V-Series Appliances A Visual Primer for the Version 8.3 CLI

Mapping the New Command Line Interface to the Previous V-Series Appliance Manager



Copyright © 2016 Forcepoint. All rights reserved. | 1

HOW TO MANAGE A V-SERIES APPLIANCE

Beginning with version 8.3, V-Series appliances are managed through an *enriched command-line interface (CLI) with interactive help*. This replaces the appliance console.

The CLI will remain in future versions, when a centralized appliance manager is added.



HOW TO MANAGE A V-SERIES APPLIANCE

This short presentation shows how to access the CLI, and *maps* the former single-appliance console to the new CLI commands.



3

TO ACCESS THE COMMAND LINE INTERFACE (CLI)

To manage the V-Series appliance with the CLI, select your preferred CLI access method, and then log on:

- Use PuTTY or similar tool on a Windows server (iTerm or similar on Mac) to access the CLI.
 - Connect to the IP address of the C interface
 - Use port 22
 - Select SSH (enabled by default)
 - Use your admin credentials to log on
 - You now have admin privileges

deper.		
tor Sensee	Basic options for your Pu	TT' income
Logging	Specify the Destructory play and 5	a talenament has -
2 Tenne	Hort Nate its IF address	Pot
Field Ref.	manufa card	1122
Fedure	Connection type Officer Officient Officien	@104 Ofe
Appearance Entenioz Turulation	Limit som o deble a doed ses Saved Sessers	-
Selector		in the second
to Comeriker	Dataut Serlings	Lost
Date		1.244
Pog		and the second second
Tehet		Dente
a 554 Send	Conversion on and Order on Chinese (2010)	nig on clean and
-		

• Or, attach a keyboard and monitor directly to the appliance.

	١
	ļ

- Or, connect to the appliance via serial port or KVM.
 - Serial port settings: 9600 baud, 8 bits, no parity

• Or, use the Virtual Console feature of the DELL Remote Access Controller (iDRAC).

After logon, for assistance with a specific CLI command, enter ? or type **help**. Use the **Tab key** for command completion.

HOW TO LOG ON TO CONTENT GATEWAY MANAGER

The new appliance logon page in Version 8.3 is used <u>only</u> to access Content Gateway Manager. To reach the Content Gateway logon page, open a browser. Enter the IP address of the C interface.

New Content Gateway logon page

marme: unity mod	UAV10k.forcepoint.com le: TRITON AP-WEB
Appliance	Management
Manage ti	e appliance with the command-line interface (CLI). Select an access method:
• Use	PuTTY or similar tool on Windows (iTerm or similar on Mac) to access thr CLI. • Connect to the IP address of the C interface
	Use port 22 Select SSH 9enabled by default)
	Use admin credentials set during firstboot
• Att	sch a keyboard and monitor directly to the appliance.
• Cor	nect to the appliance via serial port or KVM. • Serial port settings: 9600 baud, 8 bits, no parity
• Use	the Virtual Console feature of the DELL Remote Access Controller (iDRAC).
For assist	ance with specific CLI commands, see the CLI Golde
Content	iateway
Use the C	ontent Gateway Manager to configure Content Gateway settings for this appliance.

Former logon page

V5000 G3	Logon Portal
ostname: uaWeb.forcepoint.c	com
Appliance Manager	Appliance configuration and monitoring
Content Gateway Manager	Content Gateway settings and configuration
0	1996 - 2016 Forcepoint LLC

Content Gateway manager remains the same as in prior versions.

GETTING HELP WITH CLI COMMANDS

Use the **help** command to access CLI help information at any time.

- # help
- # help show
- # help show log

Use the **Tab key** to auto-complete command words, or to display a list of available words or phrases to complete a command.

Use the question mark (?) to display help information for the current command path <u>without</u> pressing Enter and without losing the current input.

```
# ?
# show ?
# show system ?
```

Use the up arrow key to display the previous command.

CLI MODES

The CLI has 3 modes. You start out in view mode.

- view displays status and settings. Also accesses the other 2 modes.
- config (contains all view commands) changes settings and enables/disables options
- diagnose performs troubleshooting; handles system and network test commands

Mode selection

- > To move to config mode: (view) # config (re-enter admin password)
- To move to diagnose mode: (view) # diagnose
- > To return to view mode: (config)# exit or (diagnose)# exit
- > To exit from the CLI: (view)# exit
- > You cannot move from **config** directly to **diagnose** or vice versa.

To bump another admin

- Only one admin can work in **config** mode at a time.
- To bump the admin who is currently working in **config** mode: (view)# clear session --config
- This moves that person to **view** mode.

CLI PASSWORD

To change the password for the admin account, you need the current one.

(config)# set account admin --password

Password requirements

Must be 8 to 15 characters in length and include: At least one uppercase character At least one lowercase character At least one number At least one character in this set:

(! # % & ' () * + , - . / ; < = > ? @ [] ^ { | } ~

Password recovery options

Go to <u>http://www.forcepoint.com</u> and select **Documentation > Forcepoint Appliances**.

See the CLI Guide section on Basic account management.

MAPPING THE V-SERIES MANAGER TO THE NEW CLI



A complete *CLI Guide* is online.

