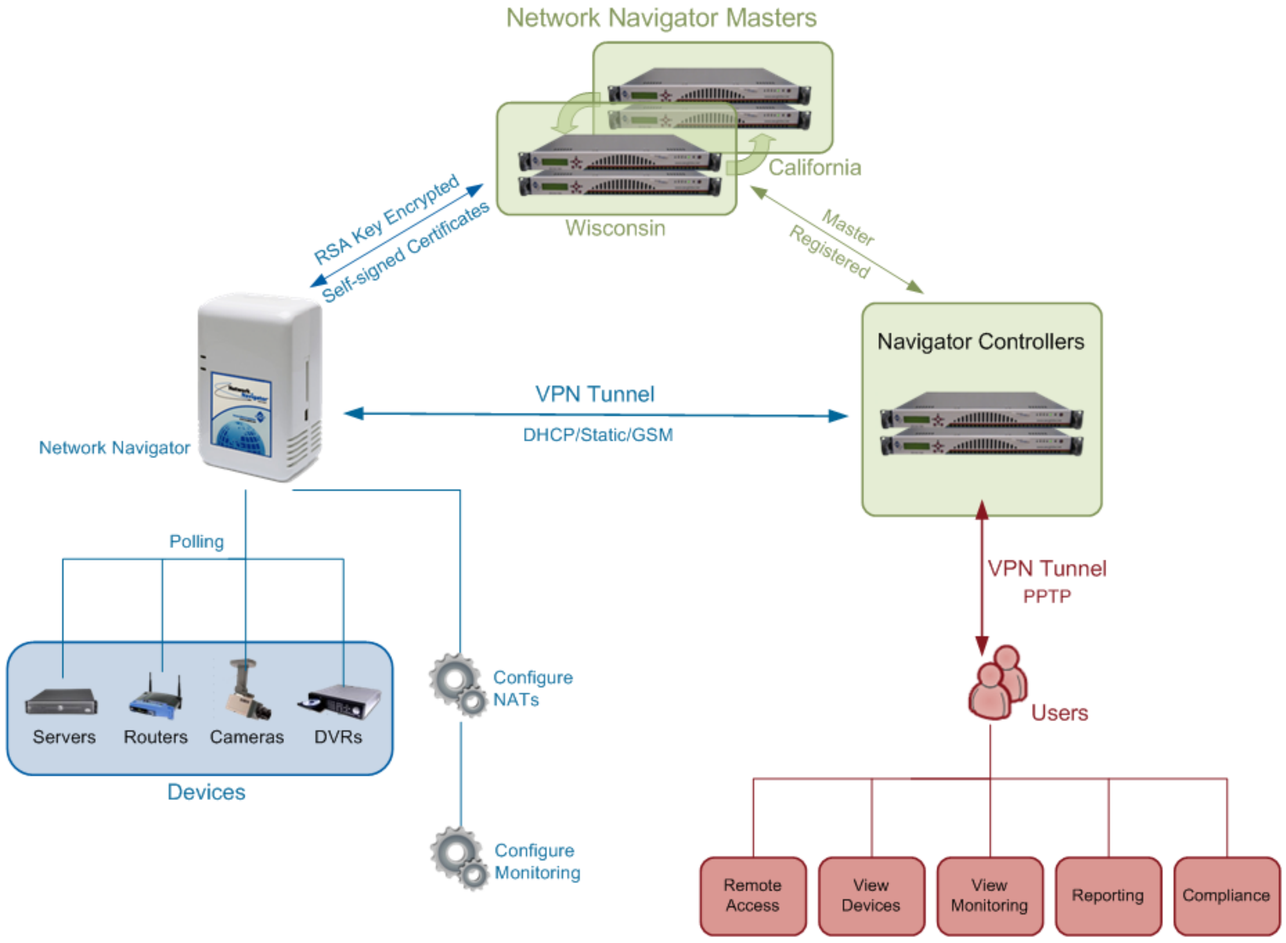
Administration Guide

Document Version 2.0.0
October, 2016
Secure Global Solutions, LLC

Table of Contents

Network Navigator Topology

This map illustrates the connectivity between Network Navigators, Navigator Controllers, Masters, and Users.



Navigator Controller Administration Guide contains information on installing and configuring a Navigator Controller.

Network Navigator Administration Guide contains information on configuring Navigators and Monitoring.

Network Navigator End-User Guide contains instructions on using the Monitoring, Reporting, and Remote Access functions.

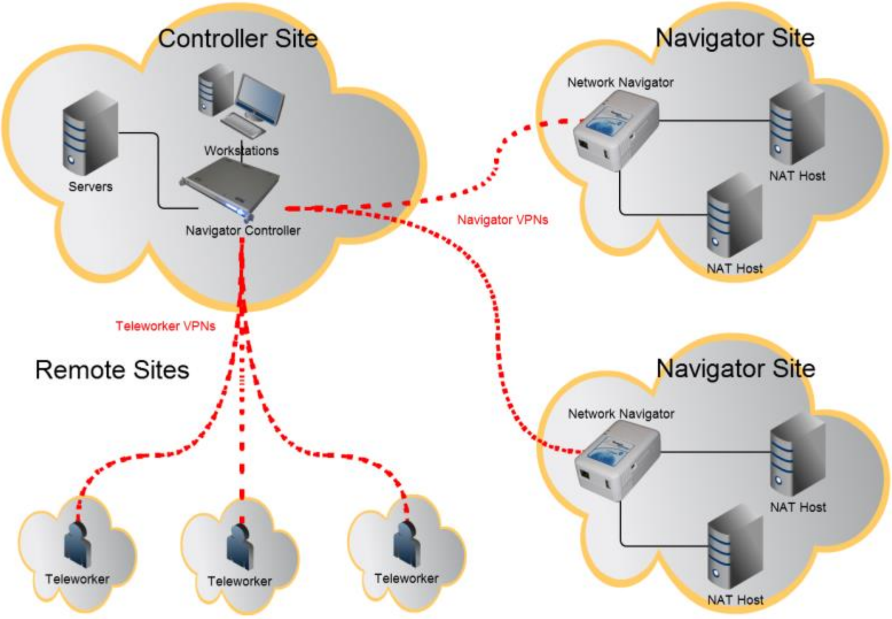
Introduction to Network Navigators

Many business processes require data communication between systems at distributed sites. A connectivity solution is required to provide access to these resources. In many cases, site-to-site VPN tunnels fulfill this role.

The Network Navigator simplifies VPN tunnel creation by eliminating the need for collaboration and advance planning between network administrators at various sites.

Network Navigators

The SGS Network Navigator ("Navigator") is a self-configuring VPN client device. Each Network Navigator is the child of a specific Navigator Controller.



Deployed on a site's internal network ("Navigator Site"), a Navigator will phone home to its Navigator Controller and establish a VPN tunnel. By default, Network Navigators request network configuration via DHCP. Static addressing is also possible.

The Network Navigator platform has been designed to eliminate or minimize routing and firewall administration at Navigator Sites. In most cases, a technician simply plugs the Navigator in. No further administration is required.

Virtually all setup and configuration tasks are completed on the Navigator Controller. This document discusses the tasks relevant to configuring an individual Navigator.

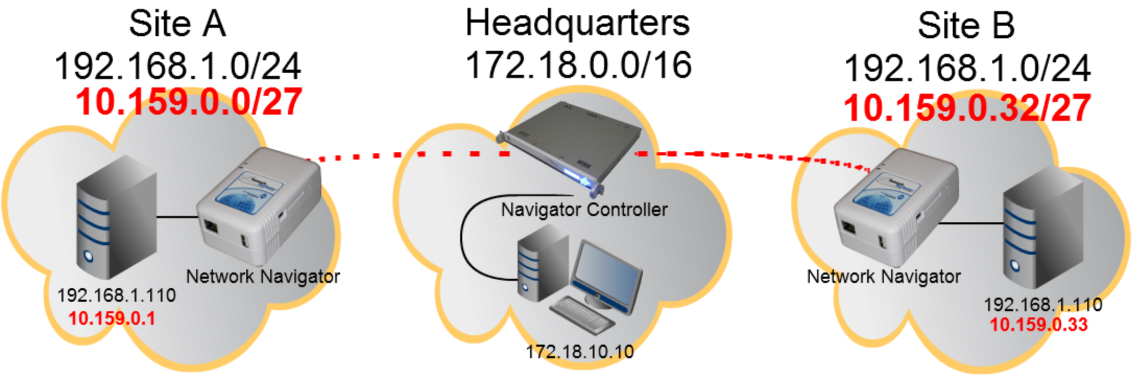
Navigator Self-Configuration

When booted, the Network Navigator automatically downloads configuration information and establishes a VPN tunnel back to its parent Navigator Controller.

This process has been designed to work automatically in most cases, without intervention from personnel at the Navigator Site.

NAT Addresses

Network Navigators allow VPN users an experience similar to a star topology of site-to-site VPNs, without forcing network administrators at Navigator Sites to modify existing network architecture. Consider this topology:



To eliminate routing problems caused by duplicate IP addresses, the Network Navigator assigns unique virtual addresses to specific devices within sites A and B. Each Network Navigator acts as a NAT firewall, translating this traffic onto the LANs within their respective Navigator Sites.

NAT Subnet Sizes

The Navigator Controller administers a large private IP subnet reserved for NAT assignments through Navigators.

From that large subnet, each Navigator is assigned a small pool of addresses. Addresses from these pools are then assigned to specific devices within the Navigator Site.

NAT pools are available in three sizes:

- 30 NAT Addresses (/27 subnet)
- 62 NAT Addresses (/26 subnet)
- 126 NAT Addresses (/25 subnet)

Navigator Installation

Unbox the Network Navigator.

Connect the Navigator to your network,
using the included Ethernet patch cable.

Connect the Navigator to electrical power.

Wait 1-2 minutes while the Navigator boots.
When connected, the green LED is solid
and the blue LED displays a heartbeat pattern.

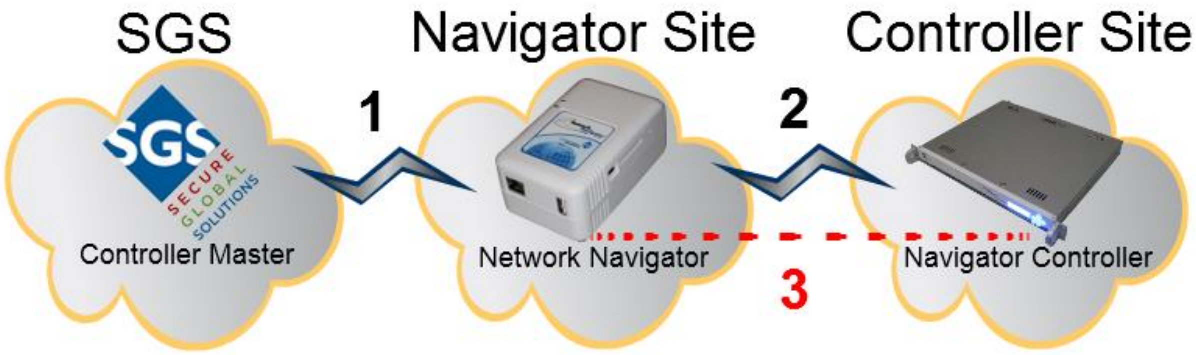
If the default DHCP configuration is desired, no further action is required. If a static IP is required, configure the device’s network settings using the Navigator Controller web-based management interface or using the included USB-to-serial console cable. Refer to the following sections of this document for additional information.

Outbound Access at Navigator Sites

The Navigator produces outbound traffic to the Internet to accomplish auto-configuration and tunnel establishment. All of this traffic uses destination TCP Port 443 (the Well Known Port reserved for HTTPS protocol). In most cases, firewall administration is not needed at the Navigator Site to allow this traffic.

Navigator Phone-Home Sequence

After a Network Navigator boots and connects to its Site's LAN (via DHCP or static addressing), it uses a phone-home sequence to establish a VPN tunnel to its Navigator Controller across the Internet. This sequence involves three steps:



First, the Navigator initiates an outbound HTTPS connection to an SGS Controller Master (1). It identifies itself and retrieves its NavCon's Public Management IP or FQDN.

Second, the Navigator initiates an outbound HTTPS connection to its Navigator Controller (2). It identifies itself and retrieves the NavCon's Public Tunnel IP or FQDN. It also retrieves tunnel establishment credentials and NAT configuration.

Third, the Navigator initiates an outbound OpenVPN to its parent NavCon's Public Tunnel IP or FQDN (3). It then creates local NAT firewall configuration.

Note If outbound access is not established, use these settings to configure the firewall:
Policy Outbound Allow Rule

SRC:	NavCon_Internal_IP
DST:	64.132.91.224/27 (SGS NOC) 98.189.69.224/28 (SGS Headquarters)
SVC:	80/tcp, 443/tcp, 10325/tcp
ACTION:	PERMIT

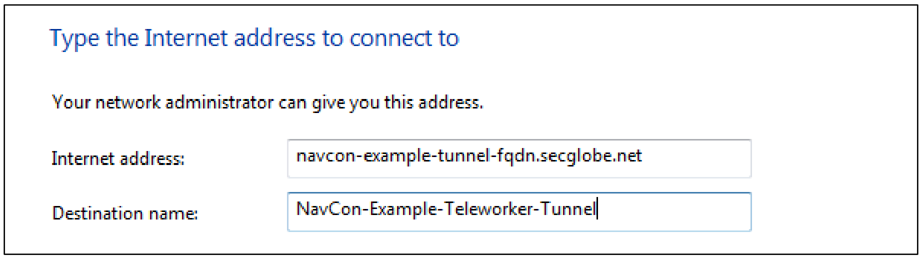
Connecting a Work Station to the NavCon

If you are working from a network external to the Navigator Controller site, you will need to establish a VPN connection to the Navigator Controller. The procedure shown here will connect a Windows 7 workstation to a Navigator Controller.

