Configure a McAfee Web Gateway to Upload Log Files to CTA System

Last updated: March 20, 2017

Contents

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* 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 McAfee Web Gateway to upload its log files to the Cisco Cognitive Threat Analytics (CTA) system. Once the log files have been uploaded to the system, CTA analyzes the data and reports findings to the CTA portal.

Note: Currently, this integration is in Limited Availability, in which versions of McAfee Web Gateway supported consist of those from a subset of customers. Until General Availability is established, integrations are to be done on a case-by-case basis with guidance from the Cisco CTA Team. Email cta-pm@cisco.com to request integration of your McAfee Web Gateway proxies with CTA.

Prerequisites

Requirements

Create a device account in the Cisco CTA portal for your McAfee Web Gateway.

1. Open http://cognitive.cisco.com in your web browser
2. Click on **Customer Login**
3. Select the type of credentials that match your case; if one is already selected, click the link on the bottom of the login dialog that says **Different login credential**
    a. **Web Security** if you have CTA as part of the CWS Premium offering
    b. **AMP for Endpoints** if you have enabled CTA within AMP for Endpoints
    c. **Cisco SSO** if you have Cisco internal login credentials
4. Sign in to CTA
5. Click the global settings menu icon in the upper-right corner of the page
6. Click **Device Accounts**
7. Click **Let's Get Started**
8. Select **Automatic** upload method and **HTTPS**
9. Enter a name

Once the device account is created, copy this information from the **Add Device Account** page in the CTA portal 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 McAfee Web Gateway, you need:

- Hostname or IP address of your McAfee Web Gateway
- Login credentials to your McAfee Web Gateway
    - Default username: **admin**
    - Default password: **webgateway**
- Web browser with the Java™ plug-in; supported browsers are Microsoft Internet Explorer, version 6.0 or newer and Mozilla Firefox, version 2.0 or newer

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:

- Virtual Appliance deployed in VMware

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

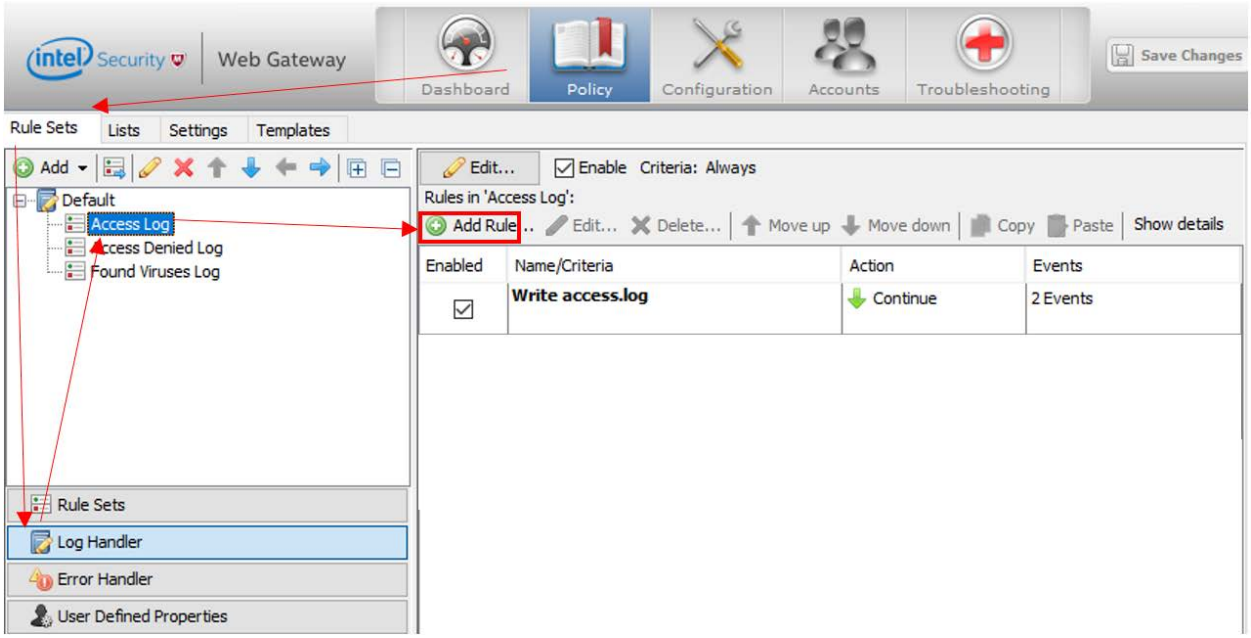
- McAfee Web Gateway Appliance ISO, version 7.6.2.8.0, build 22994