STATUS > GENERAL

General

Appliance status

(config)# show appliance status
(config)# show email
(config)# show network-agent
(config)# show proxy
(config)# show web

Appliance restart / shutdown

(config)# restart appliance
(config)# shutdown appliance

Module restart

(config)# restart email

- (config)# restart network-agent
- (config)# restart proxy
- (config)# restart web



STATUS > GENERAL (continued)

General

Module Stop / Start

(config)# stop email
(config)# start email

(config)# stop proxy

(config)# start proxy

(config)# stop web

(config)# **start web**

(config)# stop network-agent

```
(config)# start network-agent
```

ORCEPOINT V	000 63	Hostname: uaWeb.forcepoint.com 🌐 Log of
	General General	?нер -
Status General CPU and Memory Disk Usage	Alerts We also also also also also also also also	Appliance Controller (7 Resources Used: CPU: 1 Dece
Vetwork Bandwidth	n	Roun, Lask ver Interface(s): ⊘ C (claared) Restart Appliance Shut Down Appliance
ietwork Interfaces Routing Alerting	Content Gateway	Monitor status without timing out
Meb Components Administration Patches / Hotfwes Backup Utility Logs Toobox	Resources Used: CPU(0): 4 RAM: 5-70 GB Interface(0): ØP1 (dedicated) P2 (dedicated) ØP2 (dedicated) ØP2 (shared)	Services: Content Cop Content Cateway Content Cateway Manager Stop Services
locount Management	TRITON AP-WEB	Ű
	Resources Used: CPU(0): 2 RAVI: 5.79 GB Interface(s): C (chared)	Services Griffering Service Policy Database Policy Server User Service Directory Agent State Server Multiplicer Usage Monitor Control Service
	Restart	stop services

STATUS > CPU AND MEMORY / DISK USAGE / BANDWIDTH

CPU and Memory
(config)# show cpu
use Ctrl+C to quit
(config)# show mem
use Ctrl+C to quit

Disk usage

(config) # show diskio
offers a choice of modules

(config) # show diskspace
shows all partitions

Network bandwidth

(config) # show bandwidth

shows each enabled interface; updates every 5 seconds; use Ctrl+C to quit



CONFIGURATION > SYSTEM / TIME / DATE / HOST / DESCRIPTION 13

Stop all services before you reset system time and date. See slide 10.

```
(config)# show appliance info
```

```
(config)# show system timezone
(config)# set system timezone
--zone <zone_name>
--index <zone_index>
```

```
(config)# show system ntp
(config)# set system ntp
--status <on|off>
(config)# set system ntp
--server <server1>, <server2>,<server</pre>
```

```
(config)# show system clock
(config)# set system clock
--date <yyyy/mm/dd>
--time <hh:mm:ss>
```

```
(config)# show system host
(config)# set system host
--name <name>
--description <description>
```



CONFIGURATION > NETWORK INTERFACES (IPV4)

Show current interface for one module

(config)# show interface info [--module <app | email | proxy web | network-agent>]

Show unused physical interfaces

(config)# show interface unused

Enable or Disable an interface

(config) # set interface status --interface <e2 | p2 > < --enabled | --disabled >

Configure IPv4 interfaces

```
(config)# set interface ipv4
 --interface <c|n|p1|p2|e1|e2>
--ip <ipv4 address>
[--mask <ipv4_netmask>]
 --gateway <ipv4 address>
```

```
(config)# delete interface ipv4
--interface <n|p1|p2|e1|e2>
--status <enabled|disabled>
```

FORCEPOINT V50	00 G3				Hostname: uaWeb.forcepoint.	.com 🍈	Log Off
« Status ^	Network Interface	s				? Help) ~
General	Content Gateway	Interfaces (P1 and P2)					(i
CPU and Memory Disk Usage	Proxy interface fo	inbound (user requests) a	nd outbound (con	nmunication with	Internet).		
Network Bandwidth	Select interfaces l	eing used:					
Configuration ^	O P1 and P2						
System	MAC Address:	00:0A:F7:82:8F:F4					
Network Interfaces	IP Address:	10.0.0.3	Primary DNS:				
Alerting	Subnet Mask:		Secondary DNS	:	optional		
Web Components	Default Gatewa	r:	Tertiary DNS:		optional		
Backup Utility Logs Toolbox Account Management	IP Address: Subnet Mask: Network Agent II Network Agent ini	iterface (N) erface monitors all Interne n-HTTP/HTTPS traffic.	t traffic in the netv	work, reports on I	bandwidth usage and send	s blocking	(î)
	Send blocking info	rmation for non-HTTP/HTTP	S traffic via:				
	Interface C T Interface N M	ne C interface must be able t ust be connected to a bidired	o access the client. ctional span port	s' network.			
	MAC Address:	00:16:3E:36:D4:6A					
	IP Address:	10.0.0.5	Primary DNS:				
	Subnet Mask:	255.255.255.255	Secondary DNS:		optional		
	Default Gateway:		Tertiary DNS:		optional		
	L						
					ОК	Cano	el

CONFIGURATION > NETWORK INTERFACES (IPv4 continued)

General

CPU and N

Disk Usage Network E

🗙 Config

System Network

Routing Alerting Web Com

🙆 Admin

Patches / Backup Ut

Account N

Logs Toolbox

Configure appliance DNS settings

(config)# set interface dns

- [--dns1 <ipv4_address>]
- [--dns2 <ipv4_address>]
- [--dns3 <ipv4_address>]

[--module <email|network-agent|proxy>]
Omit module if configuring appliance DNS

Delete appliance DNS settings

(config)# delete interface dns

[--dns-server <dns2 | dns3 >]

[--module <email | network-agent | proxy>]
Omit module if deleting appliance DNS

Display bonded interfaces

(config)# show interface bond
Bond interfaces

(config)# set interface bond

[--mode <active-standby |load-balancing>]