The procedure on other operating systems is similar. Consult OS documentation if necessary. The connection protocol is "PPTP with GRE". This protocol is supported by most common operating systems, including Windows, OS X, and Linux.

1. Open **Start** ▶ **Control Panel** ▶ **Network and Sharing Center**: Select **Set up a new connection or network**.
2. Under **Choose a connection option,** select **Connect to a workplace**.
3. When asked **Do you want to use a connection that you already have?** Select **No, create a new connection**. Click **Next**.
4. When asked **How do you want to connect?** Select **Use my Internet connection (VPN)**.
5. When prompted to **Type the Internet address to connect to, Complete the form as follows:**
    - **Internet address:** The NavCon Administrator provides this.
    - **Destination name:** Descriptive text as appropriate.

    Click Next.



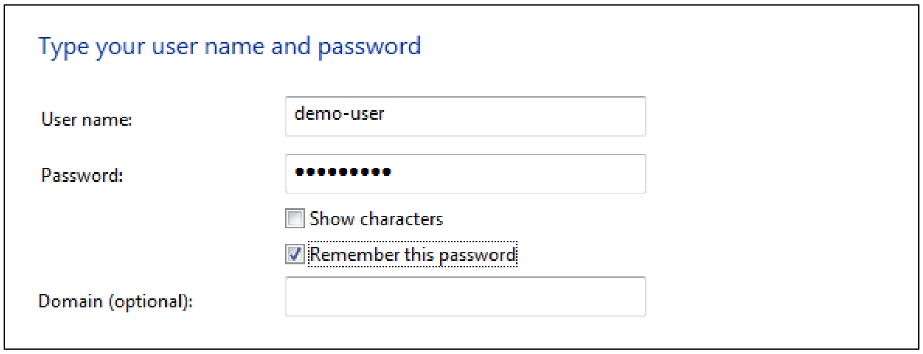
Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: navcon-example-tunnel-fqdn.secglobe.net

Destination name: NavCon-Example-Teleworker-Tunnel

6. Under **Type your user name and password**, complete the fields using credentials specified on the Navigator Controller in the **Configuration** ▶ **Users** view. Click **Connect**.



Type your user name and password

User name: demo-user

Password: •••••••••

□ Show characters

☑ Remember this password

Domain (optional):

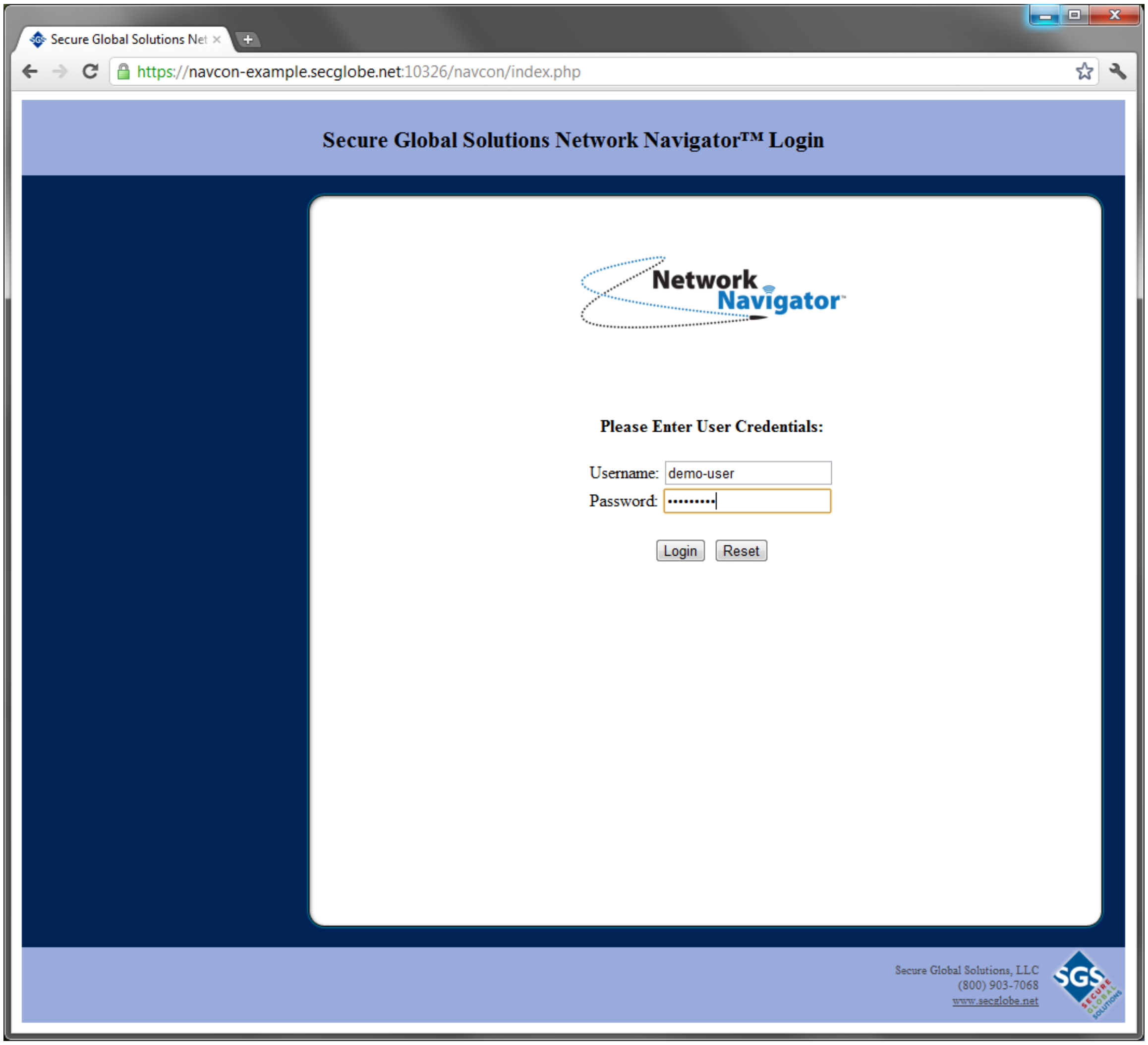
When the window displays **You are connected**, click **Close.**

Web-Based Management Interface

To administer the Navigator Controller, connect to its web interface using the internal IP or internal DNS alias as appropriate. For example:

```
https://navcon-example.secglobe.net:10326/navcon/index.php
```

> *Note* It is necessary to specify port 10326 in the URL. The built-in web server listens only on port 10326.



https://navcon-example.secglobe.net:10326/navcon/index.php

Secure Global Solutions Network Navigator™ Login

Please Enter User Credentials:

Username: demo-user

Password: •••••••••

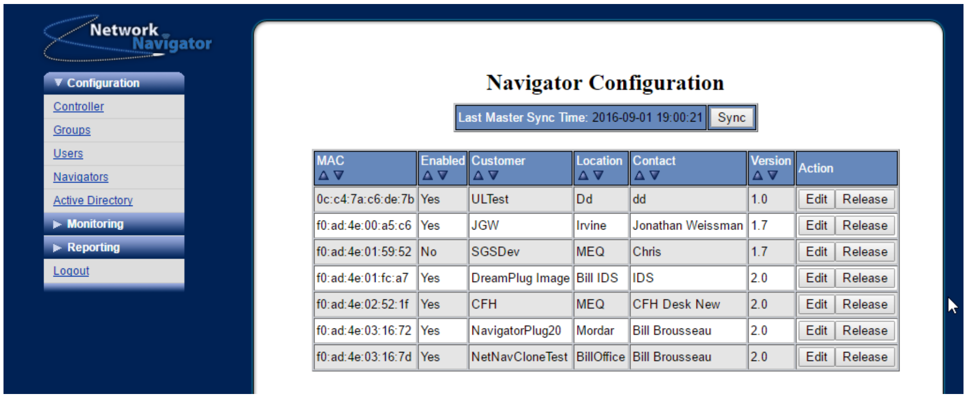
Secure Global Solutions, LLC
(800) 903-7068
www.secglobe.net

SGS provides the username and password to the systems administrator.

Navigator Configuration

Configuration ▶ Navigators

After syncing to the Controller Master, the NavCon lists all of its Navigators:



Navigator Configuration

Last Master Sync Time: 2016-09-01 19:00:21 Sync

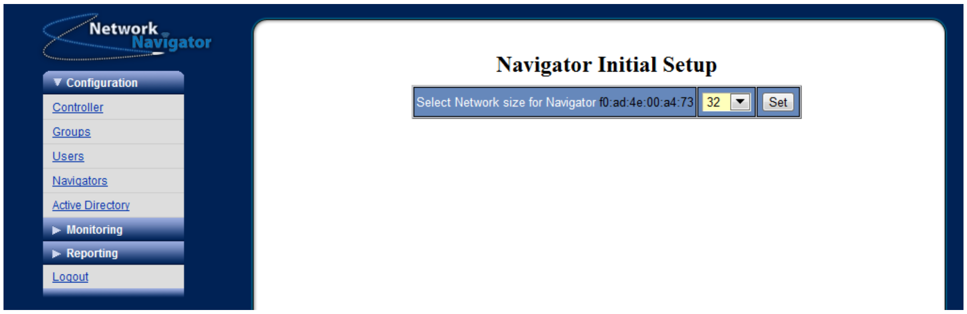
MAC	Enabled	Customer	Location	Contact	Version	Action
0c:c4:7a:c6:de:7b	Yes	ULTest	Dd	dd	1.0	Edit Release
f0:ad:4e:00:a5:c6	Yes	JGW	Irvine	Jonathan Weissman	1.7	Edit Release
f0:ad:4e:01:59:52	No	SGSDev	MEQ	Chris	1.7	Edit Release
f0:ad:4e:01:fc:a7	Yes	DreamPlug Image	Bill IDS	IDS	2.0	Edit Release
f0:ad:4e:02:52:1f	Yes	CFH	MEQ	CFH Desk New	2.0	Edit Release
f0:ad:4e:03:16:72	Yes	NavigatorPlug20	Mordar	Bill Brousseau	2.0	Edit Release
f0:ad:4e:03:16:7d	Yes	NetNavCloneTest	BillOffice	Bill Brousseau	2.0	Edit Release

Choose a Navigator to be configured. Click **Edit**.

- If this Navigator has not yet been configured, proceed to the **Navigator Initial Configuration** step.
- If this Navigator has already been configured, proceed to the **Navigator Edit** step.

Navigator Initial Configuration

On this view, choose the subnet size for this Navigator’s NAT Pool:



Navigator Initial Setup

Select Network size for Navigator f0:ad:4e:00:a4:73 32 Set

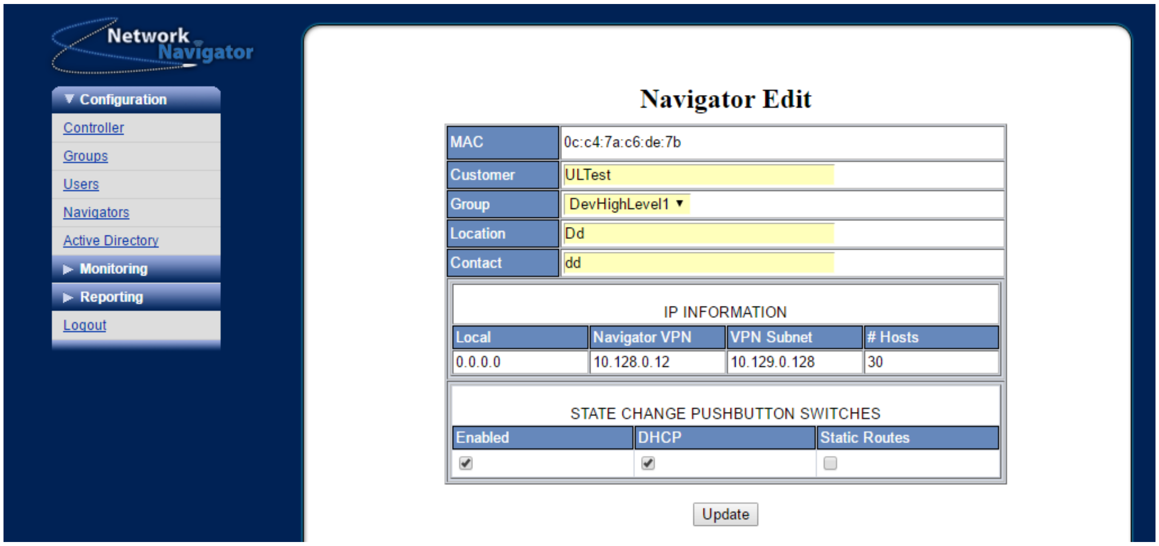
Three NAT Pool sizes are available:

- 32 – a /27 subnet with 30 assignable NAT Addresses
- 64 – a /26 subnet with 62 assignable NAT Addresses
- 128 – a /25 subnet with 126 assignable NAT Addresses

> *Note* **Choose carefully.** It is possible to release a Navigator’s NAT pool and assign a new one. However, this operation irretrievably purges all NAT Device configuration, and also causes a new set of NAT IPs to be assigned. Releasing a Navigator’s NAT Pool is discussed later in this section.

Navigator Edit – Configuration Table

Configuration for the Navigator is defined on this view.



Navigator Edit

MAC	0c:c4:7a:c6:de:7b
Customer	ULTest
Group	DevHighLevel1 ▾
Location	Dd
Contact	dd

IP INFORMATION

Local	Navigator VPN	VPN Subnet	# Hosts
0.0.0.0	10.128.0.12	10.129.0.128	30

STATE CHANGE PUSHBUTTON SWITCHES

Enabled	DHCP	Static Routes
☑	☑	□

Complete the table as discussed here. Click **Update** when finished.

