Secureworks®

CTA Inspector

Installation Guide

Last Updated: September 2017

Copyright

Due to continued service development, the information in this publication and related software may change without notice. Please report any errors to Secureworks in writing. Secureworks does not warrant that this publication or related hardware or software is error-free. Please refer to your contract with Secureworks for any provided warranty information.

Table of Contents

Document History

Document Revision #	Date Created:	Comments:
1.0	2016/12/26	Created
1.1	2017/01/17	Updated formatting and System Specifications
1.2	2017/09/01	Updated formatting

Documentation update requests

To request modifications or notify the author of errors in this document, please notify your Secureworks representative. During initial implementation, notify your Provisioning Engineer. After initial implementation, please notify the Secureworks CTOC through a portal ticket.

Introduction

The Counter Threat Appliance (CTA) is an extension of the Counter Threat Platform (CTP) that brings the intelligence of the Secureworks Counter Threat Unit (CTU) and Counter Threat Operations Center (CTOC) into your network.

The CTA will create an encrypted tunnel back to the CTOC. Using this tunnel Secureworks will be able to fully manage your CTA, including delivering security patches and any necessary configuration updates. Prior to this tunnel being established, the device must first be configured with a valid network configuration and registered with SecureWorks. This installation guide will help talk you through the steps required for this process.

Terminology (Acronyms)

- **CLI** – Command Line Interface
- **CTA** – Counter Threat Appliance
- **CTU** – Counter Threat Unit
- **CTOC** – Counter Threat Operations Center
- **VPN** – Virtual Private Network

Requirements

In order to prepare for the CTA's implementation, please follow the below steps prior to the implementation dates.

Connectivity Requirements

The following connectivity requirements are needed for the CTA.

Source	Destination	Port/Protocol	Reason
Secureworks CTA <mgmt IP>	206.55.100.0/22	TCP/10000	Secureworks Datacenter Connectivity
Secureworks CTA <mgmt IP>	DNS Server	UDP/53	Hostname Resolution*
Secureworks CTA <mgmt IP>	Client Networks	UDP/137	Hostname Resolution*

***Hostname Resolution**: By default, the Inspector will perform hostname resolution on security event data by querying any provided DNS servers, or performing a NetBIOS lookup against the host. If this functionality is desired to be changed or disabled, please let your Secureworks representative know during implementation.

PING (ICMP echo/reply): The Secureworks CTA has an integrated firewall which by default ONLY allows you to ping the CTA from its provisioned default gateway.

Alternative VPN Port: The CTA uses port TCP/10000 by default to establish its VPN connection. If desired, this port can be changed to TCP/443. If this is desired, please inform your Secureworks representative prior to completing the CTA registration process.

Unlisted additional access requirements: The Inspector will require additional access depending on the specifics of the environment being monitored. The above table only covers requirements needed to bring the Inspector online and continue the provisioning process. If it is desired to gain a full list of access requirements for your site, contact your Secureworks representative for additional guides.

Proxy Support

The CTA supports the use of a proxy for datacenter connectivity only if the proxy is not performing inspection/analysis of the SSL/TLS traffic generated by the CTA. Secureworks will not install or provide any keys used in the encryption of traffic from the CTA to the Secureworks datacenters. If it is desired for the CTA to use a proxy for connectivity please provide the proxy IP address to your Secureworks representative prior to completing the registration of the CTA.

Physical Setup

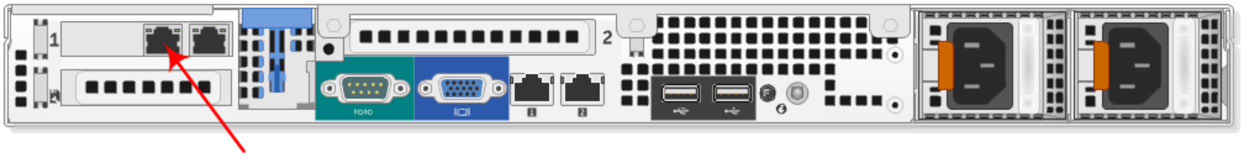
1. Rack the CTA in a 4 post rack per the Dell ReadyRails instructions included with the rail kit. The CTA requires 1U of rack space.
2. Connect the included power cable(s) to the CTA.
3. Connect the Management interface of the CTA to the network. This will be the left most network interface when looking at the back of the device.
4. Power on the device.

CTA Interface Diagram

The management interface is used for the CTA's default route. This interface cannot be changed

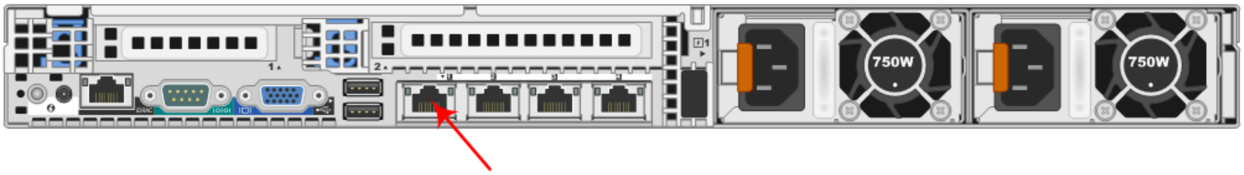
.

