

Configure Blue Coat ProxySG to Upload Log Files to Cisco Global Threat Alerts

Last updated: July 28, 2022

Contents

Introduction

Prerequisites

Requirements

Components Used

Configure

Configure the Proxy

User Authentication

Configure DNS

Next Steps

Troubleshooting

Conventions

This document uses the following conventions:	
---	--

Convention	Indication
bold font	Commands and keywords and user-entered text appear in bold font.
<i>italic</i> font	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic</i> font.
[]	Elements in square brackets are optional.
{x y z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in courier font.
< >	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note: Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

Caution: Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Warning: IMPORTANT SAFETY INSTRUCTIONS

Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Regulatory: Provided for additional information and to comply with regulatory and customer requirements.

Introduction

This document describes how to configure a Blue Coat ProxySG to upload its log files to Cisco, where cloud-based machine learning analyzes the data and reports its findings in the global threat alerts (formerly Cognitive Intelligence or Cognitive Threat Analytics) portal.

Prerequisites

Requirements

Cisco ScanCenter is the administration portal into Cisco Cloud Web Security. You must first create a device account in Cisco ScanCenter for your Blue Coat ProxySG.

- Log in to Cisco ScanCenter
- Click the **Threats** tab
- Click the global settings menu icon in the upper-right corner of the page
- Click Device Accounts
- Choose Automatic upload method

For more information, see <u>Proxy Device Uploads</u>.

Once the device account is created, copy this information from the Add Device Account page in Cisco ScanCenter to paste into your proxy configuration:

- HTTPS host: etr.cloudsec.sco.cisco.com
- HTTPS path
- Device username generated for your proxy device, case sensitive, different per proxy device
- Device password, case sensitive

In order to access your Blue Coat ProxySG, you need:

- Hostname or IP address of your Blue Coat ProxySG
- Login credentials to the Blue Coat ProxySG
 - Default username is admin
 - No default password, must be configured
- Web browser with Java[™] plug-in, Blue Coat does NOT support Google Chrome, Opera, or Safari

Caution: The information in this document was created from devices in a lab environment. If your network is live, understand the potential impact of any configuration command.

Components Used

The information in this document was tested on this hardware:

• Blue Coat ProxySG 600

The information in this document was tested on these software versions:

- SGOS 6.5.7.5
- SGOS 6.5.6.1

Note: Other versions are currently not supported as they may not work properly when uploading to global threat alerts.

Configure

Configure the Proxy

- 1. Point your web browser to your Blue Coat ProxySG:
 - a. https://sg_600.hostname:8082/ or
 - b. <u>https://a.b.c.d:8082/</u> where a.b.c.d is the proxy's IP address
- 2. If needed, accept the insecure HTTPS certificate to proceed.
- 3. Log in as admin.
- 4. If needed, accept the Java[™] security warning to proceed.
- 5. Navigate to **Configuration > Access Logging > General**.
- 6. Select the **Enable Access Logging** check box, and click the **Apply** button.
- 7. Navigate to **Configuration** > **Access Logging** > **Formats**.
- 8. Click the **New** button to create a new format entry.
- 9. Enter a unique name in the Format Name field. In this example, we used daniels:

specify below)	
Format (ELFF) string (specify below)	
ylength cs-headerlength cs(User-Agent) rs(Content-Type) cs-method sc-status cs(Referer) r	cs-ip Test Forma
rcv: Log last header ====	
	specify below) Format (ELFF) string (specify below) ylength cs-headerlength cs(User-Agent) rs(Content-Type) cs-method sc-status cs(Referer) i icy; Log last header :

OK Cancel

10. Click the radio button for **W3C Extended Log File Format (ELFF) string** and paste the following string into the field:

```
timestamp time-taken c-ip cs-username s-ip s-port c-port cs-uri cs-
bytes sc-bytes sc-bodylength sc-headerlength cs-bodylength cs-
headerlength cs(User-Agent) rs(Content-Type) cs-method sc-status
cs(Referer) cs-ip r-ip r-port rs(Location) s-action sc-filter-result
```

- 11. Click the **OK** button.
- 12. Click the **Apply** button.
- 13. Navigate to **Configuration** > **Access Logging** > **Logs**.
- 14. Click the **New** button to create a new log entry.
- 15. Choose the format name you created in Step 9 for both the Log Name and Log Format. In this example, we used daniels:

Statistics Con	nfiguration Maintenance Health: S	<u>2K</u>
 General Network ADN Services ProxyClient St 	Logs General Settings Upload Client Upload Schedule Logs: Name Format main daniels	
 SSL Proxy Settings Bandwidth Mgmt. Authentication Content Filtering Geolocation The set Broacting 	streaming bcreporterstreaming_v1 ssl bcreporterssl_v1 im im p2p p2p cifs bcreportercifs_v1 mapi mapi daniels daniels	
 External Services Forwarding Health Checks Access Logging General Logs Formats 		
Policy	New Delete	
	Preview Apply Revert Help	

- 16. Click the **OK** button.
- 17. Click the **Apply** button.
- 18. You may receive a popup warning message which can safely be ignored. Message says log entries in the previous format may be mixed with entries in the current format in the same log file.
- 19. Click the Upload Client tab.
- 20. In the Log pull-down, select the log from Step 15.
- 21. In the **Client type** pull-down, select **HTTP Client**.
- 22. Click the Settings button next to Client type, and a new window appears.
- 23. In the Host field, enter the host provided in Cisco ScanCenter; for example: etr.cloudsec.sco.cisco.com
- **24**. In the **Port** field, enter 443.
- 25. In the **Path** field, enter the path provided in Cisco ScanCenter; for example: /upload/username
- 26. In the **Username** field, enter the username generated for your device in Cisco ScanCenter. The device username is case sensitive and different for each proxy device.
- 27. For now, don't change the **Filename** field.
- 28. Select the Use secure connections (SSL) check box.
- 29. Click the Change Primary Password button, and a new window appears.
- 30. In the password fields, enter the password generated for your device in Cisco ScanCenter. The device password is case sensitive.
- 31. Click the **OK** button.
- 32. Click the **Upload Schedule** tab.

- 33. In the Log pull-down, select the format name you created in Step 9.
- 34. In the **Upload the log file** section, select upload the log file **Every** 0 hours and 55 minutes.

Number of Users Behind Proxy	Recommended Upload Period
Less than 2000	55 minutes
Unknown or 2000 to 4000	30 minutes
4000 to 6000	20 minutes
More than 6000	10 minutes

- 35. Click the **Apply** button.
- 36. Navigate to **Configuration > Policy > Visual Policy Manager**.
- 37. Click the **Launch** button, and a new window appears.
- 38. Navigate to **Policy > Add Web Access Layer**.
- 39. Name the layer Cisco Logging Web Access Layer and click **OK**.
- 40. Move your cursor to the **Action** column, right-click, and choose **Set**:
 - File Edit Policy Configuration View Help



Settings retrieved from SG Appliance 178.17.111.2 Negate 41. In the Show pull-down, choose Modify Access Logging Objects:



42. Click the New button and choose Modify Access Logging:

Existing Action Objects		
Show: Modify Acces	s Logging Objects	\$
New	Remove	Edit
Set Effective Client	: IP	Help
Deny		
Return Exception.		
Return Redirect		
Send IM Alert		
Modify Access Log	ging	
Override Access Lo	og Field	

- 43. Enter a name. For this example we will use Cisco Access Logging.
- 44. Click the radio button for **Enable logging to** and in the pull-down choose the log from Step 15. In this example, we used daniels:

Name:	Cisco_Access_	Logging	
O Disat	ole all access loggi	ng:	
⊖ Reset	to default access	logging	
💽 Enabl	e logging to:	daniels	÷
) Disat	le logging to	main streaming ssl	
l	ОК С	anc im p2p	
		cifs mapi	
		(damials	

- 45. Click the **OK** button.
- 46. Click another **OK** button.
- 47. Click the **Install Policy** button.
- 48. After the "policy installation was successful" message is shown, close the Visual Policy Manager window.

User Authentication

In order to get user details for access logs, users must be authenticated. Follow these steps to set up LDAP authentication.

- 1. Navigate to **Configuration > Authentication > LDAP**.
- 2. On the LDAP Realms tab, click the New button to create a LDAP realm.
- 3. Enter a name for the realm and the realm configuration parameters. For example:

Realm name:	bluecoat	
Realm Configura	tion	
Type of LDAP s	erver: Microsoft Active Directory	
Primary server I	nost: prg5-ad.cisco.com	Port: 389
User attribute t	ype: sAMAccountName	

Other realm configuration parameters have been set to default values.