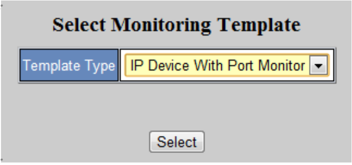
Field Name and Description	Field Value
MAC The hardware address of the Navigator's Ethernet interface	*Not configurable.*
Enabled Determines whether the Navigator is permitted to establish a VPN tunnel.	*Set or unset as appropriate.*
Customer A sortable text field on the **Navigator Configuration** view.	*Define as appropriate.*
Group A group name as defined on the **Configuration ▶ Groups** view. Groups are associated with teleworker user accounts.	*Choose from pull-down.*
Location A sortable text field on the **Navigator Configuration** view.	*Geographic location, site name, or physical location in site, as appropriate.*

Field Name and Description	Field Value
Contact A sortable text field on the **Navigator Configuration** view.	*Name, email, and/or telephone of responsible party at Navigator Site*
Local Address The internal IP reported by the Navigator when it last phoned home.	*Not configurable.*
DHCP Determines whether the Navigator should attempt DHCP network configuration when rebooted.	*Set or unset as appropriate.* *If unset, physical access to the Navigator device is required. Static procedure uses a USB console cable.*
Navigator VPN Address The VPN endpoint IP of the Navigator Tunnel.	*Configured automatically by the NavCon during Navigator Initial Setup.*
VPN Subnet The network address of the Navigator's NAT Pool	*Configured automatically by the NavCon during Navigator Initial Setup.*
Number of Hosts The number of assignable NAT Addresses in the Navigator's NAT Pool	*Configured manually by the user during Navigator Initial Setup.*

Navigator Edit – NAT Table

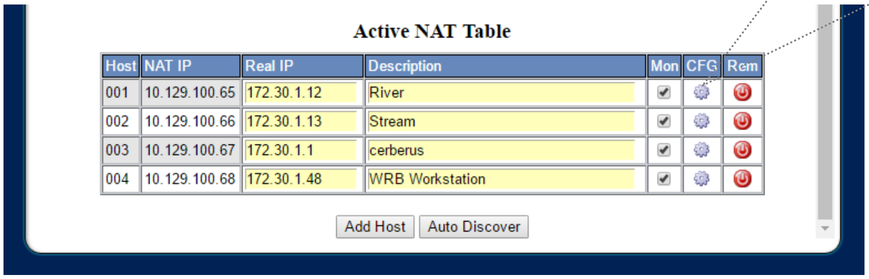
Configuration for the Navigator's NAT Devices is defined on this view.

Complete the **Real IP** and **Description** fields in the NAT Table as appropriate. Click **Update** when finished.



Select Monitoring Template

Template Type: IP Device With Port Monitor



Active NAT Table

Host	NAT IP	Real IP	Description	Mon	CFG	Rem
001	10.129.100.65	172.30.1.12	River	☑	⚙	⏻
002	10.129.100.66	172.30.1.13	Stream	☑	⚙	⏻
003	10.129.100.67	172.30.1.1	cerberus	☑	⚙	⏻
004	10.129.100.68	172.30.1.48	WRB Workstation	☑	⚙	⏻

Click the **CFG** gear at right to select a Monitoring Template and configure the monitoring thresholds. For more information see Configure Monitoring on page 14.

- Only eight NAT entries are displayed at a time. Use the numbered links below the table to browse from page to page.
- When editing the NAT table, click **Update** before moving to a new page number. Otherwise all changes will be lost.
- The NavCon tells the Navigator to reboot each time the **Update** button is clicked.

Navigator Edit – Static and Dynamic Network Configuration

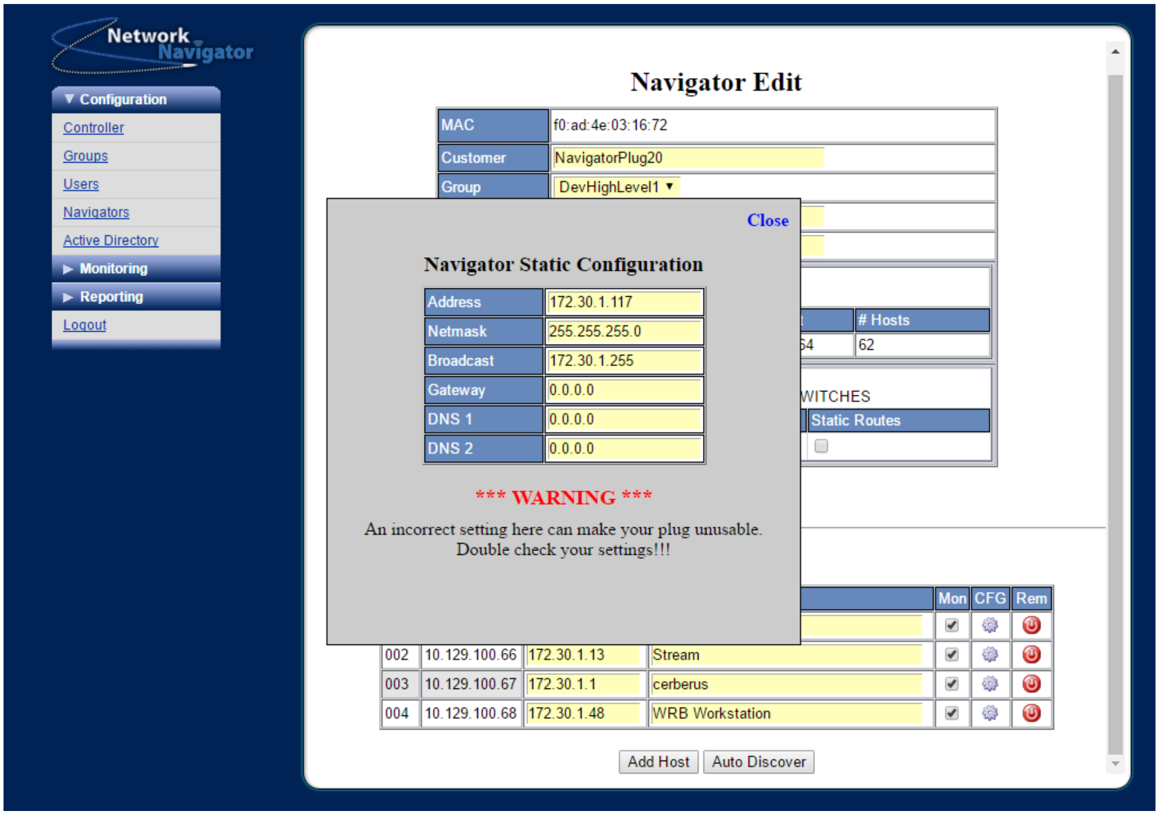
By default the Network Navigator uses DHCP. It is OK to leave the Navigator in this configuration. Use this procedure only if a static IP is required.

Note This procedure requires that the Navigator successfully executes the phone-home sequence in its default (DHCP) configuration. Allow the Navigator to connect; then complete this procedure. The Navigator will reboot after the configuration is updated.

Note If the Navigator can't successfully phone home in its default configuration, or if the Navigator becomes unreachable due to incorrectly entered network settings, its network configuration can be set using the included USB-to-serial console cable. Refer to the Additional Procedures section of this document.

Navigator Edit – Static and Dynamic Network Configuration, cont'd

On the Navigator Edit view, un-check the **DHCP** checkbox. A pop-up dialog appears.



Navigator Edit

MAC	f0:ad:4e:03:16:72
Customer	NavigatorPlug20
Group	DevHighLevel1 ▾

Navigator Static Configuration

Address	172.30.1.117
Netmask	255.255.255.0
Broadcast	172.30.1.255
Gateway	0.0.0.0
DNS 1	0.0.0.0
DNS 2	0.0.0.0

*** WARNING ***

An incorrect setting here can make your plug unusable.
Double check your settings!!!

	# Hosts
54	62

WITCHES

Static Routes
□

				Mon	CFG	Rem
				☑		
002	10.129.100.66	172.30.1.13	Stream	☑		
003	10.129.100.67	172.30.1.1	cerberus	☑		
004	10.129.100.68	172.30.1.48	WRB Workstation	☑		

Complete the **Address**, **Netmask**, **Broadcast**, **Gateway**, **DNS1**, and **DNS2** fields in pop-up dialog.

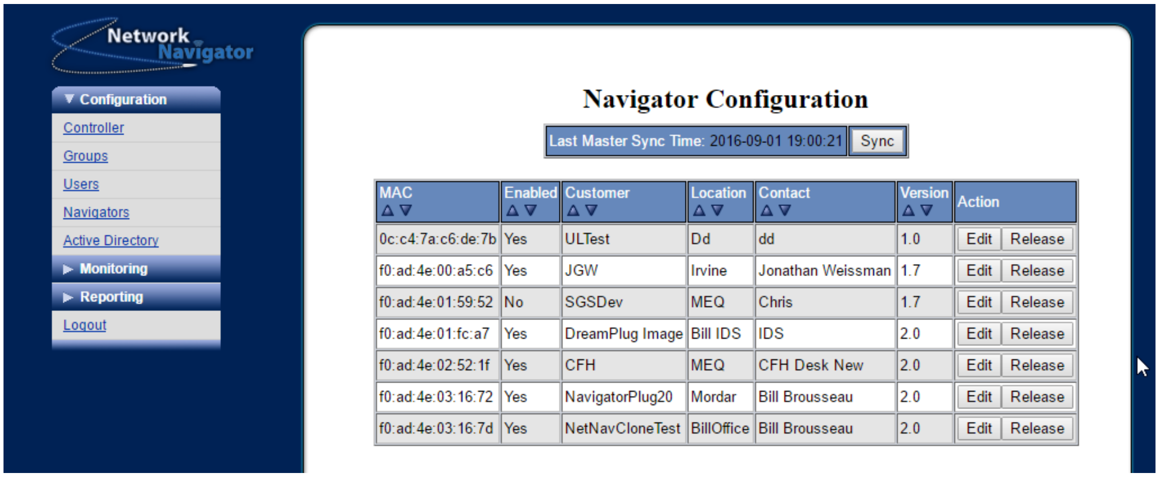
Click **Close**, then click **Update**. Allow time for the Navigator to reboot.

To revert to a DHCP network configuration after a static network configuration has been set, browse to the device's Navigator Edit view and check the **DHCP** checkbox. Click **Submit**. Allow time for the device to reboot.

Navigator Edit – Releasing a Navigator

During initial configuration for a Navigator, clicking the **Edit** button loads the Navigator Initial Setup view before loading the Navigator Edit view.

After initial configuration, clicking the **Edit** button immediately loads the Navigator Edit view.



Navigator Configuration

Last Master Sync Time: 2016-09-01 19:00:21 Sync

MAC △ ▽	Enabled △ ▽	Customer △ ▽	Location △ ▽	Contact △ ▽	Version △ ▽	Action
0c:c4:7a:c6:de:7b	Yes	ULTest	Dd	dd	1.0	Edit Release
f0:ad:4e:00:a5:c6	Yes	JGW	Irvine	Jonathan Weissman	1.7	Edit Release
f0:ad:4e:01:59:52	No	SGSDev	MEQ	Chris	1.7	Edit Release
f0:ad:4e:01:fc:a7	Yes	DreamPlug Image	Bill IDS	IDS	2.0	Edit Release
f0:ad:4e:02:52:1f	Yes	CFH	MEQ	CFH Desk New	2.0	Edit Release
f0:ad:4e:03:16:72	Yes	NavigatorPlug20	Mordar	Bill Brousseau	2.0	Edit Release
f0:ad:4e:03:16:7d	Yes	NetNavCloneTest	BillOffice	Bill Brousseau	2.0	Edit Release

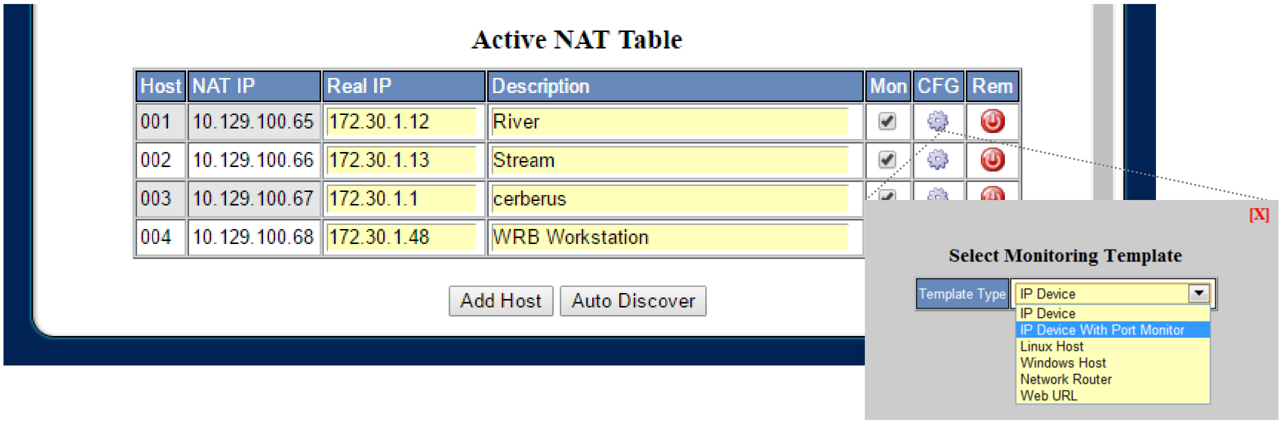
To reach the Navigator Initial Setup view again, click the **Release** button. The page will refresh, and a message will be displayed indicating that "Navigator xx:xx:xx:xx:xx:xx has been released".

Note Releasing a Navigator resets its IP configuration and purges its NAT table. IPs and descriptions for all NAT Devices are discarded. When initial setup is completed again, a different pool of NAT addresses may be assigned. This operation cannot be reversed.

Navigator Edit – Configure Monitoring

The monitoring views display graphical information about the status of the Navigator Controller, Navigators, and NAT Devices.

After checking the **CFG** gear to the right of each device, you will be prompted to select a Monitoring Template. Select the appropriate template for your device.