Note: Other versions are currently not supported, as they may not work properly when uploading to CTA.

Configure

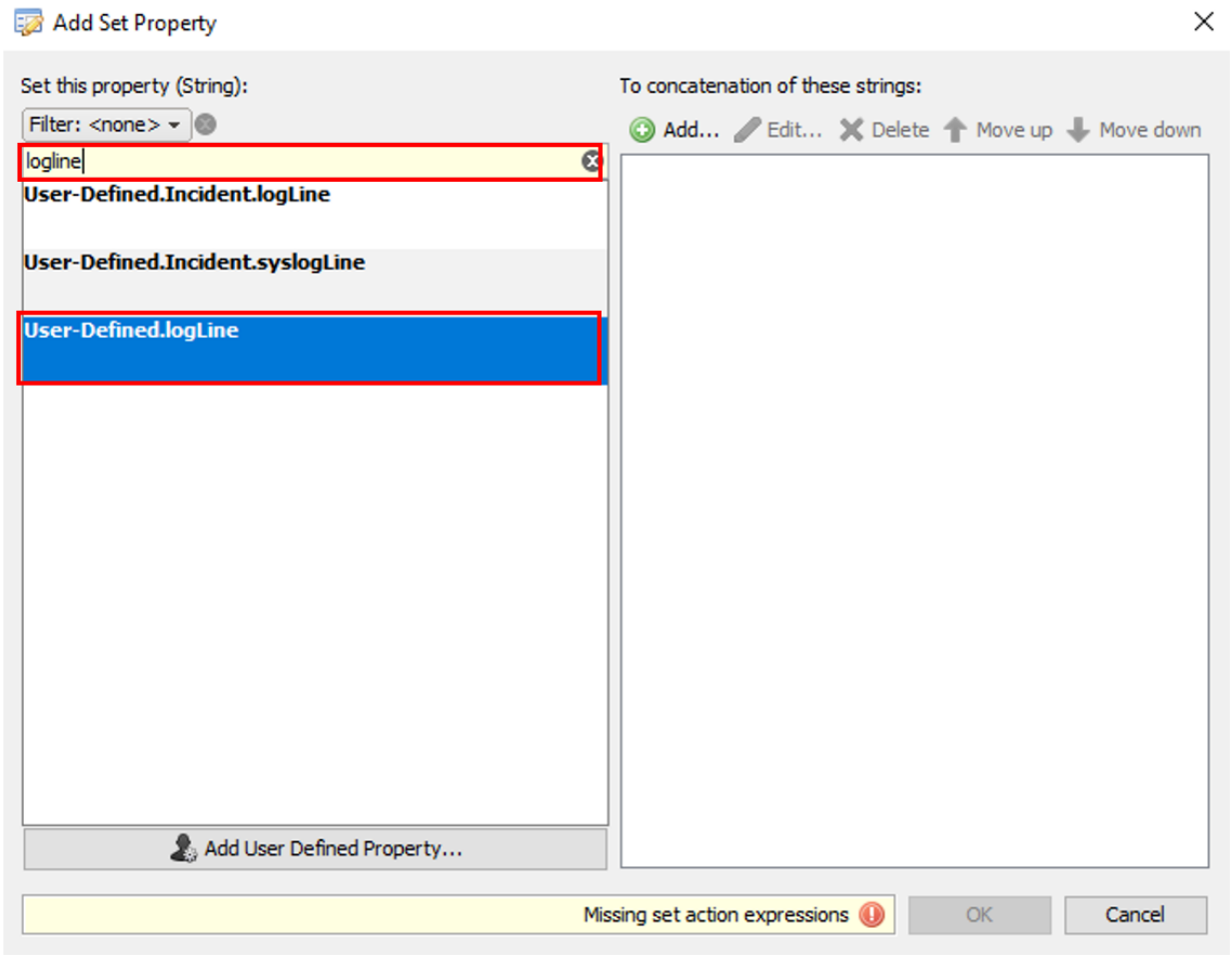
Configure the Gateway

1. Point your web browser to your McAfee Web Gateway:
   a. http://*IP address or domain name*:4711/
   b. https://*IP address or domain name*:4712/
2. Log in as the Super Administrator.
3. Navigate to **Policy > Rule Sets > Log Handler > Default > Access Log**.
4. Click **Add Rule**.