Standard CTA



Management Interface

High-End CTA



Management Interface

System Specifications

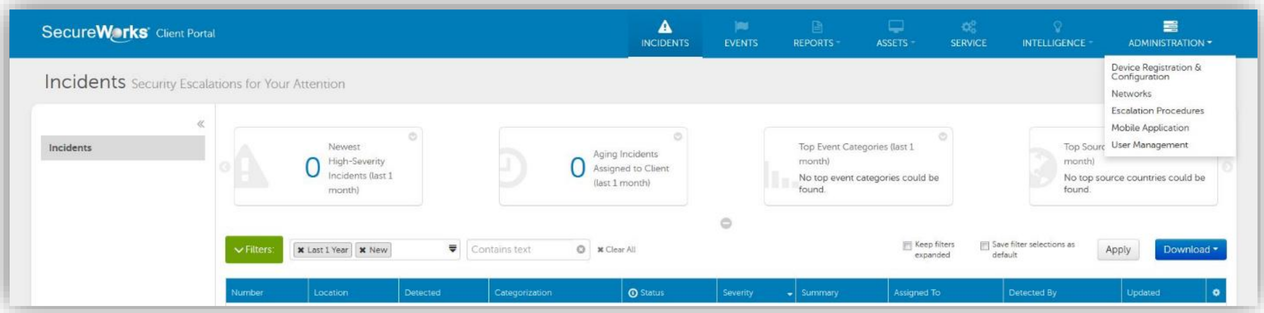
Feature	Standard (PER320)	High-End (PER630)
Purpose	Counter Threat Appliance	Counter Threat Appliance
Form factor	1U rack	1U rack
Rack Support	ReadyRails™	ReadyRails™
Power Supplies	Hot-plug redundant power supplies (350 watts each)	Hot-plug redundant power supplies (750 watts each)
Heat Dissipation	1356 BTU/hr maximum (redundant, 350W power supply)	2891 BTU/hr maximum (750W power supply)
NIC	4 x 1Gb	4 x 1Gb

Registering the CTA

All CTAs must first register with the Secureworks registration service in order to obtain a unique identity and establish a VPN connection. When the CTA first comes online it will have no network configuration and launch into a registration wizard to assist in completing the registration process. Prior to utilizing the registration wizard, a registration key must be obtained from the Secureworks Portal. If you do not have a logon to the Portal, please contact your Secureworks representative for assistance.

Obtaining a Registration Key

To obtain a registration key for your CTA, first connect to the Secureworks Portal (https://portal.secureworks.com/portal), and navigate to **Administration > Device Registration and Configuration**.



Incidents Security Escalations for Your Attention

0 Newest High-Severity Incidents (last 1 month)

0 Aging Incidents Assigned to Client (last 1 month)

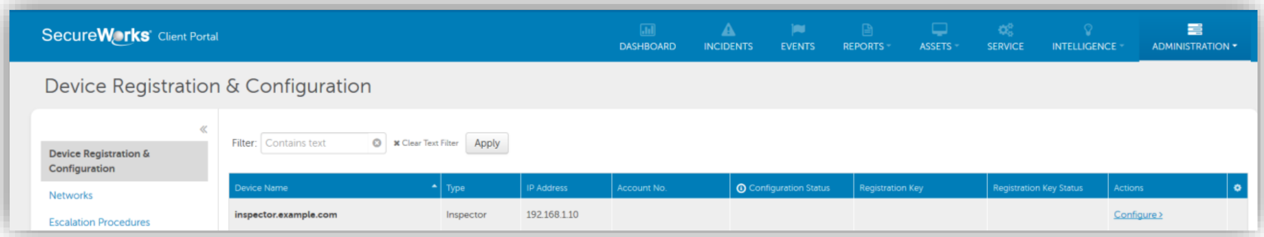
Top Event Categories (last 1 month)
No top event categories could be found.

Top Sourc month)
No top source countries could be found.

Number	Location	Detected	Categorization	Status	Severity	Summary	Assigned To	Detected By	Updated

On this page, a table will display with all devices that support registration. If you have not visited this page before, the table will only display name, type, and IP address of devices available to be configured. Entering basic networking data here is a requirement because all configuration for the CTA is centralized, so that in the event of a device failure, Secureworks can recover the full configuration and restore it on any resulting RMAs or warm spare devices. During the registration process the user must first configure network information to allow the device to communicate with Secureworks registration servers, but once registered the device will sync and run the configuration entered in this table.

Navigate to the CTA you wish to Configure, and on the far right-hand column, select the **Configure** link.