Active NAT Table

Host	NAT IP	Real IP	Description	Mon	CFG	Rem
001	10.129.100.65	172.30.1.12	River	☑	⚙	⏻
002	10.129.100.66	172.30.1.13	Stream	☑	⚙	⏻
003	10.129.100.67	172.30.1.1	cerberus	☑	⚙	⏻
004	10.129.100.68	172.30.1.48	WRB Workstation			

Select Monitoring Template

Template Type: IP Device

The following list of monitoring templates identifies the graphs associated with each.

IP Device
* Ping from Navigator

IP Device With Port Monitor
* Ping from Navigator
* TCP Polling

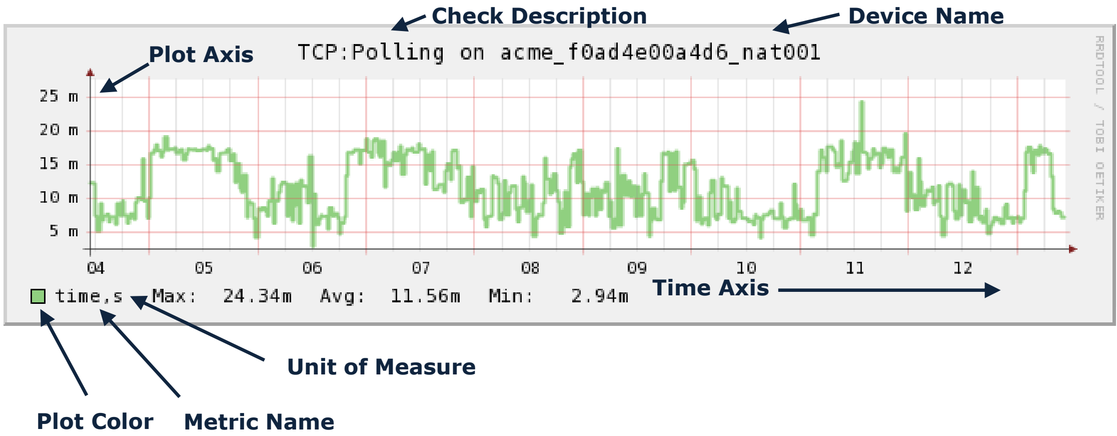
Linux Host
* Ping from Navigator
* CPU Load
* Unix disk utilization

Network Router
* Ping from Navigator
* Interface Status
* Interface Bandwidth

Web URL
* Web URL

Windows Host
* Ping from Navigator
* Windows CPU usage
* Windows disk utilization

The graphs each display a plot over time of one or more metrics, color-coded as indicated in the legend. If the metric has a unit of measure, it appears in the legend.



Hint: To zoom in on a section of any graph, click and drag your mouse to highlight that section.

Navigator Edit – Configure Monitoring, cont'd

Monitoring thresholds for the device will display after you select the appropriate template. Modify the user specified values as appropriate.

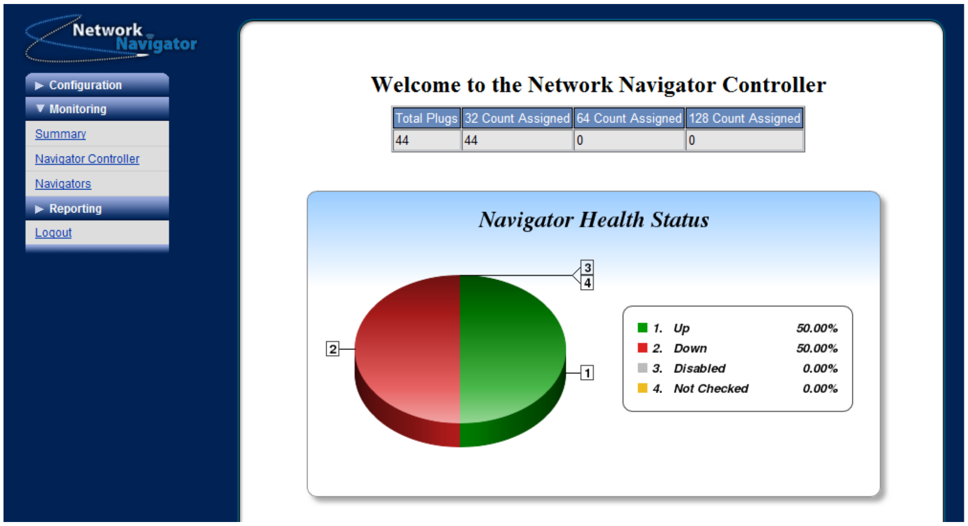
Check Name and Description	Field Values	Purpose
Ping from Navigator – Measures Latency and Packet Loss within Navigator Site	Ping count: 4 Warning Threshold (ms,loss%): 200,21% Critical Threshold (ms,loss%): 400,41%	High network response times or any packet loss is a result of data network problems.
TCP Polling – Measures User-specified TCP port response time	TCP Port Number: user specified (recommended 80) Warning Threshold (seconds): 2 Critical Threshold (seconds): 4	High port response times means slow application response to the users.
CPU Load – Measures Unix CPU load	Warning Threshold (1min,5min,15min): 4,3,2 Critical Threshold (1min,5min,15min): 6,5,4	High Unix load values are signs of server problems. Unix load is combination of disk, cpu, and memory. High load can be degraded server or application process.
Unix disk utilization – Delivers low disk space alert	Disk Device: User specified Warning Threshold (Used%): 80 Critical Threshold (Used%): 90	When disk drives reach capacity it can be disastrous to the applications. Alerts are proactively generated to avoid data loss.
Interface Status – Delivers Alert on Any Interface Not Administratively Down	ifTypes to ignore (comma-separated): User specified (recommended 23)	Routers facilitate communications between data networks. Interfaces that are down mean loss of connectivity to that whole network.

Check Name and Description	Field Values	Purpose
Interface Bandwidth – Provides graph and alert on user-specified interface bandwidth	Interface Name: User specified Warning Threshold %: 80 Critical Threshold %: 90	Sustained high bandwidth utilization can cause user applications to run very slow and be costly. Bandwidth is tracked for capacity planning and alerts are generated as the bandwidth capacity is reached.
Web URL – Measures HTTP Response Time	Warning threshold (seconds): 2 Critical threshold (seconds): 4 Complete URL: User Specified	The Navigator can proactively test the response to a web site. When response times are slow, users experience will be slow as well.
Windows CPU usage – Measures CPU usage total percent	Warning Threshold %: 80 Critical Threshold %: 90	Sustained high CPU usage is a sign of application problems or capacity limits on the server. User experiences and processing can be greatly affected.
Windows disk utilization – Delivers alert on low disk space	Drive letter: User specified Warning Threshold (Used%): 80 Critical Threshold (Used%): 90	When disk drives reach capacity it can be disastrous to the applications. Alerts are proactively generated to avoid data loss.

Monitoring

Monitoring ▶ Summary

The Summary view depicts the current connectivity status for Network Navigators associated with the user's group.



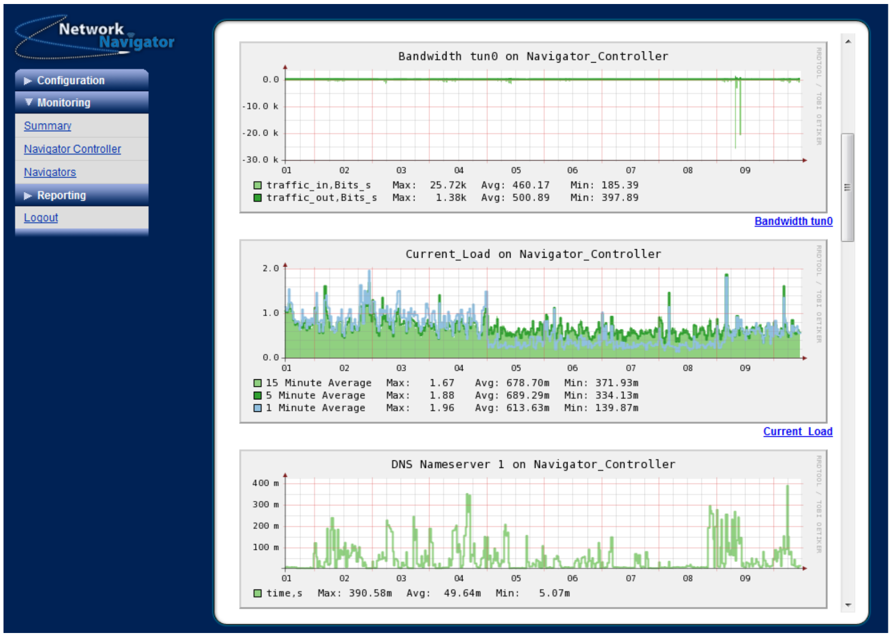
Welcome to the Network Navigator Controller

Total Plugs	32 Count Assigned	64 Count Assigned	128 Count Assigned
44	44	0	0

🟩 1.	*Up*	*50.00%*
🟥 2.	*Down*	*50.00%*
■ 3.	*Disabled*	*0.00%*
🟨 4.	*Not Checked*	*0.00%*

Monitoring ▶ Navigator Controller

This view shows health information for the Navigator Controller appliance.

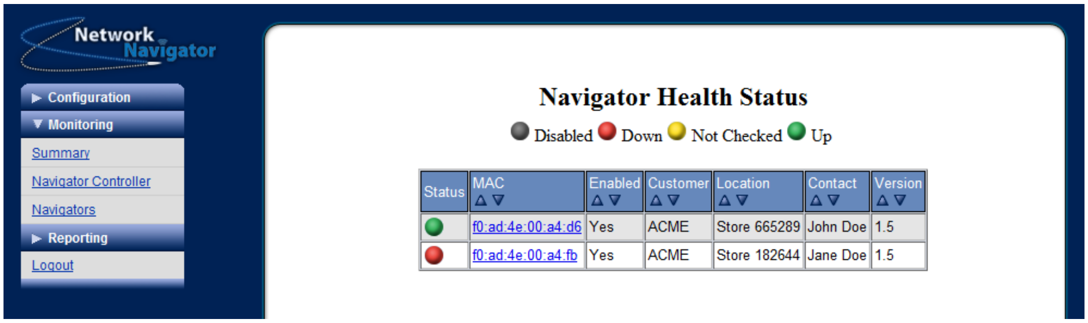


```
■ traffic_in,Bits_s    Max:  25.72k  Avg: 460.17   Min: 185.39
■ traffic_out,Bits_s   Max:   1.38k  Avg: 500.89   Min: 397.89

■ 15 Minute Average   Max:   1.67   Avg: 678.70m   Min: 371.93m
■ 5 Minute Average    Max:   1.88   Avg: 689.29m   Min: 334.13m
■ 1 Minute Average    Max:   1.96   Avg: 613.63m   Min: 139.87m

■ time,s   Max: 390.58m   Avg:   49.64m   Min:    5.07m
```

All graphs are displayed in daily, weekly, and monthly time ranges. Use the collapse ⊟ and expand ⊞ controls in each graph section to display the desired time ranges.

Monitoring ▶ Navigators

This view lists the Navigators in the user's group.



Navigator Health Status

● Disabled ● Down ● Not Checked ● Up

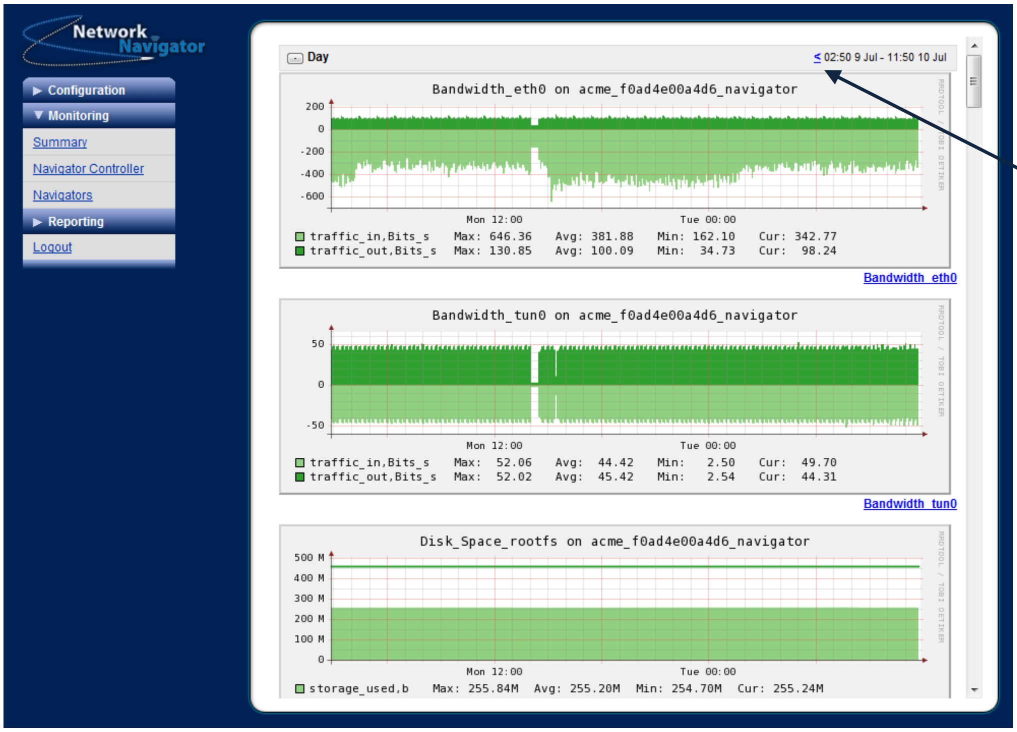
Status	MAC △▽	Enabled △▽	Customer △▽	Location △▽	Contact △▽	Version △▽
🟢	f0:ad:4e:00:a4:d6	Yes	ACME	Store 665289	John Doe	1.5
🔴	f0:ad:4e:00:a4:fb	Yes	ACME	Store 182644	Jane Doe	1.5

- Mouse-over a Navigator's colored status dot to see its ping graph.
- Click the colored status dot to go to the Navigator Graphs view.
- Click the MAC address to go to the NAT Hosts view.