Remove bonding

(config)# set interface unbond

POINT V5	000 G3		Hostname	: uaWeb.forcepoint.com	n ())	Log Off
;	Network Interfaces				? Help	~
	Content Gateway Interfaces (P1 and P2)					(i)
lemory	Proxy interface for inbound (user requests) a	and outbound (com	munication with Internet)			
andwidth	Select interfaces being used:					
uration	P1 and P2					
	MAC Address: 00:0A:F7:82:8F:F4					
Interfaces	IP Address: 10.0.0.3	Primary DNS:]		
	Subnet Mask:	Secondary DNS:		optional		
oonents	Default Gateway:	Tertiary DNS:		optional		
ictration	P2					
Istation	MAC 00:0A:F7:82:8F:F5					
HOTTIXES	IP					
inc y	Address:					
	Mask:					
lanagement						
	Network Agent Interface (N)					(i)
	Network Agent interface monitors all Interne	t traffic in the netw	ork reports on bandwidtl	usade and sends bl	ockina	
	information for non-HTTP/HTTPS traffic.		ond, reports on bundwidd	rusuge and senas bi	ocking	
	Send blocking information for non-HTTP/HTTP	S traffic via:				
	Interface C The C interface must be able	to access the clients	' network.			
	Interface N Must be connected to a bidire	ctional span port				
	MAC Address: 00:16:3E:36:D4:6A					
	IP Address: 10.0.0.5	Primary DNS:				
	Subnet Mask: 255.255.255.255	Secondary DNS:		optional		
	Default Gateway:	Tertiary DNS:		optional		
				ОК	Cance	el

CONFIGURATION > NETWORK INTERFACES (IPv6)

🔕 Adr

IPv6 interfaces

```
(config)# set interface ipv6
--interface <c|n|p1|p2|e1|e2>
[--status <enabled | disabled>]
[--ip <ipv6 address>]
[--prefixlen <integer>]
```

```
[--gateway <ipv6_address>]
```

```
(config)# delete interface ipv6
 --interface <c|n|p1|p2|e1|e2>
```

DNS settings configured for IPv4 are automatically applied

TRITON AP-EMAIL does not support IPv6

FORCEPOINT V50)00 G3		Hostname: uaWeb.forcepoint.com		Log Off
~	Network Interfaces			? Help	
Status ^ General CPU and Memory Disk Usage Network Bandwidth	IPv4 IPv6 Networking: Disable Enable Appliance Controlle	IPv6 r Interface (C)			(i)
Configuration System Network Interfaces Routing Alerting Web Components	Configure IPv6 addr MAC Address: IPv6 address: Subnet prefix length Default Gateway:	essing for the C inter	face. DNS settings configured for IPv4 are automatically applied.		
Administration ^	Content Gateway In	nterface (P1)			í
Patches / Hotfixes Backup Utility Logs Toolbox Account Management	Configure IPv6 addr P1 MAC Address: IPv6 address: Subnet prefix leng Default Gateway: To configure IPv6 for	essing for the P1 inte	rfaces. DNS settings configured for IPv4 are automatically applied.		
	Network Agent Inte	erface (N)			í
	Configure IPv6 addm Send blocking inform Interface C The Interface N Mus MAC Address: IPv6 address: Subnet prefix length Default Gateway:	essing for the N inter Nation for non-HTTP/H C interface must be al t be connected to a bio	face. DNS settings configured for IPv4 are automatically applied. ITTPS traffic via : ble to access the clients' network. directional span port		
		_	ОК	Cance	el

CONFIGURATION > ROUTING (STATIC IPV4)

Display a table of configured static IPv4 routes

(config)# show route

Add a static route in IPv4 format

(config)# set route

--dest <ipv4_address> --interface <c|p1|p2|e1|e2> --mask <ipv4_netmask> --gateway <ipv4_address>

Delete a single IPv4 static route

(config) # **delete route**

- --dest <ip_address>
- --mask <ipv4_netmask>
- --interface <c|p1|p2|e1|e2>
- --gateway <ipv4_address>

FORCEPOINT V50	00 G3				Hostnam	e: uaWeb.forcepoint.com		Log Off
« Status ^	Routing						?	Help -
General CPU and Memory Disk Usage	IPv4 Static IPv4 Routes	IPv6						
Network Bandwidth	Manage static IPv4 corresponding serv	routes for all app rices.	liance interface	es. When a rou	ite is added/imported	or deleted, restart the	compon	ent's
X Configuration	Destination	on Network	Subnet Mask		Gateway	Interface		
System Network Interfaces	Export Table					Add/Imp	ort	Delete
Routing	Component Routes	5						
Alerting Web Components	Configure traffic be route is added or d	tween component leleted, restart the	s and various component's	hosts to be ro corresponding	uted through the Appli services.	ance Controller interfac	ce (C). V	Vhen a
Administration ^	Module			Destination Net	work	Subnet Mask		
Patches / Hotfixes Backup Utility							Add	Delete
Logs								
Toolbox								
Account Management								

CONFIGURATION > ROUTING (Static IPv4 continued)

Export IPv4 static routes

Do these in sequence shown: 1. Define a remote storage location: (config)# set filestore --alias <alias_name> --type <ftp|samba|tftp> --host <ip_address> --path <share_directory> [--user <user_name>] [--port <port>]