OK

Cancel

- 4. Click the **OK** button.
- 5. Click the **LDAP Servers** tab.
- 6. In the **Realm name** pull-down, choose the LDAP realm you previously created.
- 7. Select the **Follow referrals** check box.
- 8. Choose the Type of LDAP server, and enter the Primary server host. For example:

General	LDAP Realms LDAP Servers LDAP DN	LDAP Search & Groups
Network		
ADN	Dealer annua	
Services	keaim name: bluecoat	
ProxyClient	Turne of LDAP convert	2211
SSL	Microsoft Active Directo	ry
Proxy Settings	I DAP Protocol Version	A Clever
Bandwidth Mgmt.	2 BAF HOROCOT VEISION.	Follow refer
Authentication	r Servers	
Console Access		
Windows Domain	Primary server host: prg5-ad.cisco.com	Port: 389
Realms	Alternate server host:	Port: 389
IWA		Contract Proven
Windows SSO	s SSI Ontions	
► LDAP*		
Novell SSO	Enable SSL	
RADIUS	SSL device profile: default ‡	
Local		
Certificate	r Test Configuration	
CA e Trust SiteMinder		
Oracle COREId	Validation the realm configuration requires the username and parswork	Test Configuration
SAML	valuating the real configuration requires the username and passwor.	. Test configuration
AML Boline Substitution	5	
Sequences	r LDAP Specific Settings	
Transparent Prove		
Forms	Timeout request after 60 seconds	
Content Filtering	Core consistive	
a content intering		
Geolocation		
Geolocation		
Geolocation Threat Protection External Services	Preview Apply Revert	Help

- 10. Click the **LDAP DN** tab.
- 11. Click the **New** button.
- 12. In the Add Base DNs field, enter the distinguished name string. For example:

Γ	Add Base DNs
	dc=prg5-ad,dc=cisco,dc=com
L	
	OK Cancel

- 13. Click the **OK** button.
- 14. Click the LDAP Search & Groups tab.
- 15. In the **Realm name** pull-down, choose the LDAP realm you previously created.
- 16. Enter the Search user DN information. For example:

Statistics Com	nguration maintenance ne	nun - 2012 -
Ø General	LDAP Realms LDAP Servers LDAP DN LDAP Search & G	roups
Network		
O ADN	Baster same:	
Services	bluecoat	;
ProxyClient	r Search	
SSL SSL	Anonymous search allowed	
Proxy Settings		
Bandwidth Mgmt.	Search user DN: CN=bluecoat,CN=users,DC=prg5-ad,DC=cisco,DC=com	
Authentication Console Access	Change Password	
Windows Domain	Dereference aliases: always	
Realms		
IWA	r Group information	
Windows SSO	Membership type: 🕞 Liser 🔘 Group	
LDAP*		1
Novell SSO	Membership attribute: memberOf	
RADIUS	Username type to lookup: FQDN Relative	
Local	C Nexted Course Summer	
Certificate	i Nested Groups Support	
CA eTrust SiteMinder	Nested group attribute: member	
Oracle COREid	Construction Date:	
SAML	Group constraint inter.	
XML		
Policy Substitution		
Sequences		
Fransparent Proxy		
Forms		
Content Filtering		
Geolocation		
Fineat Protection	Preview Apply Revert	Help
External Services	Insaved changes, press "Apply" to save changes	

- 17. Click the **Change Password** button.
- 18. Enter the password in the password fields, and click the **OK** button.
- 19. Click the **Apply** button.

Configure DNS

The following configuration section is optional. Please consult your IT department before making these changes. If you use Microsoft Active Directory, you may need to add its address to the list of DNS servers. For example:

Routing	Group Name	Servers	Domains	
► DNS	primary	83.167.232.110		
WCCP	alternate	195.140.254.242		
Private Network				
Advanced				
ADN				
Services				
ProxyClient				
SSL				
Proxy Settings				
Authentication				
Content Filtering				
Geolocation				
Threat Protection				
External Services				
Forwarding				
Health Checks				
Access Logging				
Policy				
	Nicital	Edit	Delete	

ervers	Domains	
3.167.232.110	*	

Next Steps

Sign in to Cisco ScanCenter and check the DEVICE ACCOUNTS page to verify that the uploading is successful. When you browse the web from devices behind your Blue Coat ProxySG, the telemetry data logged in the files will be uploaded to Cisco's cloud-based machine learning system for analysis and displayed in the Threats tab and global threat alerts portal. For details, see <u>Proxy Device Uploads</u>.

Troubleshooting

- 1. Log into your Blue Coat ProxySG.
- 2. Navigate to Configuration > Access Logging > Logs > Upload client.
- 3. Click the **Test upload** button.
- 4. View the log files by navigating to Statistics > Advanced > Event Log.
- 5. Click Show event log tail with refresh time.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <u>www.cisco.com/go/trademarks</u>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2016-2022 Cisco Systems, Inc. All rights reserved.