Monitoring ▶ Navigators ▶ Navigator Graphs

This view shows health and status graphs for a Network Navigator.

> *Note* To reach this view, browse to Monitoring ▶ Navigators and click the colored status dot for a Navigator.



```
■ traffic_in,Bits_s    Max: 646.36    Avg: 381.88    Min: 162.10    Cur: 342.77
■ traffic_out,Bits_s   Max: 130.85    Avg: 100.09    Min:  34.73    Cur:  98.24
```

```
■ traffic_in,Bits_s    Max:  52.06    Avg:  44.42    Min:   2.50    Cur:  49.70
■ traffic_out,Bits_s   Max:  52.02    Avg:  45.42    Min:   2.54    Cur:  44.31
```

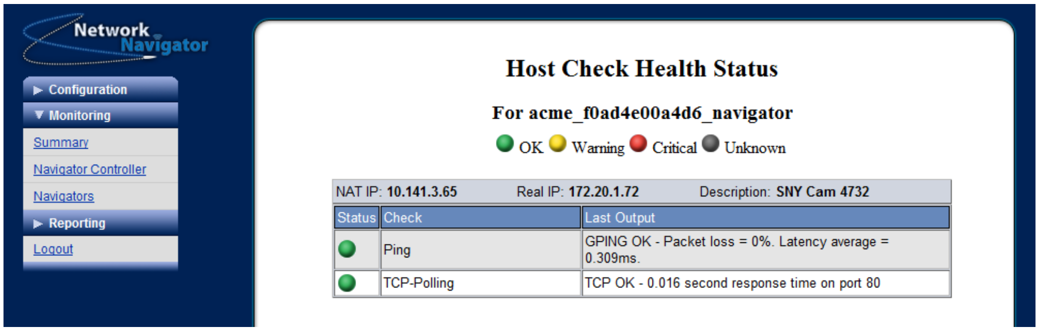
```
■ storage_used,b    Max: 255.84M   Avg: 255.20M   Min: 254.70M   Cur: 255.24M
```

Hint: Click on the arrows at the top right to view previous days' graphs.

Monitoring ▶ Navigators ▶ NAT Hosts

This view shows current monitoring status for NAT Devices on a Navigator.

> *Note* To reach this view, browse to Monitoring ▶ Navigators and click the MAC address for a Navigator.



Host Check Health Status

For acme_f0ad4e00a4d6_navigator

● OK ● Warning ● Critical ● Unknown

NAT IP: **10.141.3.65** Real IP: **172.20.1.72** Description: **SNY Cam 4732**

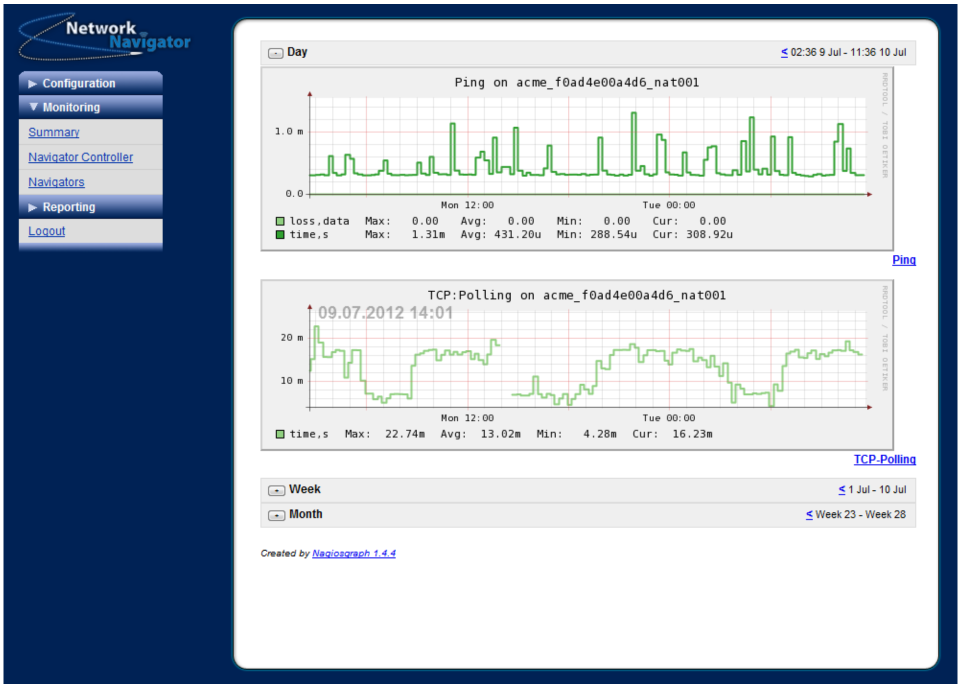
Status	Check	Last Output
●	Ping	GPING OK - Packet loss = 0%, Latency average = 0.309ms.
●	TCP-Polling	TCP OK - 0.016 second response time on port 80

- Mouse-over a check's colored status dot to see its graph.
- Click the colored status dot to go to the NAT Hosts Graphs view.

Monitoring ▶ Navigators ▶ NAT Host Graphs

This view shows graphs for all checks on a NAT Device.

> *Note* To reach this view, browse to Monitoring ▶ Navigators ▶ NAT Hosts and click the colored status dot for a check on a NAT Device.



```
■ loss,data   Max:   0.00   Avg:   0.00    Min:   0.00    Cur:   0.00
■ time,s      Max:   1.31m  Avg: 431.20u   Min: 288.54u   Cur: 308.92u
```

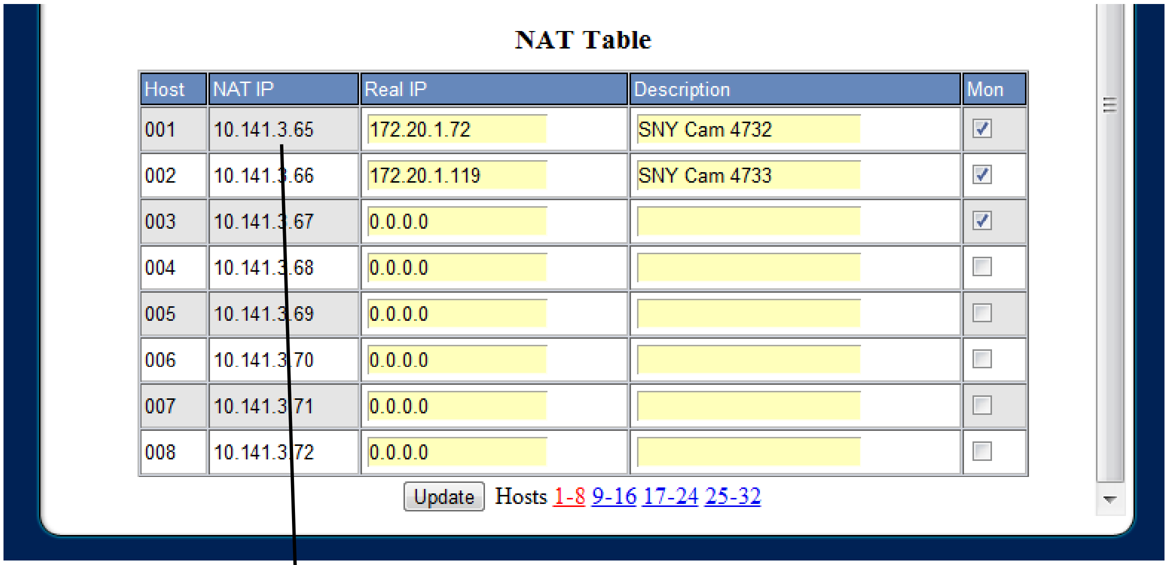
```
■ time,s   Max:  22.74m   Avg:  13.02m   Min:   4.28m   Cur:  16.23m
```

Created by Nagiosgraph 1.4.4

Monitoring – Accessing a Device

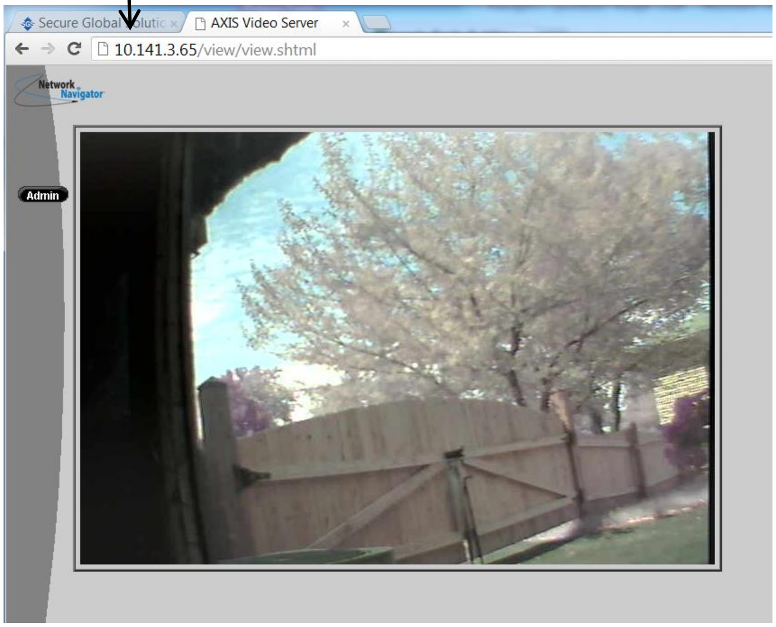
Use a device’s virtual IP address to obtain access. To find the virtual IP address, select **Navigator** under the **Configuration** menu, find the Navigator you want to access, and select **Edit**.

Copy the virtual IP address from the NAT Table, paste it into a new tab on your browser, and press Enter.



NAT Table

Host	NAT IP	Real IP	Description	Mon
001	10.141.3.65	172.20.1.72	SNY Cam 4732	☑
002	10.141.3.66	172.20.1.119	SNY Cam 4733	☑
003	10.141.3.67	0.0.0.0		☑
004	10.141.3.68	0.0.0.0		☐
005	10.141.3.69	0.0.0.0		☐
006	10.141.3.70	0.0.0.0		☐
007	10.141.3.71	0.0.0.0		☐
008	10.141.3.72	0.0.0.0		☐

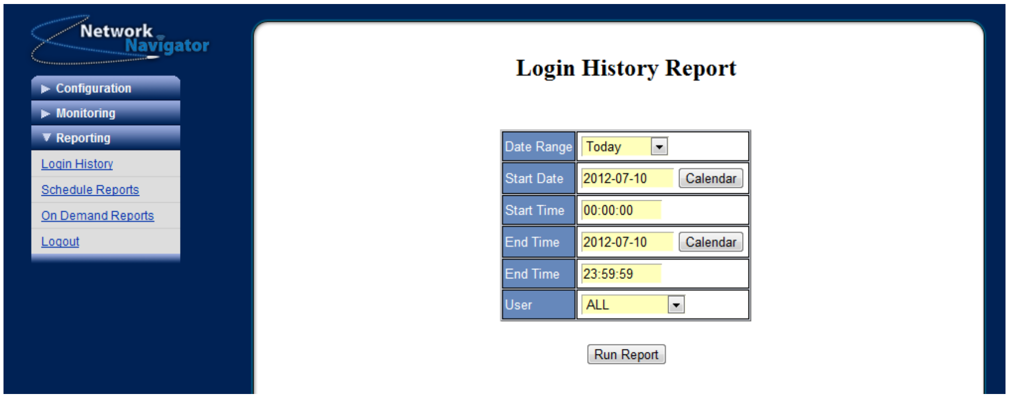


Reporting

Three reporting options allow you to track Navigator history and status:

Reporting ▶ Login History

Submitting this form generates a report of Teleworker VPN login history.



Login History Report

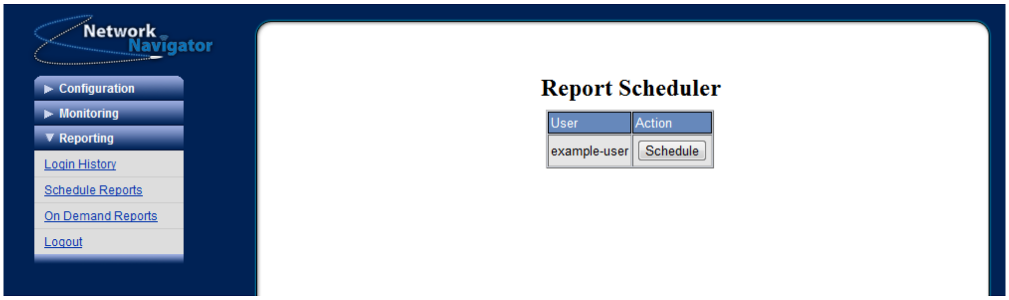
Date Range	Today	
Start Date	2012-07-10	Calendar
Start Time	00:00:00	
End Time	2012-07-10	Calendar
End Time	23:59:59	
User	ALL	

Run Report

The report output can be exported to Excel-compatible CSV format.

Reporting ▶ Schedule Reports

Users can receive the Summary Report by email.



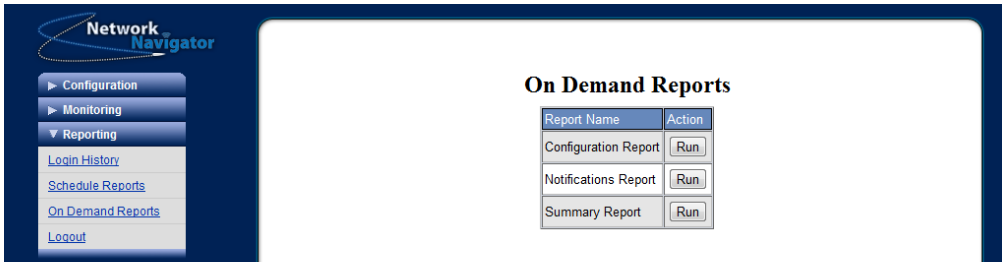
Report Scheduler

User	Action
example-user	Schedule

Report frequency can be set to None, Daily, Weekly, or Monthly.