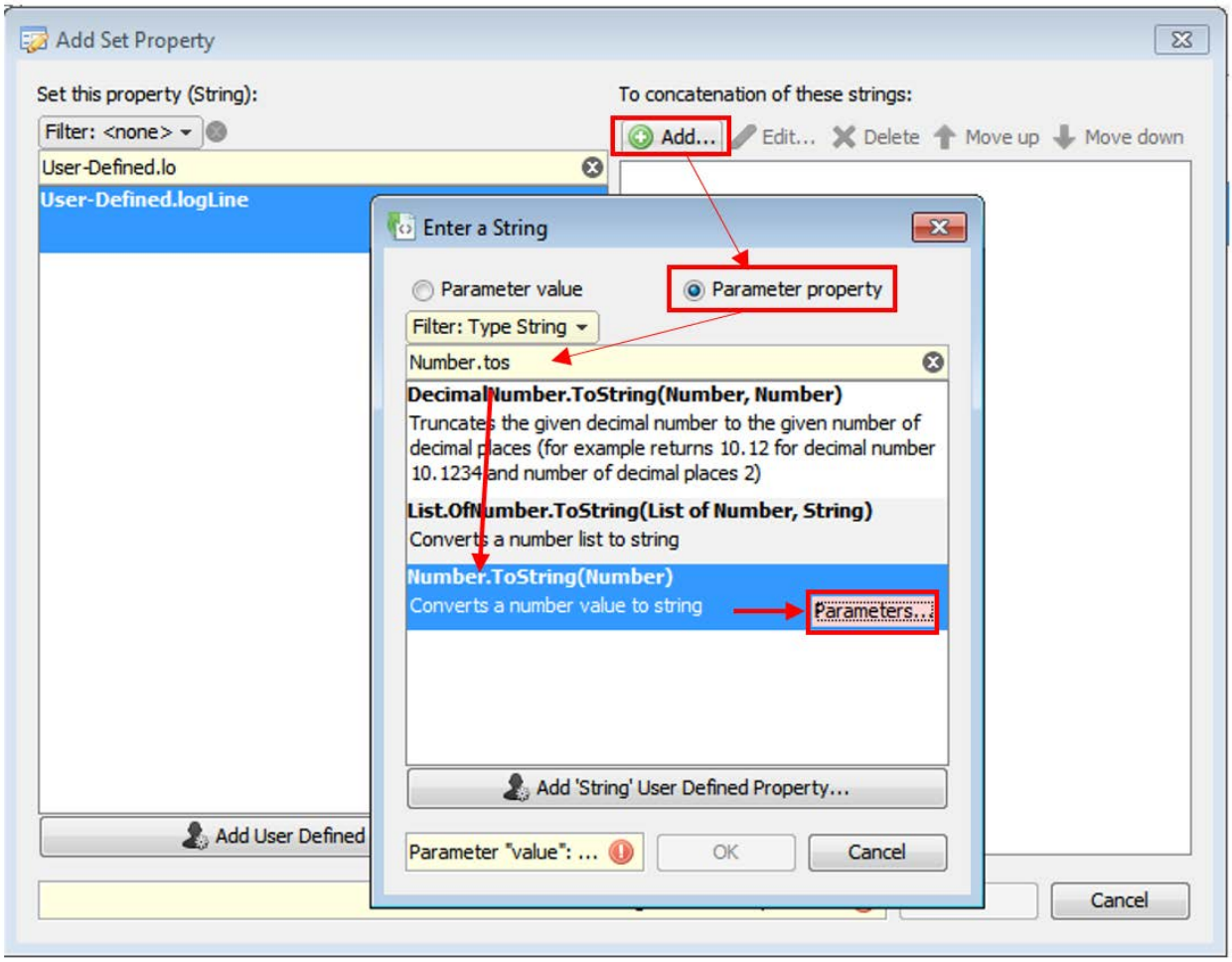


5. Name: enter a name of your choosing
6. Rule Criteria: **Always**
7. Action: **Continue**