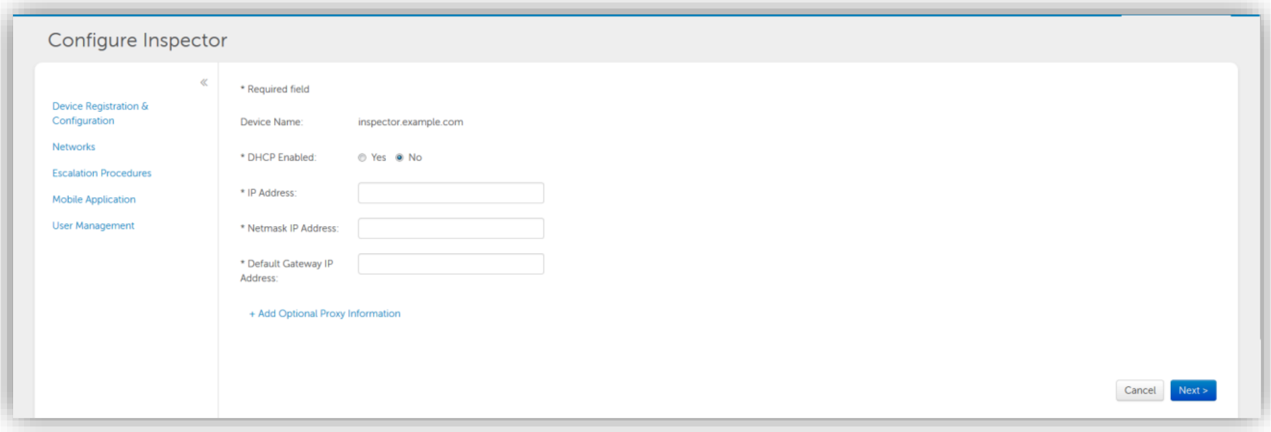


Device Registration & Configuration

Device Name	Type	IP Address	Account No.	Configuration Status	Registration Key	Registration Key Status	Actions
inspector.example.com	Inspector	192.168.1.10					Configure >

On the Configuration page, you will be asked to enter the required network information.

- DHCP Enable toggle: Change to yes if you wish to use DHCP.
- IP Address: The IP address to configure on the management interface. Additional interfaces can be configured after the device has been registered. Configuration is entered in dotted quad decimal format.
- Netmask: The netmask to be used on the management interface. Configuration is entered in dotted quad decimal format.
- Default Gateway: The default gateway IP address. Configuration is entered in dotted quad decimal format.
- **Optional** Proxy Configuration: If a proxy is desired to be used for the CTA's VPN connection, select this option to add proxy information. The CTA will use the proxy IP address for communication with both VPN connections (Secureworks primary and disaster recovery sites). IP address and port are required if a proxy is to be used. Additionally, a user can supply a username and password if authentication to the proxy is required.



Configure Inspector

* Required field

Device Name: inspector.example.com

* DHCP Enabled: ○ Yes ● No

* IP Address:

* Netmask IP Address:

* Default Gateway IP Address:

Once all information has been entered select **Next**. You will be asked to review the information entered for accuracy. Once reviewed, select **Submit**.

You will be redirected back to the main Registration page. The table will update with the information you entered.

- Account No.: This column will remain blank. Account Numbers are used when sharing the CTA image with a 3rd party account, such as AWS. This is not required for this guide.
- Configuration Status: This column displays the status of storing the information collected from the Configuration page. You can click on the information icon on the header of the column to see information on all available statuses. Within a few seconds, the Configuration Status will change to Complete.
- Registration Key: Once the Configuration Status is Complete the Registration Key column will contain a 16-character key. This key will be used to register the CTA and link it to your unique configuration. Retain this key as this will be used to register the CTA with the CTP registration servers.
- Registration Key Status: This column displays the status of your registration key. When configuration first completes, the registration key will show "Active", indicating the key is ready to be used. Registration keys are valid for a one-time use, or 30 days. If the key expires or needs to be reused, a Reactivate link will display in this table.

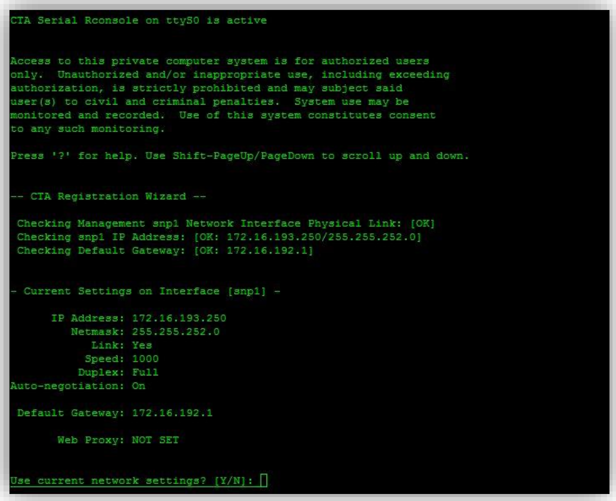
Once you have your registration key, proceed to the Using the Registration Wizard section.