2. Export all IPv4 static routes
(config)# save route
--location <filestore_alias>

Note: To export IPv6 static routes, set up a filestore alias_name and then (config)# save route6 --location <filestore_alias>

FORCEPOINT	V50	00 G3				Hostn	ame: uaWeb.forcepoint.com		Log Off
Ctatus	**	Routing						?	Help -
General	~	IPv4	IPv6						
CPU and Memory		Static IPv4 Rout	es					_	
Disk Usage Network Bandwidth		Manage static IP corresponding se	v4 routes for all a rvices.	ppliance interfa	ces. When a rou	ite is added/importe	d or deleted, restart the	compon	ent's
X Configuration	^	Destina	tion Network	Subnet Mask		Gateway	Interface		
System Network Interfaces		Export Table					Add/Imp	ort	Delete
Routing		Component Rout	es						
Alerting Web Components		Configure traffic l route is added or	oetween compon deleted, restart	ents and various the component's	s hosts to be ro s corresponding	uted through the Ap services.	pliance Controller interfac	:e (C). V	Vhen a
Administration	^	Module			Destination Net	work	Subnet Mask		
Patches / Hotfixes								Add	Delete
Backup Utility									
Logs									
Toolbox									
Account Management									

CONFIGURATION > ROUTING (Static continued)

Add or delete one or more IPv4 static route definitions via a text file

load route

- --file <file_name>
- --location <filestore_alias>
- --action <add|del>

(Web only) Add or delete one or more IPv6 static route definitions via a text file

```
load route6
--file <file_name>
--location <filestore_alias>
```

```
--action <add|del>
```

FORCEPOINT V50	00 G3				Hostnam	e: uaWeb.forcepoint.com		Log Off	
« Status ^	Routing		_				?	Help -	
General CPU and Memory	IPv4 Static IPv4 Rou	IPv6							1
Disk Usage Network Bandwidth	Manage static IF corresponding s	v4 routes for all ap ervices.	pliance interfac	es. When a rou	te is added/imported o	or deleted, restart the co	ompon	ent's	
X Configuration ^	Destin	ation Network	Subnet Mask		Gateway	Interface			
System Network Interfaces	Export Table					Add/Impo	rt	Delete	
Routing	Component Rou	tes							L
Alerting Web Components	Configure traffic route is added o	between compone r deleted, restart ti	nts and various he component's	hosts to be ro corresponding	uted through the Appli services.	ance Controller interface	(C). V	/hen a	
Administration ^	Module	2		Destination Net	work	Subnet Mask			
Patches / Hotfixes						4	\dd	Delete	
Backup Utility									1
Logs									
Toolbox									
Account management									

CONFIGURATION > ROUTING (Component IPv4)

Show table of configured component routes

(config)# show component_route

Configure traffic from appliance component to be routed through the C Interface. Dest is the subnet address for which traffic will be routed.

(config)# set component_route
 --dest <ipv4 address>

--mask <ipv4_netmask>

--module <proxy | email>

Delete routing between appliance component and C interface.

```
(config)# delete component_route
--dest <ipv4_address>
--mask <ipv4_netmask>
--module <proxy|email>
```

FORCEPOINT V50)00 G3					Ho	stname: ua	Web.forcepoint.com		Log Off	
X Status	Routing								?	Help -	
General	1	Pv4	IPv6								
CPU and Memory	Static II	Static IPv4 Routes									
Disk Usage Network Bandwidth	Manage correspo	static IPv4 onding serv	routes for all app ices.	liance interfa	ces. When a ro	ute is added/impo	rted or de	leted, restart the o	ompon	ent's	
X Configuration		Destinatio	n Network	Subnet Mask		Gateway		Interface			
System	Expo	rt Table						Add/Impo	rt	Delete	
Network Interfaces											
Routing	Compon	ent Routes									
Alerting Web Components	Configur route is	e traffic bei added or d	tween component eleted, restart the	s and various component'	hosts to be ro corresponding	uted through the g services.	Appliance	Controller interface	e (C). V	When a	
Administration ^		Module			Destination Net	work		Subnet Mask			
Patches / Hotfixes									Add	Delete	
Backup Utility											
Logs											
Toolbox											
Account Management											

CONFIGURATION > ALERTING SETUP (Monitoring)

Display SNMP monitor server information
(config)# show snmp config

Enable or disable SNMP monitoring

(config)# set snmp service

--status <on|off>

Configure SNMP v1 monitoring

(config)# set snmp v1
 --community <name>

Configure SNMP v2c monitoring

(config)# set snmp v2c

--community <name>

See the CLI Guide for full details about SNMP v3 monitoring

FORCEPOINT V50	00 G3			Hostname: ua	Web.forcepoint.com		Log Off
«	Alerting			_		? H	elp -
Status ^	Setun	Alerts					
General	octop	Acto					
CPU and Memory	SNMP						
Disk Usage Notwork Pandwidth	Monitoring Server						
Network bandwidth	Monitor standard SN	IMP counters on the app	ance using your organizatio	n's SNMP server.			
X Configuration	Off						
System	O On						
Network Interfaces	SNMP version:	VI 🗸					
Routing	Community nam	e:					
Alerting							
Web Components	Trap Server						
Administration	Send traps (alerts) f	from the appliance to you	SNMP server. Use the appl	iance <u>MIB file</u> for t	rap interpretation.		
	Off						
Patches / Hottixes	⊖ On						
Logs	SNMP version:	VI V					
Toobox	Community nam	e.					
Account Management	TD addresses		Burti (100				
	IP address:						
		Send Test Trap					
					OK	Ca	ncel