Reporting ▶ On Demand Reports

Configuration and Summary reports can be generated on-demand.



On Demand Reports

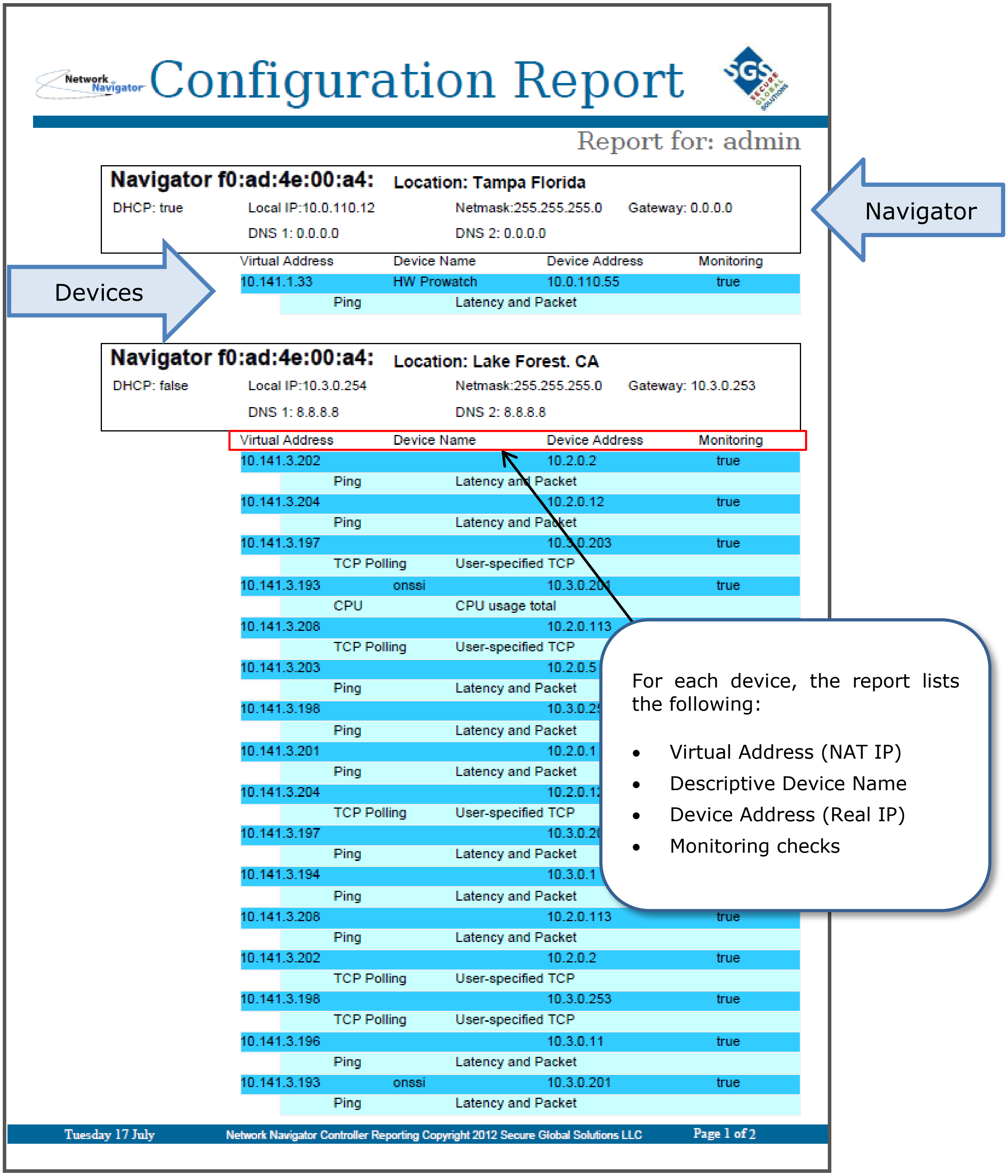
Report Name	Action
Configuration Report	Run
Notifications Report	Run
Summary Report	Run

The report output is generated in PDF format.

Samples of the Configuration and Summary reports are shown in the following section.

Configuration Report

This report is a comprehensive list of all of the Navigators and devices in your group. Use this report to find devices, and access them through the Navigator VPN using the Virtual Addresses.



Network Navigator Configuration Report

Report for: admin

Navigator f0:ad:4e:00:a4: Location: Tampa Florida

DHCP: true Local IP:10.0.110.12 Netmask:255.255.255.0 Gateway: 0.0.0.0

DNS 1: 0.0.0.0 DNS 2: 0.0.0.0

Virtual Address	Device Name	Device Address	Monitoring
10.141.1.33	HW Prowatch	10.0.110.55	true
	Ping	Latency and Packet	

Navigator f0:ad:4e:00:a4: Location: Lake Forest. CA

DHCP: false Local IP:10.3.0.254 Netmask:255.255.255.0 Gateway: 10.3.0.253

DNS 1: 8.8.8.8 DNS 2: 8.8.8.8

Virtual Address	Device Name	Device Address	Monitoring
10.141.3.202		10.2.0.2	true
	Ping	Latency and Packet	
10.141.3.204		10.2.0.12	true
	Ping	Latency and Packet	
10.141.3.197		10.3.0.203	true
	TCP Polling	User-specified TCP	
10.141.3.193	onssi	10.3.0.201	true
	CPU	CPU usage total	
10.141.3.208		10.2.0.113	
	TCP Polling	User-specified TCP	
10.141.3.203		10.2.0.5	
	Ping	Latency and Packet	
10.141.3.198		10.3.0.2	
	Ping	Latency and Packet	
10.141.3.201		10.2.0.1	
	Ping	Latency and Packet	
10.141.3.204		10.2.0.1	
	TCP Polling	User-specified TCP	
10.141.3.197		10.3.0.2	
	Ping	Latency and Packet	
10.141.3.194		10.3.0.1	
	Ping	Latency and Packet	
10.141.3.208		10.2.0.113	true
	Ping	Latency and Packet	
10.141.3.202		10.2.0.2	true
	TCP Polling	User-specified TCP	
10.141.3.198		10.3.0.253	true
	TCP Polling	User-specified TCP	
10.141.3.196		10.3.0.11	true
	Ping	Latency and Packet	
10.141.3.193	onssi	10.3.0.201	true
	Ping	Latency and Packet	

Tuesday 17 July Network Navigator Controller Reporting Copyright 2012 Secure Global Solutions LLC Page 1 of 2

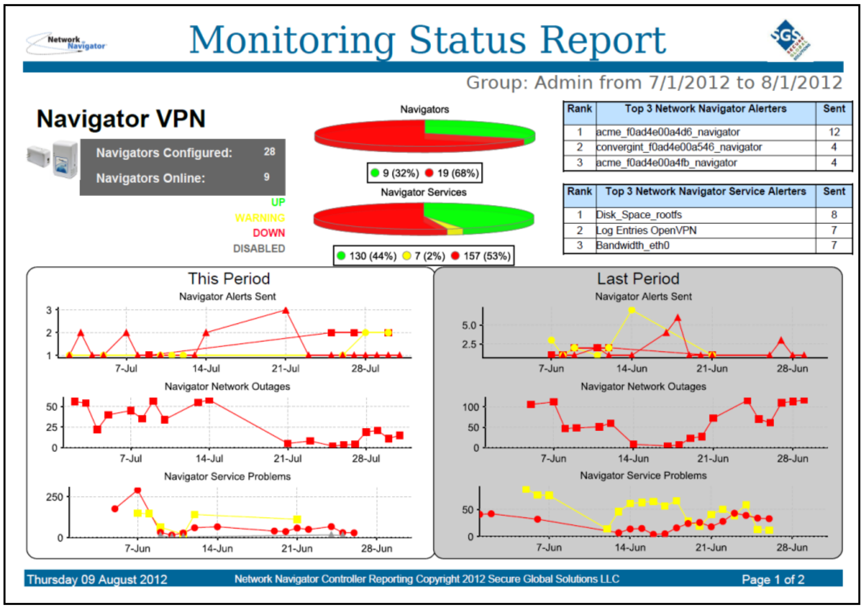
For each device, the report lists the following:

- Virtual Address (NAT IP)
- Descriptive Device Name
- Device Address (Real IP)
- Monitoring checks

Summary Report

The summary report is a two-page report that offers a “big picture” representation of the status of Navigators and devices.

View Navigator statuses on page 1



Monitoring Status Report

Group: Admin from 7/1/2012 to 8/1/2012

Navigator VPN

Navigators Configured: 28

Navigators Online: 9

UP
WARNING
DOWN
DISABLED

Rank	Top 3 Network Navigator Alerters	Sent
1	acme_f0ad4e00a4d6_navigator	12
2	convergint_f0ad4e00a546_navigator	4
3	acme_f0ad4e00a4fb_navigator	4

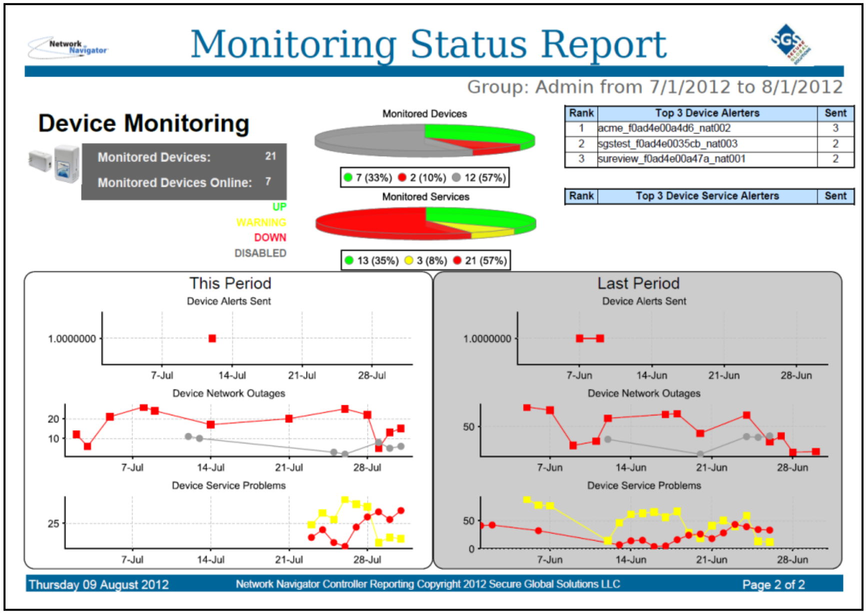
Rank	Top 3 Network Navigator Service Alerters	Sent
1	Disk_Space_rootfs	8
2	Log Entries OpenVPN	7
3	Bandwidth_eth0	7

Thursday 09 August 2012 Network Navigator Controller Reporting Copyright 2012 Secure Global Solutions LLC Page 1 of 2

Pie charts display the overall health of your Navigators and devices.

The tables on the upper right display the top 3 alerters for Navigators and Devices.

View device statuses on page 2



Monitoring Status Report

Group: Admin from 7/1/2012 to 8/1/2012

Device Monitoring

Monitored Devices: 21

Monitored Devices Online: 7

UP
WARNING
DOWN
DISABLED

Rank	Top 3 Device Alerters	Sent
1	acme_f0ad4e00a4d6_nat002	3
2	sgstest_f0ad4e0035cb_nat003	2
3	sureview_f0ad4e00a47a_nat001	2

Rank	Top 3 Device Service Alerters	Sent

Thursday 09 August 2012 Network Navigator Controller Reporting Copyright 2012 Secure Global Solutions LLC Page 2 of 2

Graphs below display alerts sent during the current and last time periods.

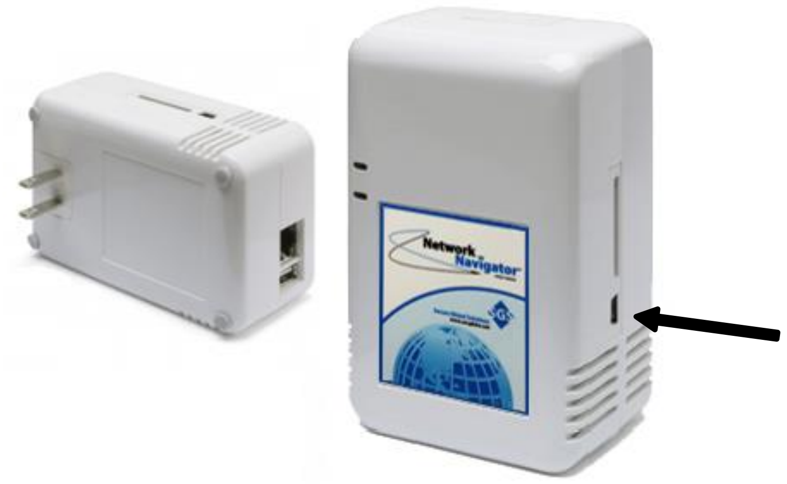
Additional Procedures

Network Navigator USB-to-Serial Console Session

The Network Navigator accepts a serial TTY session via the included USB-to-serial cable. A user account permits the administrator at a Navigator Site to manually alter the IP configuration of the Navigator.

It is preferred to use the Navigator Controller's web-based management interface to set IP configuration for Network Navigators. Refer to the Web-Based Management Interface section of this document. Allow the Navigator to boot and phone home in its default configuration; then change its IP configuration via the NavCon. The Navigator will reboot automatically when the changes are saved.

It is not necessary to use a serial console session unless the Navigator won't phone home to its Navigator Controller to retrieve configuration information.



The serial console port is located on the side of the device. It looks like a USB Mini-B port, but it uses serial TTY protocols, not USB communication protocols.

Note The included console cable is not a standard USB cable. Do not attempt to substitute a standard USB cable for the included serial console cable.

Note Some Windows systems may require device driver installation to communicate with the Navigator. A procedure for installing Windows device drivers is included later in this section.