Using the Registration Wizard

When connecting a monitor and keyboard to a CTA, you will be given access to a restricted shell called the Recovery Console. Prior to a CTA being registered, this console will display a Registration Wizard to the user. This wizard can be used to complete the registration process and establish a secure VPN connection back to SecureWorks, permitting further configuration and management of the device from SecureWorks CTOC. Note that you may need to press enter if no output is seen on the screen to wake the console.

By default, if the management interface is connected, the Registration wizard will:

- Obtain a DHCP IP address if a DHCP server exists on that network.
- Check if the supplied IP can be configured on the interface without an ARP conflict.
- Check if default gateway is reachable.
- It will display the result of these checks to the user, and prompt to either use the configured network settings, or change them.

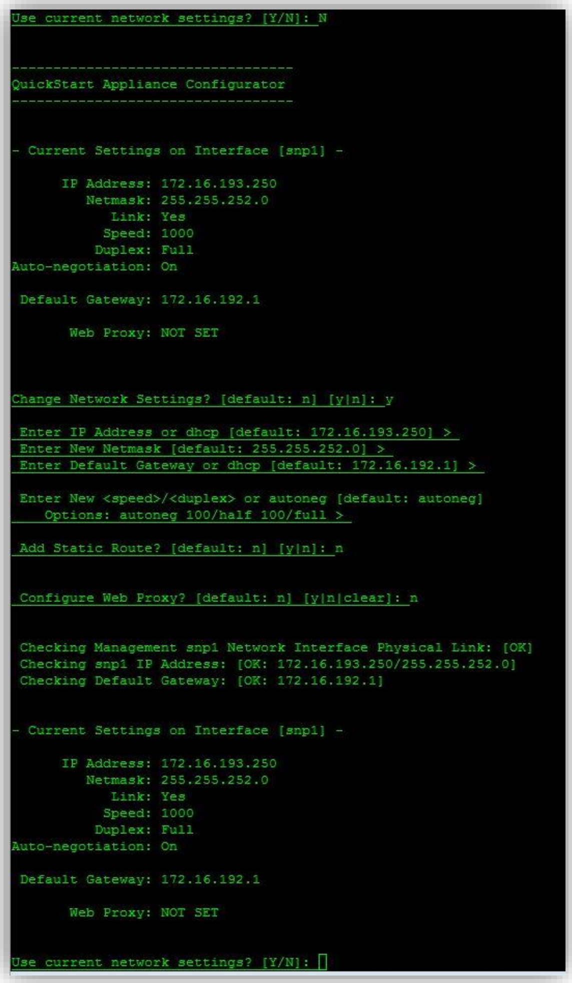


```
CTA Serial Rconsole on ttyS0 is active


Access to this private computer system is for authorized users
only.  Unauthorized and/or inappropriate use, including exceeding
authorization, is strictly prohibited and may subject said
user(s) to civil and criminal penalties.  System use may be
monitored and recorded.  Use of this system constitutes consent
to any such monitoring.

Press '?' for help. Use Shift-PageUp/PageDown to scroll up and down.


-- CTA Registration Wizard --

 Checking Management snp1 Network Interface Physical Link: [OK]
 Checking snp1 IP Address: [OK: 172.16.193.250/255.255.252.0]
 Checking Default Gateway: [OK: 172.16.192.1]


- Current Settings on Interface [snp1] -

      IP Address: 172.16.193.250
         Netmask: 255.255.252.0
            Link: Yes
           Speed: 1000
          Duplex: Full
Auto-negotiation: On

 Default Gateway: 172.16.192.1

       Web Proxy: NOT SET


Use current network settings? [Y/N]: 
```

If you wish to change the network settings enter N, press enter, and continue to step 3. Otherwise, press Y. The CTA will prompt you to enter your network settings.

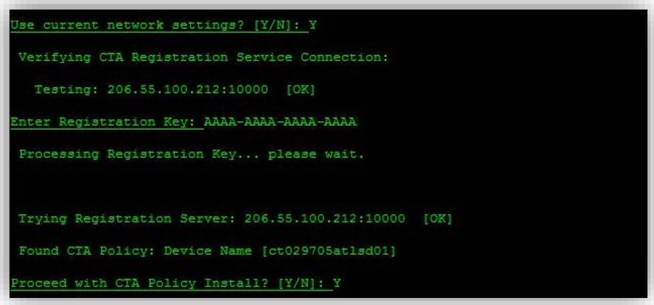
- IP address or DHCP configuration
- Netmask
- Default gateway
- Interface speed/duplex
- Any required static routes
- Utilization of a web proxy

Once these values are entered, the device will redirect back to the same 3 checks and prompt again if it should continue.