CONFIGURATION > ALERTING SETUP (SNMP Traps)

Display SNMP trap server status and version
(config)# show trap config

Display table of SNMP trap events and settings
(config)# show trap events

Save SNMP trap events settings for editing or use

1. Define a remote storage location: (config)# set filestore --alias <alias_name> --type <ftp|samba|tftp> --host <ip_address> --path <share_directory> [--user <user_name>] [--port <port>]

2. Save trap settings (config)# save trap --location <filestore_alias> [--default]

FORCEPOINT V5	000 G 3					Hostname: ua	Web.forcepoint.com	•	Log Off
Ktatus (Alerting			_	_	_		?	-lelp
General	Setup	Alerts							
CPU and Memory	SNMP								
Disk Usage	Monitoring Server								
Network Bandwidth	Monitor standard SI	NMP counters on the app	liance usir	g your orga	anization's S	NMP server.			
Configuration	 Off 								
System	O On								
Network Interfaces	SNMP version:	VI 💙							
Routing	Community nam	ne:	_						
Alerting	· · · · · · · · · · · · · · · · · · ·								
Web Components	Trap Server								
	Send traps (alerts)	from the appliance to yo	ur SNMP se	erver. Use t	he appliance	<u>MIB file</u> for t	rap interpretation.		
Administration	 Off 								
Patches / Hotfixes	On								
Backup Utility	SNMP version	VI V							
Toobox			_						
Account Management	Community nam	ie:							
-	IP address:		Port:	162					
		Send Test Trap							
						_	ОК	6	ancel

CONFIGURATION > ALERTING SETUP (SNMP Traps continued)

Enable or disable SNMP traps

(config)# set trap service

--status <on|off>

Load SNMP trap events settings from a file (config)# load trap

--location <filestore_alias>

--file <name>

Send a test trap to verify communication (config)# test trap event

Configure SNMP v1 traps for alerting

(config)# set trap v1

- --community <name>
- --ip <ip_address>
- --port <port>



FORCEPOINT V50	100 G3			Hostname: uaV	Veb.forcepoint.com		Log	m
«	Alerting					?	Help	v
Conorol	Setup	Alerts						
CPU and Memory Disk Usage Network Bandwidth	SNMP Monitoring Server Monitor standard SNMP	P counters on the applia	nce using your organization's	s SNMP server.				7
System Network Interfaces	On SNMP version:	V1 V	_					
Alerting Web Components	Community name:							
Administration ^ Patches / Hotfixes Backup Utility	Send traps (alerts) from Off On	m the appliance to your :	SNMP server. Use the appliar	nce <u>MIB file</u> for tra	ap interpretation.			
Logs Toolbox Account Management	SNMP version: Community name: IP address:		Port: 162					
		Send Test Trap						
					ок	(ancel	

ADMINISTRATION > PATCHES

24

Display available appliance upgrades

(config)# **show upgrade**

- --list
- --history
- --status

Download or upload an upgrade file

(config)# load upgrade

[--file <filename>]

[--location <file location>]

Run without parameters to see a list of choices

Display status of upgrade file download (config)# show download

--file <filename>

Cancel, pause, resume download

(config)# cancel download

--file <filename>

(config)# pause download

--file <filename>

(config)# resume download

--file <filename>

Install upgrade file

(config)# install upgrade

--file <upgrade_file> [--force <upgrade_file]</pre>

ORCEPOINT V50	100 G3			Hostname: uaWeb.forcepoint.com	Log Off			
« Status ^	Patches / Ho	otfixes			? Help -			
General	Patche	es Hotfixes	Proxy Settings					
CPU and Memory	Patch Upgr	ades						
Disk Usage Network Bandwidth	Download a The applian	Download and install available patches to ensure that the appliance is updated with the latest software. The appliance automatically checks for patches once a day.						
Configuration ^	Appliance cu	urrent version: 8.2.0						
System	Available pa	atches:						
letwork Interfaces	Version No patche.	Description s available,		Status	Action			
Routing Alerting	Check	for Patches Last updated: /	(i) Upload Pa	tch Manually				
Web Components	Patch Histo	лү						
Administration ^	Version	Date	Comments		Log Files			
Patches / Hotfixes	8.1.0	Apr 13, 2016 17:03:41	Patch has been installed successfully.		<u>View log</u>			
Backup Utility								
Logs								
Loolbox								
Account management								

ADMINISTRATION > HOTFIXES

View available appliance hotfixes

(config)# show hotfix list

[--id <hotfix_id>] [--module <app|web|proxy|email>]

Download or upload a hotfix to appliance

(config)# load hotfix

- --id <hotfix id>
- --file <name>
- --location <alias>

Display status of hotfix download

(config)# show download hotfix

--file <filename>
--id <hotfix id>

Show hotfix history

(config)# show hotfix history

FORCEPOINT V50	00 G3			Hostname: uaWel	.forcepoint.com ()) Log Off			
«	Patches / Hotfixes				? Help -			
Status ^								
General	Patches	Hotfixes	Proxy Settings					
CPU and Memory	Hotfix Installation							
Disk Usage Network Bandwidth	Locate a hotfix to download and install on the appliance.							
Configuration	Describer de dibertéries							
System	Downloaded hotfixes:							
Network Interfaces	Hotfix ID D	escription		Status	Action			
Routing	No notrixes available.			0	Line of Lintée Menuelle			
Alerting				(I)				
Web Components	Hotfix History							
Administration ^	Manage installed hotfi	kes and view unins	talled hotfixes for the	current appliance version.				
Patches / Hotfixes	Appliance Version: 8.2	.0						
Backup Utility	Manuel Installed hotfixes	\sim						
Logs	VIEW: Installed Houlikes	•						
Toolbox	Hotfix ID +	Name •	Module	Date Installed	Status +			
Account Management	No hotfixes installed.							
					Uninstall Hotfix			