8. Events: Select **Add... > Set Property Value**

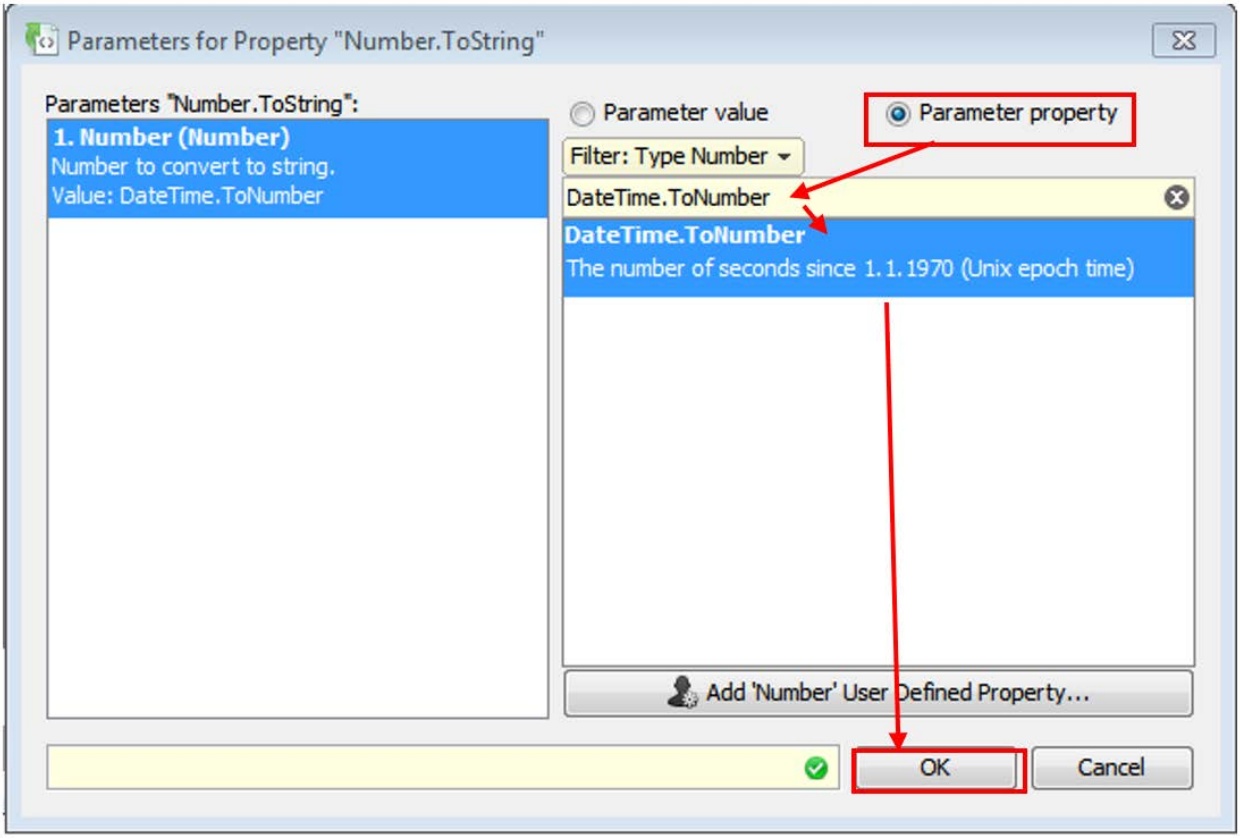
9. Search for and select **User-Defined.logLine**