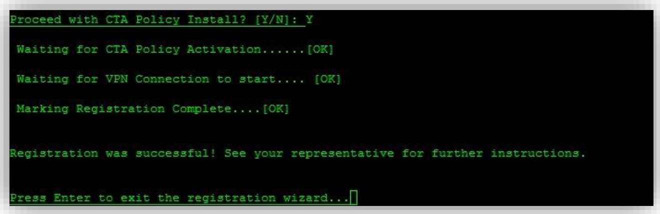
```
Use current network settings? [Y/N]: N


----------------------------------
QuickStart Appliance Configurator
----------------------------------


- Current Settings on Interface [snp1] -

      IP Address: 172.16.193.250
         Netmask: 255.255.252.0
            Link: Yes
           Speed: 1000
          Duplex: Full
Auto-negotiation: On

 Default Gateway: 172.16.192.1

       Web Proxy: NOT SET



Change Network Settings? [default: n] [y|n]: y

 Enter IP Address or dhcp [default: 172.16.193.250] >
 Enter New Netmask [default: 255.255.252.0] >
 Enter Default Gateway or dhcp [default: 172.16.192.1] >

 Enter New <speed>/<duplex> or autoneg [default: autoneg]
    Options: autoneg 100/half 100/full >

 Add Static Route? [default: n] [y|n]: n


 Configure Web Proxy? [default: n] [y|n|clear]: n


 Checking Management snp1 Network Interface Physical Link: [OK]
 Checking snp1 IP Address: [OK: 172.16.193.250/255.255.252.0]
 Checking Default Gateway: [OK: 172.16.192.1]


- Current Settings on Interface [snp1] -

      IP Address: 172.16.193.250
         Netmask: 255.255.252.0
            Link: Yes
           Speed: 1000
          Duplex: Full
Auto-negotiation: On

 Default Gateway: 172.16.192.1

       Web Proxy: NOT SET


Use current network settings? [Y/N]:
```

Using the configured network settings, the CTA will test its connectivity to the Secureworks registration servers. If this connection succeeds, you will be prompted to enter the registration key gathered in the previous section, “Obtaining a Registration Key”. Once the key is entered, the CTA will authenticate to the registration service and obtain the name of the device being registered, and prompt the user to continue with the policy installation from that device.



```
Use current network settings? [Y/N]: Y

 Verifying CTA Registration Service Connection:

   Testing: 206.55.100.212:10000  [OK]

Enter Registration Key: AAAA-AAAA-AAAA-AAAA

 Processing Registration Key... please wait.


 Trying Registration Server: 206.55.100.212:10000  [OK]

 Found CTA Policy: Device Name [ct029705atlsd01]

Proceed with CTA Policy Install? [Y/N]: Y
```

Once policy installation starts, the CTA will apply the policy configuration retrieved from the registration service and start its OpenVPN connection. Once connected via OpenVPN, the registration will be marked as complete, invalidating further uses of the registration key unless it is reactivated. Now that OpenVPN is connected, your Secureworks Secureworks representative can continue further setup of the device. The wizard will prompt the user to press any key to exit.



```
Proceed with CTA Policy Install? [Y/N]: Y

 Waiting for CTA Policy Activation......[OK]

 Waiting for VPN Connection to start.... [OK]

 Marking Registration Complete....[OK]


Registration was successful! See your representative for further instructions.


Press Enter to exit the registration wizard...
```

Appendix A: Recovery Console

Once your CTA is registered the Secureworks CTOC can connect remotely and configure, manage, and assist in troubleshooting the device using the VPN connection that was set up. However, should an issue occur with the VPN connection, or the device needs to be configured locally (for example, an IP change across subnets is required), the CTA will continue to provide a restricted shell known as the Recovery Console.

CLI Navigation

While using the Recovery Console CLI, you can use the **"?"** for help and listing of possible commands. You may use the **Shift-PageUp/PageDown** to scroll up and down the terminal as well. Tab can be used to auto-complete commands or show available options.

Help Examples:

```
CTA(ct012345atlsd02)-> ?

show                      Show Settings
run                       Execute Programs
exit                      Exit
clear                     Clear the Screen

CTA(ct012345atlsd02)->
CTA(ct012345atlsd02)-> show ?

arp                       Show the Arp Information
int                       Show Network Interface Configuration
route                     Show the Routing Information
system                    Show the System Information

CTA(ct012345atlsd02)->
```

Show Command

The **"show"** command can be used to show system and network information. The options for the show command are as follows.

Syntax: **show** [**arp**|**int** {snp1|snp2|snp3|snp4}|**route**|**system** {**health**}]

```
CTA(ct012345atlsd02)-> show ?

arp                       Show the Arp Information
int                       Show Network Interface Configuration
route                     Show the Routing Information
system                    Show the System Information

CTA(ct012345atlsd02)->
```

show arp

The “show arp” command is used to display the Address Resolution Protocol (ARP) table.