ADMINISTRATION > HOTFIXES (Continued)

Stop, pause, or resume download (config)# cancel download hotfix [--id <id>] [--file <filename>] (config)# pause download hotfix [--id <id>] [--file <filename>] (config) # resume download hotfix [--id <id>] [--file <filename>] Install hotfix (config)# install hotfix [--id <hotfix id>] Remove hotfix

```
(config)# delete hotfix
  [--id <id>]
  [--file <filename>]
```

Uninstall hotfix

(config)# uninstall hotfix [--id <hotfix id>]

ORCEPOINT V500	0 G3				Hostname: uaWe	b.forcepoint.com		Log O	ff
Status ^	Patches / Hotfixes						?	Help	~
General	Patches	Hotfixes	Proxy Settings						
CPU and Memory	Hotfix Installation								
Disk Usage Network Bandwidth	Locate a hotfix to download and install on the appliance.								
Configuration									
System	Downloaded hotfixes	:		0			_		
Network Interfaces	No hotfixes available			36	atus	ACUO	1		
Routing Alerting	Upload Hotfix Manually								
Web Components	Hotfix History								
Administration ^	Manage installed hot	fixes and view uninst	alled hotfixes for th	e current appliar	nce version.				
Patches / Hotfixes	Appliance Version: 8.	2.0							
Backup Utility Logs	View: Installed hotfixe	s 🗸							
Foolbox	Hotfix ID +	Name +	Modu	e •	Date Installed 🔻	Status +			
Account Management	NO NOLTIXES INSTAILED					Į	Jninstall	Hotfix	

ADMINISTRATION > PROXY SETTINGS

Display the current internet proxy information

(config)# show internet_proxy

Configure the proxy interface that the appliance will use to contact Forcepoint servers for hotfixes and upgrades

(config)# set internet proxy

- --ip <ip address>
- --port <port>
- [--user <username>]
- [--password <password>]

Delete the current internet proxy information

(config)# delete internet_proxy

FORCEPOINT V50	00 G3			Hostname: ua	Web.forcepoint.com	Log Off
Status ^	Patches / Hotfixes	Hotfixes	Provy Settings	1		?Help -
General CPU and Memory Disk Usage	Proxy Settings	Tiotixes	Troxy Security			
Network Bandwidth	If the appliance manag and download hotfixes,	ement interface (C) /patches.	does not have a dire	ect Internet connection, a pro	xy server can be use	ed to check for
X Configuration ^ System	 Use proxy server Proxy IP address: 		Port: 8080			
Network Interfaces Routing Alerting	User name: Password:		optional			
Web Components		Test Connection				
Administration Administration Patches / Hotfixes						
Backup Utility Logs						
Account Management						
			_		ОК	Cancel

ADMINISTRATION > BACKUP UTILITY

View available backups

(config)# **show backup list** --location

<local | filestore_alias>

Display configured backup schedule (config)# show backup schedule

Create a full appliance backup now

1. Define a remote storage location: (config)# set filestore --alias <alias_name> --type <ftp|samba|tftp> --host <ip_address> --path <share_directory> [--user <user_name>] [--port <port>] 2. Create backup (config)# create backup now

```
<local | filestore_alias>
```

```
[--desc "<description>"] --type <full|email|web>
```

CEPUINT VSC	00 G3		Hostname: uaW	eb.forcepoint.com				
«	Backup Utility			? Help				
eral	Backup Restore							
nd Memory	Perform Backup							
Jsage ork Bandwidth	Run the Backup Utility now or schedul all appliance settings, as well as confi do not include Content Gateway. To p	e backups to be performed or guration and policy informatio erform backups for Content G	n a regular basis. A Full Appl n for all active components. ateway only, Use <u>Content (</u>	iance Configuration backup sav Component configuration back Gateway Manager .				
onfiguration ^	Backup Type	Schedule Frequency	Last Scheduled Backup	Next Scheduled Backup				
m	Full Appliance Configuration	Not scheduled	Not scheduled	Not scheduled				
ork Interfaces	O Web Configuration	Not scheduled	Not scheduled	Not scheduled				
ing	Run Backup Now	Configu	Configure Backup Schedule					
Components	Local Backup Files							
dministration ^	Manage all backup files stored on this	appliance.						
ies / Hotfixes	View backups for: Full Appliance Con	figuration 🗸						
up Utility	Date File name	Ve	ersion Backup source	Comments				
	No backup file found.							
unt Management	Maximum of 20 full appliance configuration backup files Delete							
ane Managemente								

ADMINISTRATION > BACKUP UTILITY (continued)

Define a schedule of automated backups

(config)# create backup schedule

--location

<local|filestore_alias>

--freq

<daily|weekly|monthly>

--day <Mon|Tue|Wed|Thu|

Fri|Sat|Sun>

--date <integer>

--time <hh:mm>

--type <full|web|email>

Cancel all scheduled backups (config)# cancel backup schedule

Delete all backup files in a specific location or delete one file

(config)# **delete backup**

[--file <file_name|all>]