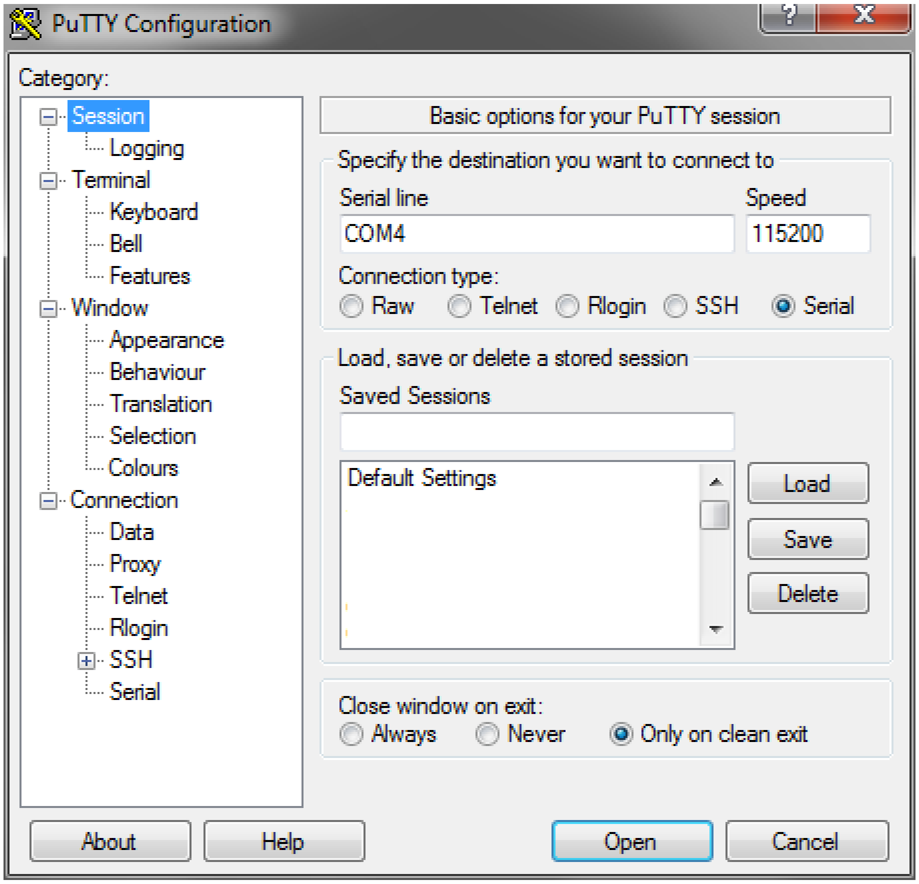
Connecting and Disconnecting with PuTTY (Windows)

Use the included USB-to-serial console cable to connect the Navigator to the Windows workstation.

Connect the Navigator to electrical power.

If the Windows workstation does not find drivers for the connected hardware, download and install the drivers as discussed in the Additional Procedures section of this document.

Launch PuTTY.



Basic options for your PuTTY session

Specify the destination you want to connect to

Serial line: COM4

Speed: 115200

Connection type:
○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

Load, save or delete a stored session

Saved Sessions

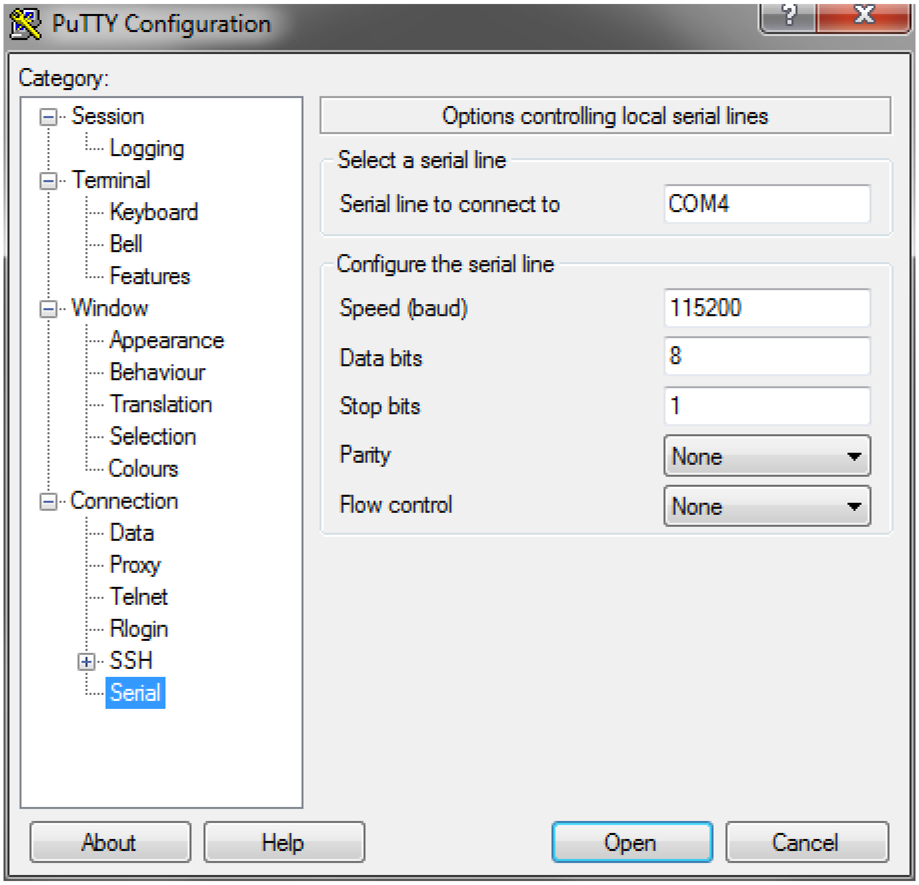
Default Settings

Close window on exit:
○ Always ○ Never ● Only on clean exit

In the **Session** category, select the **Serial** radio button.

Then click the **Serial** category.

Connecting and Disconnecting with PuTTY (Windows), cont'd



Options controlling local serial lines

Select a serial line

Serial line to connect to: COM4

Configure the serial line

Speed (baud): 115200

Data bits: 8

Stop bits: 1

Parity: None

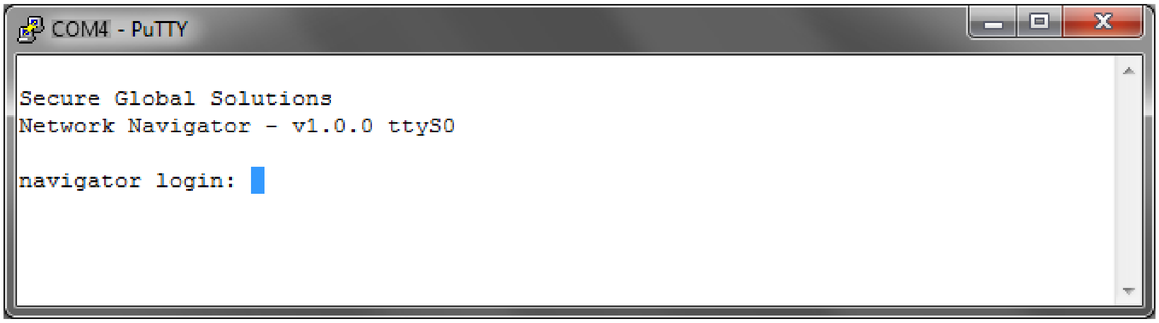
Flow control: None

In the Serial category, complete the fields as follows:

• **Serial line to connect to**	*As shown in Device Manager for USB Serial Port*
• **Speed (baud)**	115200
• **Data bits**	8
• **Stop bits**	1
• **Parity**	None
• **Flow control**	None

Click **Open**.

Connecting and Disconnecting with PuTTY (Windows), cont'd



```
Secure Global Solutions
Network Navigator - v1.0.0 ttyS0

navigator login:
```

To disconnect, simply close the PuTTY window.

Connecting and Disconnecting with screen (Linux)

Use the included USB-to-serial console cable to connect the Navigator to the Linux workstation.

Connect the Navigator to electrical power.

In a command shell with sufficient privilege, enter the following command. It may be necessary to press enter a few times to redisplay the login prompt.

```
[bash ~]# screen /dev/ttyUSB0 115200

Secure Global Solutions
Network Navigator - v1.0.0 ttyS0

navigator login:
```

> *Note* In Linux, the **screen** command invokes a text-based window manager with terminal emulation. From the workstation's command shell, type **man screen** for additional information. If the Linux workstation is not equipped with **screen**, another serial-compatible terminal emulator such as **minicom** may be used. Consult the relevant man pages.

To terminate the console session using **screen**, press **CONTROL-a**, then type **D D** (case-sensitive):

```
C-a D D
Screen session of root 0.0 ttyS0 ended.
[bash ~]
```

Setting Static IP Configuration

Note Use this procedure only when the Navigator and NavCon cannot communicate. If the Navigator is tunneling to the NavCon, use the NavCon web interface instead of this procedure. Refer to the Navigator Edit – Static and Dynamic Network Configuration procedure in the Web-Based Management Interface section of this document.

Start a console session as described in the previous procedures.

Type username ‘**recovery**’ and password ‘**br1ckbr3ak3r**’ to log in.

The system supplies prompts for setting static IP configuration. Refer to the following example. Substitute appropriate input values.

The Navigator will reboot after the inputs are confirmed.

```
Secure Global Solutions
Network Navigator - v1.0.0 ttyS0

navigator login: recovery
Password: br1ckbr3ak3r

[system messages omitted from sample output]

The current Navigator DHCP state is: Enabled

Would you like to change it (Y/N)? y

*** WARNING ***

Be sure your Navigator Controller is configured correctly
Before making this change and rebooting!!!

Please enter the following Static information.
IP Address: 192.168.100.100
Netmask: 255.255.255.0
Broadcast: 192.168.100.255
Gateway: 192.168.100.1
DNS1: 8.8.8.8
DNS2: 8.8.4.4

[continued on next page]
```

Setting Static IP Configuration, cont’d

```
[continued from previous page]

You entered:
IP:             192.168.100.100
Netmask:        255.255.255.0
Broadcast:      192.168.100.255
Gateway:        192.168.100.1
DNS1:           8.8.8.8
DNS2:           8.8.4.4
Is this Correct (Y/N)? y

Broadcast message from recovery@navigator
        (/dev/ttyS0) at 15:26 ...

The system is going down for reboot NOW!

[system messages omitted from sample output]

Secure Global Solutions
Network Navigator - v1.0.0 ttyS0

navigator login:
```

Setting DHCP IP Configuration

> *Note* Use this procedure only when the Navigator and NavCon cannot communicate. If the Navigator is tunneling to the NavCon, use the NavCon web interface instead of this procedure. Refer to the Navigator Edit – Static and Dynamic Network Configuration procedure in the Web-Based Management Interface section of this document.

Start a console session as described in the previous procedures.

Type username '**recovery**' and password '**br1ckbr3ak3r**' to log in.

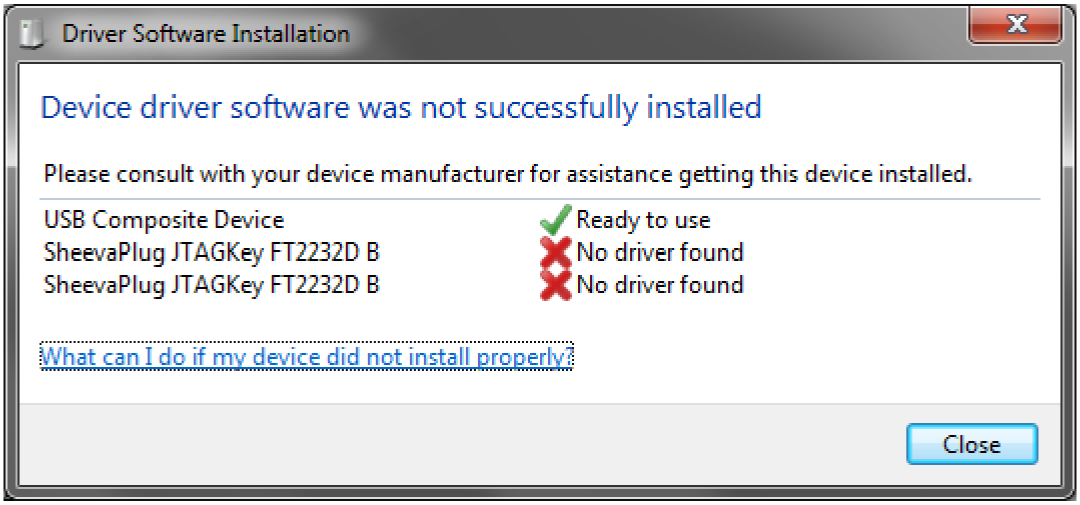
The system supplies prompts for setting DHCP IP configuration. Refer to the following example.

The Navigator will reboot after the inputs are confirmed.

```
Secure Global Solutions
Network Navigator - v1.0.0 ttyS0

navigator login: recovery
Password: br1ckbr3ak3r

[system messages omitted from sample output]

The current Navigator DHCP state is: Disabled

Would you like to change it (Y/N)? y

*** WARNING ***

Be sure your Navigator Controller is configured correctly
Before making this change and rebooting!!!

I am going to enable DHCP and restart the Navigator.
Is this OK (Y/N)? y

Broadcast message from recovery@navigator
        (/dev/ttyS0) at 15:27 ...

The system is going down for reboot NOW!

[system messages omitted from sample output]

Secure Global Solutions
Network Navigator - v1.0.0 ttyS0

navigator login:
```

Installing Navigator Device Drivers (Windows)

The Windows workstation will attempt automatic driver configuration when the Navigator is connected via console cable. If appropriate USB-to-Serial drivers are not found, an error dialog may appear:


Driver Software Installation

Device driver software was not successfully installed

Please consult with your device manufacturer for assistance getting this device installed.