Syntax: show arp

```
CTA(ct012345atlsd02)-> show arp

Arp Table:

IP Addr         Iface HW Addr              NUD
-----------------------------------------------------------
123.123.123.62  snp1  00:00:0c:07:ac:e1    REACHABLE

CTA(ct012345atlsd02)->
```

show int

The “show int” command is used to display the interface(s) status as well as the VPN tunnel status used to communicate with the Secureworks CTOC. If you find that the management interface (snp1) is in a down state, please refer to the “Connectivity Requirements” section to determine if the correct interface has been connected to the network.

Syntax: show int <*snp1*|*snp2*|*snp3*|*snp4*> Network Interface Name (ie. snp1 which is the primary management interface)

```
CTA(ct012345atlsd02)-> show int

  snp1: UP      123.123.123.40 / 255.255.255.192   [1000Mb/s|Full AN=on]
  snp2: DOWN                   /
  snp3: DOWN                   /
  snp4: DOWN                   /

  vpn1: UP         10.1.1.43 / 255.255.255.255   [206.55.100.212 tcp/10000]


CTA(ct012345atlsd02)->
```

show route

The “show route” command is used to display the active entries in the routing table.

Syntax: show route

```
CTA(ct012345atlsd02)-> show route

Routing Table:

Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
-----------------------------------------------------------------------------
208.89.41.14    208.89.41.23    255.255.255.255 UGH   0      0        0 vpn1
208.89.41.15    208.89.41.23    255.255.255.255 UGH   0      0        0 vpn1
206.55.103.159  208.89.41.23    255.255.255.255 UGH   0      0        0 vpn1
206.55.101.159  208.89.41.23    255.255.255.255 UGH   0      0        0 vpn1
208.89.41.72    208.89.41.23    255.255.255.255 UGH   0      0        0 vpn1
208.89.41.74    208.89.41.23    255.255.255.255 UGH   0      0        0 vpn1
208.89.41.75    208.89.41.23    255.255.255.255 UGH   0      0        0 vpn1
208.89.41.68    208.89.41.23    255.255.255.255 UGH   0      0        0 vpn1
208.89.41.69    208.89.41.23    255.255.255.255 UGH   0      0        0 vpn1
208.89.41.23    0.0.0.0         255.255.255.255 UH    0      0        0 vpn1
208.89.41.70    208.89.41.23    255.255.255.255 UGH   0      0        0 vpn1
208.89.42.60    208.89.41.23    255.255.255.255 UGH   0      0        0 vpn1
206.55.101.50   208.89.41.23    255.255.255.255 UGH   0      0        0 vpn1
206.55.101.6    208.89.41.23    255.255.255.255 UGH   0      0        0 vpn1
63.239.86.129   208.89.41.23    255.255.255.255 UGH   0      0        0 vpn1
208.89.41.67    208.89.41.23    255.255.255.255 UGH   0      0        0 vpn1
208.89.42.48    208.89.41.23    255.255.255.248 UG    0      0        0 vpn1
123.123.123.0   0.0.0.0         255.255.255.192 U     0      0        0 snp1
208.89.43.0     208.89.41.23    255.255.255.0   UG    0      0        0 vpn1
208.89.44.0     208.89.41.23    255.255.254.0   UG    0      0        0 vpn1
0.0.0.0         123.123.123.62  0.0.0.0         UG    0      0        0 snp1

CTA(ct012345atlsd02)->
```

show system

The ”show system” command is used to show information pertaining to the system.

Syntax: show system [health]

```
CTA(ct012345atlsd02)-> show system

          CTA Model: 5104
            Version: 5.2.3

        Device Name: ct012345atlsd02
       CTA Hardware: PowerEdge R620
        Service Tag: ABCDE12
      Network Ports: 4
          Total RAM: 32 GB

CTA(ct012345atlsd02)->
CTA(ct012345atlsd02)-> show system health

Health

Main System Chassis

SEVERITY : COMPONENT
Ok       : Fans
Ok       : Intrusion
Ok       : Memory
Ok       : Power Supplies
Ok       : Power Management
Ok       : Processors
Ok       : Temperatures
Ok       : Voltages
Ok       : Hardware Log
Ok       : Batteries


CTA(ct012345atlsd02)->
```

Run Command

The **“run”** command is used to execute programs authorized through the Recovery Console session. The options for the run command are as follows.

Syntax:

```
CTA(ct012345atlsd02)-> run ?

hc                     Health Checker
ping                   Ping Remote Host
quickstart             Setup Program
reboot                 Reboot System
refresh                Refresh Data
shutdown               Halt the system in one minute
traceroute             Traceroute

CTA(ct012345atlsd02)->
```

run hc

The “run hc” command is used to execute the Health Checker program. Health Checker checks the status of the management interface (snp1) as well as the VPN tunnel to Secureworks CTOC.