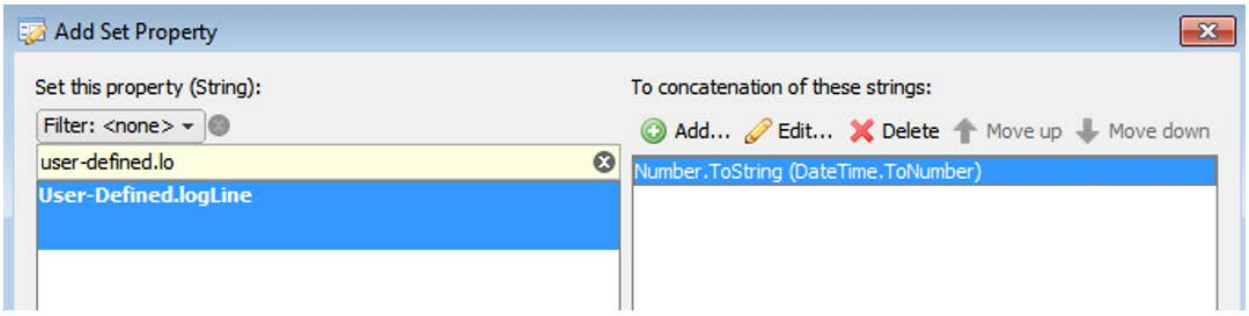
10. Click **Add...** and in the pop-up, select the **Parameter property** radio button.
11. Search for the **Number.To.String(Number)** entry, and click **Parameters**.



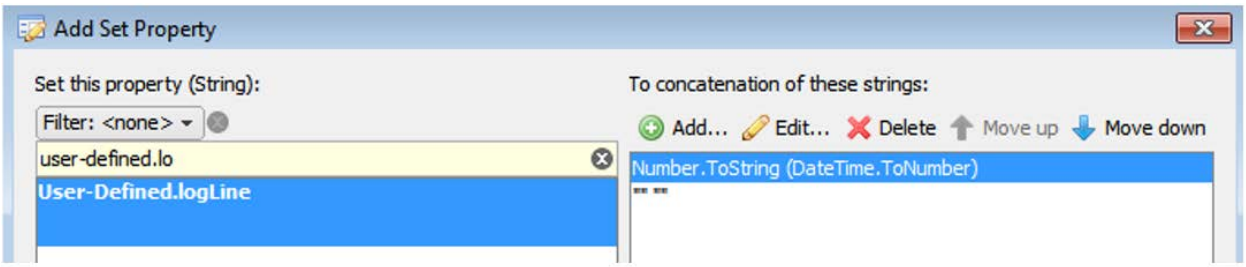
12. In the pop-up, select **Parameter property** and search for **DateTime.ToNumber**.
13. Select it and click **OK**.