FORCEPOINT V50	00 G3				Hostname: ua\	Web.forcepoi	nt.com 🌐	Log Off	
General CPU and Memory CPU and	Backup Utility Backup Perform Backup	Restore					1	}Help ∽	
Disk Usage Network Bandwidth	Run the Backup Utility now or schedule backups to be performed on a regular basis. A Full Appliance Configuration backup saves all appliance settings, as well as configuration and policy information for all active components. Component configuration backups do not include Content Gateway. To perform backups for Content Gateway only, Use <u>Content Gateway Manager</u> .								
X Configuration ^	Backup Type		Schedule Frequency	Last	Scheduled Backup		Next Schedule	d Backup	
System Network Interfaces	 Full Appliance Web Configura 	Configuration tion	Not scheduled Not scheduled	Not scheduled		1	Not scheduled Not scheduled		
Routing Alerting Web Components	Run Backup No	Run Backup Now Configure Backup Schedule Cancel Scheduled Backup						łackup	
Administration ^	Local Backup File	s files stored on this app	liance.						
Patches / Hotfixes	View backups for:	Full Appliance Configura	tion 🗸						
Backup Utility Logs	Date	File name		Version	Backup source	ce Comments			
Toolbox Account Management	Maximum of 20 full appliance configuration backup files Delete							Delete	

ADMINISTRATION > RESTORE

30

Restore appliance settings saved in a specific backup file (config)# restore backup --location <local | filestore_alias> [--file <file_name>] Omit the --file parameter to see a list of choices

FORCEPOINT V50)00 G3			Hostname: uaWe	b.forcepoint.com		Log Off	l
General CPU and Memory Disk Usage Network Bandwidth	Backup Res Backup Res Restore your module or full appli Content Gateway configuration. Select restore mode: Select restore mode:	store iance configu	ration from an existing ba	nckup file. Use <u>Content Gate</u>	away Manager to	? resto	Help -	r
System Network Interfaces Routing Alerting Web Components	Full Appliance Configuration Web Configuration Run Restore Wizard							
Administration Patches / Hotfixes Backup Utility Logs Toolbox Account Management								

ADMINISTRATION > LOGS & CONFIGURATION SUMMARY

Create a configuration summary for Technical Support analysis

1. Define a remote storage location: (config)# set filestore --alias <alias_name> --type <ftp|samba|tftp>

--host <ip_address>

--path <share_directory>

[--user <user_name>]

[--port <port>]

2. Create configuration summary

(config)# save configsummary

--location

<filestore_alias>

Display a list of log file types

(config)# show log typelist

--module <app|all>]

App means list the file types for the entire appliance. All means list file types for the modules.

FORCEPOINT V50	00 © 3 Hostname: uaWeb.forcepoint.com		Lo	g Off
~	Logs	?	Help	~
💹 Status 🔷 ^				-
General CPU and Memory Disk Usage Network Bandwidth Configuration ^ System Network Interfaces Routing Alerting Web Components	Logs Forcepoint Technical Support may request log files to assist you with unexpected results. Select Module: Appliance Controller Content Gateway TRITON AP-WEB Network Agent View options: Image: 11/14 - Present v View options: Image: Image: <th></th> <th>Subm</th> <th>(i) hit</th>		Subm	(i) hit
Administration Administration Patches / Hotfixes Backup Utility Logs Toolbox Account Management				

ADMINISTRATION > LOGS (continued)

Display last "n" lines of the appliance log file

(config)# show log lastline

--line <integer>

```
--type <audit|module|system>
```

--module <app|email|proxy|

web|network-agent>

Display data as it is appended to the appliance log file

(config)# show log realtime

--filter <string>

--type <audit|module|system>

--module <app|email|proxy|web|

network-agent>

--timeout <integer>

FORCEPOINT V50	000 G3	Hostname: uaWeb.forcepoint.com	Log Off
() Ctature	Logs		? Help -
Status	Loas		(i)
General			~
CPU and Memory	Forcepoint Technical Support may req	uest log files to assist you with unexpected results.	
Disk Usage	Select Module:	Appliance Controller Log Options	
Network Bandwidth	Appliance Controller	Log files are available in weekly increments for up to 5 weeks.	
Configuration	TRITON AP-WEB	Date range: 11/14 - Present V	
System		View ontions: View last 50 View	
Network Interfaces			
Routing		O Download entire log lile	
Alerting			Submit
Web Components			
Administration ^			
Patches / Hotfixes			
Backup Utility			
Logs			
Toolbox			
Account Management			

ADMINISTRATION > LOGS (continued)

Configure when log files are to be archived

(config)# set log archive

--type <system|audit|email| network-agent|web>

--size <integer|string|

--freq <weekly|monthly|yearly>

Display log file archiving settings

(config)# show log archive

--type <system|audit|email| network-agent|web>

Zip the log file and move it to a remote filestore

(config)# save log

--module <all|app|email|

network-agent|proxy|web>

--type <all|audit|module|system>

--location <filestore_alias>

See slide 31 for filestore definition command.