Syntax: run hc

```
CTA(ct012345atlsd02)-> run hc

Checking Interface Status:

  snp1: UP      123.123.123.40 / 255.255.255.192   [1000Mb/s|Full AN=on]
  snp2: DOWN                   /
  snp3: DOWN                   /
  snp4: DOWN                   /

  vpn1: UP         10.1.1.43 / 255.255.255.255   [206.55.100.212 tcp/10000]


 VPN1 bound to active interface "SNP1": [OK]

Checking Default Gateway:

 Ping Test (icmp) to "123.123.123.62": [OK] (time: 0.55 ms)

Checking VPN Connection:

 vpn1: VPN tcp Connect 206.55.100.212:10000 [OK] (time=4430 ms)

Health Check Testing Finished.
CTA(ct012345atlsd02)->
```

run ping

The “run ping” command is used to execute the ping program for testing of connectivity.

Syntax: run ping <value> Remote Host IP Address

```
CTA(ct012345atlsd02)-> run ping 123.123.123.62
PING 123.123.123.62 (123.123.123.62) 56(84) bytes of data.
64 bytes from 123.123.123.62: icmp_seq=1 ttl=255 time=0.358 ms
64 bytes from 123.123.123.62: icmp_seq=2 ttl=255 time=0.336 ms
64 bytes from 123.123.123.62: icmp_seq=3 ttl=255 time=0.353 ms
64 bytes from 123.123.123.62: icmp_seq=4 ttl=255 time=0.340 ms
64 bytes from 123.123.123.62: icmp_seq=5 ttl=255 time=0.354 ms

--- 123.123.123.62 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.336/0.348/0.358/0.014 ms
CTA(ct012345atlsd02)->
```

run quickstart

The “run quickstart” command is used to initiate the network reconfiguration process. This command should only be used while working with the Secureworks CTOC to change the network configuration of the CTA. Changes made locally will be overwritten with the last known configuration saved by the Secureworks CTOC if the system detects that the running configuration is not that of the last known configuration saved by the Secureworks CTOC. See the QuickStart section of this guide for more information on using QuickStart.

Syntax: run quickstart

```
CTA(ct012345atlsd02)-> run quickstart
```

If it is desired to change the network configuration of the CTA, please refer to **“Using QuickStart”** for guidance.

run reboot

The “run reboot” command can be used to reboot the CTA.

Syntax: run reboot

```
CTA(ct012345atlsd02)-> run reboot
```

run refresh

The “run refresh” command is used to refresh the CLI data.

Syntax: run refresh

```
CTA(ct012345atlsd02)-> run refresh

Refreshed CLI.

CTA(ct012345atlsd02)->
```

run shutdown

The “run shutdown” command is used to gracefully shutdown/halt the system in one minute.

Syntax: run shutdown

```
CTA(ct012345atlsd02)-> run shutdown
```

run traceroute

The “run traceroute” command is used to execute the traceroute program for displaying the route (path) and measuring transit delay of packets to the specified destination. Below “vpn1” represents the primary access point in which the CTA terminates its VPN tunnel.

Syntax: run traceroute [<value>|vpn1|vpn2]

```
CTA(ct012345atlsd02)-> run traceroute 123.123.123.62
traceroute to 123.123.123.62 (123.123.123.62), 30 hops max, 60 byte packets
 1  123.123.123.61  1.755 ms  1.890 ms  2.034 ms

CTA(ct012345atlsd02)-> run traceroute vpn1

traceroute to 206.55.100.212 (206.55.100.212), 30 hops max, 52 byte packets
 1  * * *  0.315 ms  0.447 ms  0.614 ms
 2  * * *  0.999 ms  1.001 ms  0.994 ms
 3  * * *
 4  * * *  2.805 ms  2.798 ms  2.793 ms
 5  * * *  3.345 ms  3.347 ms  3.342 ms
 6  * * *  3.948 ms  3.513 ms  3.458 ms
 7  * * *  5.416 ms  5.049 ms  5.003 ms
 8  * * *
 9  * * *  114.332 ms  114.749 ms  114.758 ms
10  * * *  31.578 ms  31.882 ms  31.841 ms
11  * * *  90.439 ms  89.945 ms  89.932 ms
12  * * *
13  * * *
14  vsi-vpn.mss.secureworks.com (206.55.100.212) 31.834 ms 32.277 ms 32.250 ms

CTA(ct012345atlsd02)->
```

Additional Commands

exit

The “exit” command is used to exit the Recovery Console session.

clear

The “clear” command is used to clear the screen of its current content.

Using QuickStart

The **“run quickstart”** command is used to initiate the network reconfiguration process. This command should only be used while working with the Secureworks CTOC to change the network configuration of the CTA. Changes made locally will be overwritten with the last known configuration saved by the Secureworks CTOC if the system detects that the running configuration is not that of the last known configuration saved by the Secureworks CTOC.

Syntax: **run quickstart**

Type **“run quickstart”** to execute the QuickStart program.