USB Composite Device	✓ Ready to use
SheevaPlug JTAGKey FT2232D B	✗ No driver found
SheevaPlug JTAGKey FT2232D B	✗ No driver found

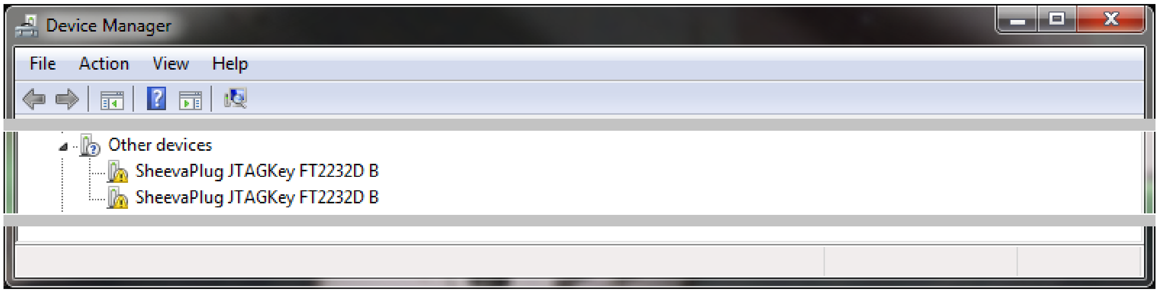
What can I do if my device did not install properly?
Close

In this case the drivers must be downloaded and installed manually. Visit the Navigator website for download instructions:

`http://www.secglobe.net/navigator`

Download the driver archive and unzip it. Note the folder path where the archive has been unzipped.

Click **Start** ▶ **Control Panel** ▶ **Device Manager**. Locate the unrecognized devices:



Right-click one of the devices and choose **Update Driver Software...**

Installing Navigator Device Drivers (Windows), cont'd

In the **Update Driver Software** wizard, do the following:

Click **Browse my computer for driver software**.

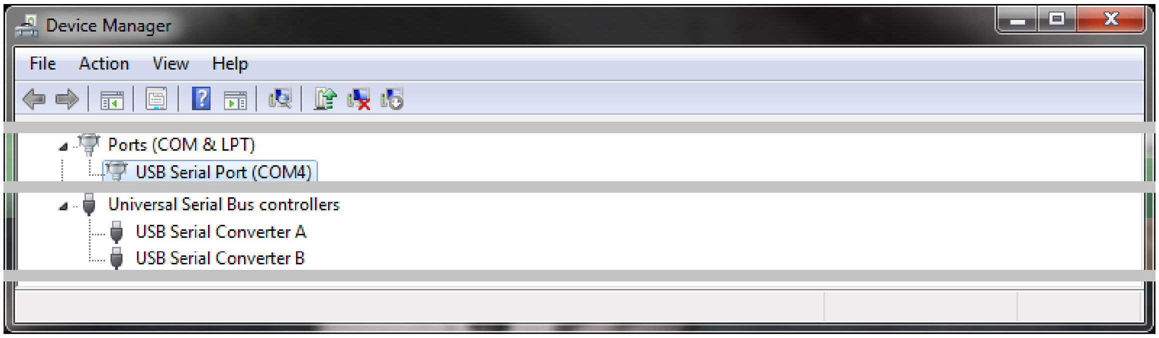
Specify the folder path where the archive has been unzipped. Click to select **Include Subfolders**. Click **Next**.

Windows may not recognize the publisher's signature. Click **Install this driver software anyway**.

The driver is installed.

Repeat for other unrecognized devices as necessary.

When finished, the Device Manager shows all devices properly recognized.



Note When establishing a serial console session via the USB-to-serial cable, You will need to know the COM port number assigned to the USB Serial Port. With necessary drivers properly installed, this information is displayed in the Device Manager as shown here

Glossary of Terms

Active Controller – In a pair of Navigator Controller mates, the active controller is the device currently functioning in the active role.

Alarm Panel – In the security alarm industry, a device which originates alarm signals in response to inputs from sensors or user interfaces. When the Network Navigator Platform is integrated with an alarm automation system such as SGS Stages, NavCons and Navigators are represented as alarm panels.

Alarm Receiver – In the security alarm industry, a device which receives alarm signals from alarm panels and queues them for processing by an alarm automation system. When the Network Navigator Platform is integrated with an alarm automation system such as SGS Stages, NavCons behave as alarm receivers.

Alarm Signal – A message transmitted from an alarm panel to an alarm receiver, containing information about an alarm event.

Automation System – A solution used by security alarm companies to process alarm signals queued by alarm receivers. The Stages application developed by Secure Global Solutions exemplifies such a system.

brickbreaker – An administrative recovery procedure used by a Navigator Administrator to alter network settings on a Network Navigator using a serial connection and terminal emulator.

Check – On the Network Navigator Platform, a check is a status condition on a device. The NavCon's monitoring subsystem executes checks on devices and generates notifications or alarm signals when problems are detected.

Check Description – A text label describing a check.

Check Template ID – A numeric value indicating how a check is run. For automation alarms on NAT devices, the check template ID is represented in the alarm signal's point value.

Connectivity – The condition necessary for two devices to communicate across an IP network. The Network Navigator Platform is designed to establish connectivity between users and NAT devices my means of VPN tunnels and virtual addresses.

Controller – See **Network Navigator Controller**

Controller Master – See **Network Navigator Controller Master**

Controller Mate – When Navigator Controllers are deployed in pairs for system redundancy, the Controllers are said to be "mates" to each other.

Controller Site – The location or business network where a Navigator Controller is deployed. When Navigators phone home to a NavCon, the Controller Site becomes the hub of a star topology of VPN tunnels.

Deployment – A set of devices and configuration which implement the Network Navigator Platform. Also, the process of installing and configuring components of the Network Navigator Platform.

Deployment Technician – A person who participates in the deployment process.

Device – A piece of computer hardware that is connected to an IP network. Servers, routers, switches, firewalls, workstations, access points, DVRs, cameras, sensors, multimedia equipment, or any other components which can be plugged into an IP network are regarded as devices.

Device Address – On the Network Navigator Platform, the device address is the "real" IP address of a device. In most cases, it is the device's LAN address.

Device Driver – A piece of software which allows a computer operating system to communicate with a connected peripheral. For example, an administrative workstation must have the proper serial device driver installed in order to communicate with a Network Navigator using the included USB-to-serial cable.

Device Enumerator – A numeric value indicating the position in a Navigator's NAT table where a NAT device has been defined. The device enumerator affects the NAT address assigned to the device. For automation alarms on NAT devices, the device enumerator is represented in the alarm signal's point value.

Device Name – A descriptive text string assigned to a NAT device.

End-User – A person who uses the Navigator Controller Platform to communicate with NAT devices.

Event Code – In an alarm signal, the event code is a short data field indicating the signal's type, such as alarm or recovery.

Firewall – A network security device which inspects network traffic and decides whether to deliver, modify, discard, or reject it. Firewalls are typically used to prevent undesirable traffic from entering or leaving a network, or to perform Network Address Translation.

FQDN – See **Fully-Qualified Domain Name**

Fully-Qualified Domain Name – A name that can be used to reach a specific computer across the Internet using DNS. A domain name is said to be "fully-qualified" if the domain portion is completely specified. For example, 'host001' is not an FQDN; whereas 'host001.example.com' is.

Generic Route Encapsulation – A network protocol for carrying remote-access VPN traffic. When a workstation connects to a Navigator Controller by VPN, PPTP and GRE are used together.

Global System for Mobile Communications – A communication standard for wireless cellular networks. Network Navigators can be connected to GSM peripherals via USB cable, to form Navigator Tunnels back to a NavCon via a wireless cellular ISP.

Graph – In the Monitoring views of the NavCon web interface, graph images are used to depict check history.

GRE – See **Generic Route Encapsulation**

Group – On Navigator Controllers, groups allow sets of users to display information about sets of Navigators.

GSM – See **Global System for Mobile Communications**

Host – See **Device**

MAC Address – The hardware address of an Ethernet interface. Navigators use MAC addresses to uniquely identify themselves to their Controllers. MAC addresses are also referenced in the NavCon web interface. If Automation integration is enabled, MAC addresses are used in constructing transmitter numbers for alarm signals.

Master – See **Network Navigator Controller Master**

Metric – On a graph, more than one measured quantity can be plotted together. These quantities, or metrics, are color coded. The graph legend shows the metric name, its unit of measure (if any), its color, and some statistics.

NAT – See **Network Address Translation**

NAT Device – A device at a Navigator Site that has been assigned a virtual address on a Navigator Controller. Users cannot communicate with devices at Navigator Sites unless this is done.

NAT Pool – The IP subnet on a Navigator Controller from which NAT Device addresses are assigned.

NavCon – See **Network Navigator Controller**

NavCon Administrator – The person or team at a Controller Site responsible for the physical deployment, connectivity status, and configuration of a Navigator Controller.

Navigator – See **Network Navigator**

Navigator Administrator – The person or team at a Navigator Site responsible for the physical deployment and connectivity status of a Network Navigator.

Navigator Controller – See **Network Navigator Controller**

Navigator Site – A facility or location where a Network Navigator has been deployed. Also, the IP network or networks that can be accessed through that Navigator.

Network Address Translation – A firewall technique for forwarding network traffic to and from a device using virtual or external IP addresses.

Network Navigator – A small SGS device which acts as a VPN client and maintains a connection to a Navigator Controller.

Network Navigator Controller – An SGS appliance which serves as a VPN concentrator and web interface for using Network Navigators.

Network Navigator Controller Master – A server operated and administered by SGS which manages the relationships between NavCons and Navigators.

Network Navigator Platform – A deployment of SGS devices including at least one Navigator Controller and at least one Network Navigator.

Notification – The monitoring subsystem on a Navigator Controller can generate alert messages when a problem is reported for a check on a device. These notification events can take the form of emails to users, alarm signals to automation, or both.

OpenVPN – The software application used for VPN tunnels between Network Navigators and Navigator Controllers.

Parent Device – In a network topology, a parent device is responsible for providing connectivity to its children. For example, there is no connectivity from a NavCon to the NAT devices at a Navigator Site unless the Navigator at that site is up and has established a VPN tunnel to the NavCon. Thus, from the perspective of the NavCon, the Navigator is the parent device of all its NAT devices. The NavCon monitoring subsystem uses parent-child relationships to suppress notifications for child devices when the parent device is down. This reduces signal flooding when Navigator tunnels are disrupted.

Ping – See **Connectivity**

Phone-Home Sequence – When a Network Navigator is booted, it takes a sequence of actions to fetch configuration settings and establish a VPN tunnel to its Navigator Controller.

Platform – See **Network Navigator Platform**

Plot – On a graph, historical values for a metric are represented as a plot which forms a line or filled area in the image.

Point – In an alarm signal, the point is a short data field indicating which check is being reported. For NAT devices, the point encodes both the host enumerator and the check template ID. For Navigators and NavCons, point values are statically defined for each check.

Point-to-Point Tunneling Protocol – A network protocol for carrying remote-access VPN control information. When a workstation connects to a Navigator Controller by VPN, PPTP and GRE are used together.

PPTP – See **Point-to-Point Tunneling Protocol**

PuTTY – Free terminal emulation software for Microsoft Windows. PuTTY can be used to create serial TTY connections and SSH connections for administering devices via text command interface.

Remote Site – An arbitrary location on the Internet from where a Teleworker needs to connect to a NavCon via PPTP/GRE VPN.

RFC 1918 – A memo published by the Internet standards community which designates specific portions of the IPv4 address space for use in private, internal networking. Subnets within these address spaces are used by the Network Navigator Platform to assign virtual IPs to NAT devices.

Router – Any device which can forward IP traffic from one network onto another. Navigator Controllers and Network Navigators incorporate routing functionality.

SGS – Secure Global Solutions

SIA Format – See **Signal Indicated Alarm Format**

Signal Indicated Alarm Format – A message format for transmitting alarm signals from alarm panels to alarm receivers. The SIA format encodes several pieces of information, including a transmitter number, an event code, and a point number. Navigator Controllers use a SIA-compatible format when submitting notification events to automation.

Site-to-Site VPN – A secure connection between network devices at two or more locations which connects the networks together, allowing devices at both locations to communicate with each other.

Stages – The alarm automation system developed by Secure Global Solutions.

Star Topology – An arrangement of network connections between three or more devices which puts one device at the "hub" and all other devices as "spokes" around the hub. Network Navigators phone home to a Navigator Controller, the NavCon becomes the hub of a star topology of VPN tunnels.

Teleworker – A user connecting to a NavCon using a remote-access PPTP/GRE VPN tunnel.

Transmitter Number – In an alarm signal, the transmitter number is a data field identifying the device that originated the signal. On the Network Navigator Platform, transmitter numbers are constructed from the MAC addresses of Navigators and NavCons.

Tunnel – See **Virtual Private Network**

Terminal Emulator – Workstation software which allows a Navigator Administrator to use the text command interface of a Network Navigator via the included USB-to-serial console cable.

TTY Session – The virtual terminal though which a Navigator's text command interface is presented when a Terminal Emulator is used.

Virtual Address – On the Network Navigator Platform, the virtual address is the "NAT" IP address of a NAT device. NavCon users can communicate with the device through the Navigator tunnel using its virtual address.

Virtual Private Network – A secure connection between devices on a network which allows connectivity between networks that would not otherwise be available. Two types of VPNs are used on the Network Navigator Platform: Navigator tunnels (using OpenVPN) and teleworker tunnels (using PPTP / GRE).

VPN – See **Virtual Private Network**

VPN Client – In a VPN connection, the VPN client is the device which requests the connection, and the VPN server is the device which grants the request. For Navigator VPNs, the Network Navigator is the client. For Teleworker VPNs, the workstation is the client. In both cases, the Navigator Controller is the VPN server.

VPN Concentrator – A device, such as a Navigator Controller, which acts as the server for multiple VPN tunnels. A NavCon can serve up to 1000 Navigator tunnels and a large number of Teleworker tunnels.

VPN User – A person or system that connects to a NavCon via remote-access VPN tunnel, for the purpose of reaching NAT hosts via Navigator tunnels.

XMIT Number – See **Transmitter Number**

Zone – See **Point**