ORCEPOINT V50	00 63	Hostname: uaWeb.forcepoint.com		Log Off
« Status ^	Logs		?н	elp -
General CPU and Memory Disk Usage Network Bandwidth Configuration System Logs Forcepoint Technical Support Select Module: Appliance Controller Content Gateway TRTON AP-WEB Network Agent	Logs Forcepoint Technical Support may request log files to Select Module: Appliance C Appliance Controller Log files are Content Gateway Date range: TRITON AP-WEB Network Agent View option: View option:	assist you with unexpected results. ontroller Log Options available in weekly increments for up to 5 weeks. 11/14 - Present \checkmark s: • View last $50 \checkmark$ lines		(I
Network Interfaces Routing Alerting Web Components		O Download entire log file	5	šubmit
Administration ^ Patches / Hotfixes Backup Utility				
Logs Toolbox Account Management				

ADMINISTRATION > TOOLBOX

Custom block pages are described in the online AP-WEB API Guide

Enable or disable remote CLI access via SSH.

(config)# set access ssh --status <on|off>

Display whether remote CLI access via SSH is enabled

(config)# show access ssh
 --status

RCEPOINT V5	i000 G3 Hostname: uaW	eb.forcepoint.com 🌐	Log Off			
Status	Toolbox	?	Help			
Status -	Web Security Block Pages		(i			
eneral PU and Memory sk Usage atwork Bandwidth	Use <u>http://testdatabasewebsense.com</u> to test current block pages based on the policy config Customize block pages if desired. Use Apply Changes to confirm your customizations. Specify block page type:	uration in your environmer	ıt.			
Configuration	Custom block page					
stem twork Interfaces uting erting eb Components	Download files from the editable directory to customize. Upload desired changes and any are etc.). Files in editable directory (on appliance): Diock html DiockFrame.html DiockFrame.html DiockFrame.html	dditional files (custom logo	s, jpegs,			
Administration	continueFrame.html					
tches / Hotfixes	messagetile.txt moreInfo.html					
ckup Utility	quotaFrame.html					
gs	webDLPPolicyViolation.html					
count Management	Initial File(e) Download File(e) Dalata					
	oprodu i nela) continuari nela) perere	Apply Cha	nges			
	Appliance Command Line					
	Remote Access Command Line Utility					
	Access the appliance command line using a remote SSH Execute basic network tro appliance modules in a con	ubleshooting commands fo nmand line environment.)E			
	● On Save	Launch U	tility			
	Technical Support Tools					

ADMINISTRATION > ACCOUNT MANAGEMENT

Change the account password

(config)# set account admin

--password

You will be prompted to enter the new password.

Define an email address for admin account password recovery

(config)# set account email
 --address <address>

Display the SMTP server settings used with admin email address,

(config)# show account smtp

Define an SMTP server for admin account password recovery

```
(config)# set account smtp
```

--host <location>

```
--port <port>
```

```
--user <name>
```

Test the email address for password recovery

```
(config)# send test_email
```

DRCEPOINT V50	00 G3 Hostname: uaWeb.forcepoint.com	0	Log Off
«	Account Management	? Help	÷
eneral	Change Password		(i)
PU and Memory	Current password:		
isk Usage	New password:		
etwork Bandwidth	Confirm new password:		
Configuration ^	Email Settings		
ystem etwork Interfaces	In the event the appliance admin password is lost or forgotten, a password recovery email is sent to the admin Provide the SMTP server settings to use for sending password recovery emails.	email add	ress.
lerting	Notification email address: Password recovery emails are sent to this address		
eb Components	SMTP server: IP address or hostname		
	Port: 25		
Administration ^	Test Connection		
atches / Hotfixes			
ackup Utility	SMTP server requires authentication		
ogs	Account:		
oolbox	Password:		
ccount management			
	Content Gateway Manager Password Reset		
	Click Reset Password to reset your Content Gateway Manager password. Log on to <u>Content Gateway Manager</u> Configure > My Proxy > UI Setup > Login to change the new password.	and go t	D
	Rese	t Password	
	Help Language Preference		
	Select preferred language for displaying Help information.		
	Language: English 🗸		
	ок	Cance	2

ADMINISTRATION > ACCOUNT MANAGEMENT (continued)

A

Delete the password recovery email address

(config) # delete account email

Delete SMTP settings

(config)# set account smtp --address <address>

Display Technical Support account access or activity history

```
(config)# show account tech-support
 --status
```

```
(config)# show account tech-support
   --history
```

The two parameters cannot be used at the same time.

Enable or disable access for Technical Support

```
(config)# set account tech-support
 --status <on|off>
```

FORCEPOINT V50	DO 63 Hostname: uaWeb.forcepoint.com 🌐 Log Off						
« Status	Account Management ? Help ·						
Canami	Change Password (
CPU and Memory	Current password:						
Disk Usage	New password:						
Network Bandwidth	Confirm new password:						
Configuration ^	Email Settings						
System	In the event the appliance admin password is lost or forgotten, a password recovery email is sent to the admin email address.						
Routing	Torride the SHTT Server Settings to use for Sending passion a recovery chains.						
Alerting	Notification email address: Password recovery emails are sent to this address						
Web Components	SMTP server: IP address or hostname						
A	Port: 25						
	Test Connection						
Patches / Hottixes	SMTD server requires authentication						
Logs							
Toobox	Account:						
Account Management	Password:						
	Content Gateway Manager Password Reset						
	Click Reset Password to reset your Content Gateway Manager password. Log on to <u>Content Gateway Manager</u> and go to Configure > My Proxy > UI Setup > Login to change the new password.						
	Reset Password						
	Help Language Preference						
	Select preferred language for displaying Help information.						
	Language: English V						
	OK Cancel						

All commands in this *Visual Primer*, plus additional commands that do not map to a previous console screen, are described in the TRITON Appliances *CLI Guide* for version 8.3.

The *CLI Guide* is at the Support website under **Documentation** > **Forcepoint Appliances**.