Now enter the password provided to you by a member of Secureworks. When entering the password, stars will be displayed on the screen to mask the entered password. If you enter an incorrect password, re-run QuickStart before attempting to enter the password.

```
CTA(ct012345atlsd02)-> run quickstart

----------------------------------
QuickStart Appliance Configurator
----------------------------------

QuickStart Password> ********
```

- Upon entering the correct password, you will be asked to select an interface. To change the default management interface (snp1), type 1 and press enter. The current network information will be displayed.
- Type “**y**” and press enter to change the network configuration.

```
Select Network Interface Number [default: 1] [1-4] > 1

- Current Settings on Interface [snp1] -

      IP Address: 123.123.123.40
         Netmask: 255.255.255.192
            Link: Yes
           Speed: 1000
          Duplex: Full
Auto-negotiation: On

 Default Gateway: 123.123.123.62


Change Network Settings? [default: n] [y|n]: y
```

- Enter the new values for the IP Address, Netmask and Gateway, and press enter. The device will show that it has updated the values.

```
Enter New IP Address [default: 172.16.1.40] > 123.123.123.40
Enter New Netmask [default: 255.255.255.192] > 255.255.255.192
Enter New Default Gateway [default: 172.16.1.62] > 123.123.123.62
Enter New <speed>/<duplex> or autoneg [default: autoneg]
  Options: autoneg 100/half 100/full > autoneg

Updating IP Address and Netmask: [OK]

Updating Default Gateway: [OK]
```

Verify Configuration

Now that you have changed the network configuration, use the commands **“show int”**, **“show route”** and **“run hc”** to verify your configuration change.

Save Configuration

ATTENTION: QuickStart changes will **NOT** survive a reboot. To survive a reboot, Secureworks must save the configuration with the CTOC as the last known configuration. Please make sure this step has been completed or the CTA will roll back the last known network configuration.

Appendix B: Verification of Connectivity

This section can be used to validate the connectivity of the CTA to the Secureworks datacenters.

Method #1

CTA Connectivity can be verified via the Recovery Console. The Recovery Console is accessible on the CTA by connecting a monitor and keyboard to the system. Once you have connected a monitor and keyboard to the system you should see similar output as follows.

Note: You may need to press ENTER if there is no output present to wake the console.

```
CTA(ct012345atlsd02)->

Access to this private computer system is for authorized users
only.  Unauthorized and/or inappropriate use, including exceeding
authorization, is strictly prohibited and may subject said
user(s) to civil and criminal penalties.  System use may be
monitored and recorded.  Use of this system constitutes consent
to any such monitoring.


Press '?' for help. Use Shift-PageUp/PageDown to scroll up and down.



CTA(ct012345atlsd02)->
```

The **“run hc”** command is used to execute the Health Checker program. Health Checker checks the status of the management interface (snp1) as well as the VPN tunnel to Secureworks CTOC.

Syntax: **run hc**

```
CTA(ct012345atlsd02)-> run hc

Checking Interface Status:

  snp1: UP      123.123.123.40 / 255.255.255.192   [1000Mb/s|Full AN=on]
  snp2: DOWN                   /
  snp3: DOWN                   /
  snp4: DOWN                   /

  vpn1: UP         10.1.1.43 / 255.255.255.255   [206.55.100.212 tcp/10000]


 VPN1 bound to active interface "SNP1": [OK]

Checking Default Gateway:

 Ping Test (icmp) to "123.123.123.62": [OK] (time: 0.55 ms)

Checking VPN Connection:

 vpn1: VPN tcp Connect 206.55.100.212:10000 [OK] (time=4430 ms)

Health Check Testing Finished.
CTA(ct012345atlsd02)->
```

The above command allows for the following verification steps to be done:

1. Please ensure that the CTA has the correct IP address information.
2. If the IP address in not correct, this could cause the firewall to block the network traffic.
3. If the Ping Test fails (assuming gateway allows ping), it is most likely a layer two issue (mostly likely VLAN related).
4. If the Ping Test is successful, but the VPN Test fails this would indicate one or more of the following:
5. Firewall ports have not been opened
6. Another device between CTA and Secureworks Counter Threat Operations Center is blocking connection on port 10000

Method #2

1. Verify Connectivity to Counter Threat Operations Center
    a. On most firewalls, you should be able to use the source IP address of the CTA to view inbound and outbound communications from and to the device. You should be able to see the VPN connections specified in the "Connectivity Requirements" section of this guide. If the connections are not visible, this indicates that some appliance on your network is blocking the connections.

Method #3

To verify that all firewall requirements have been performed correctly, the following can be done:

1. Unplug CTA from network
2. Plug in a laptop to the port that was being used for the CTA
3. Give laptop same IP address information as CTA (flush ARP tables on network switches)
4. Ping local gateway assigned to the CTA
5. If ping is not successful, it is most likely a VLAN issue (assuming gateway allows ping)
6. Telnet to the Secureworks destination addresses and ports mentioned in the "Connectivity Requirements" section of this guide.
    a. If these tests are unsuccessful, it indicates that the proper network access has not been allowed.