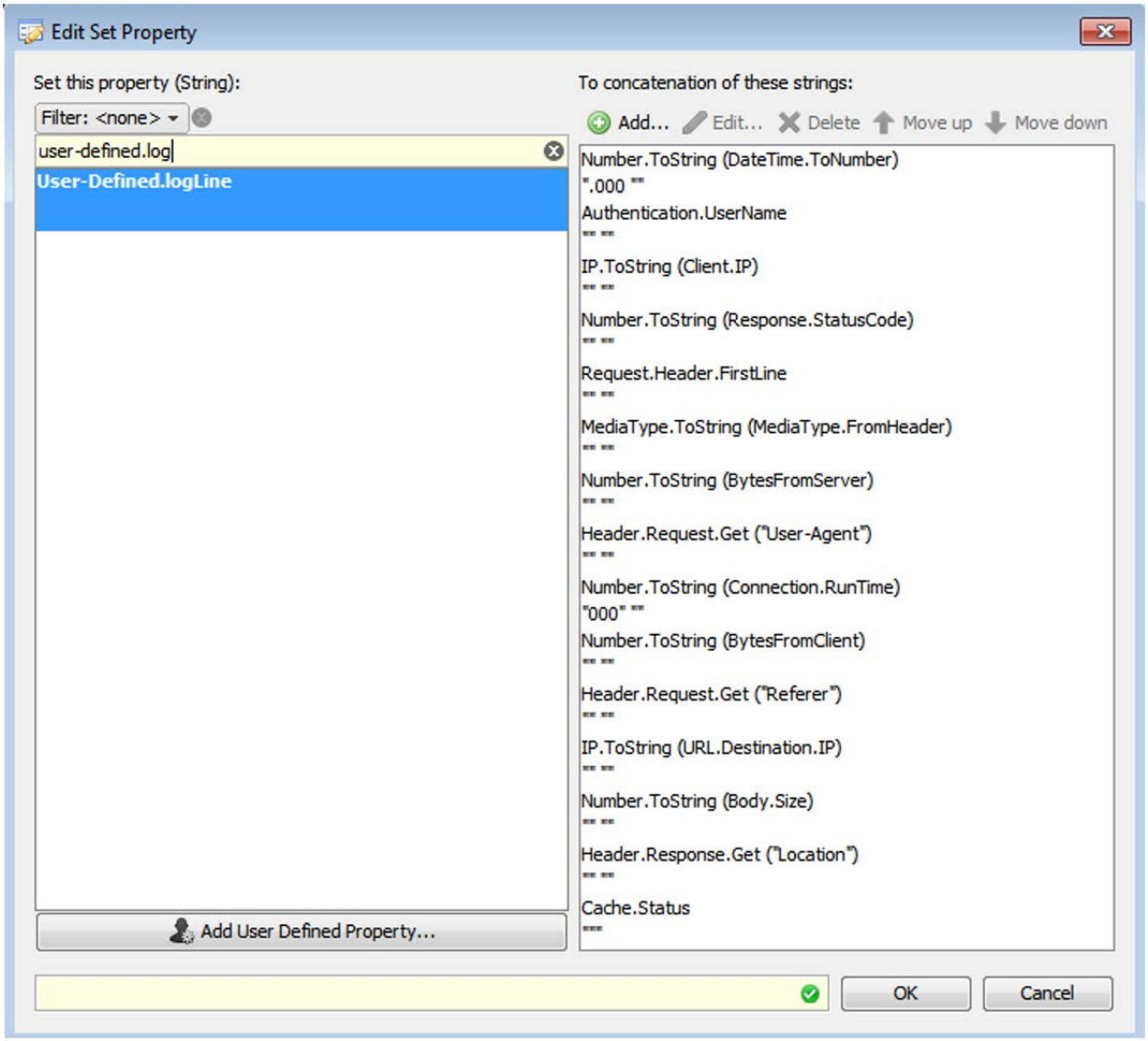
14. Click **OK** and notice that the first line of the format has been set up.



15. Click **Add...** and in the pop-up, select the **Parameter value** radio button.
16. Enter “ “
17. Click **OK** and notice that the second line of the format has been set up. Your entered text gets wrapped in quotes and results in the “” “” being shown.



18. Continue with this process until the list looks like this:

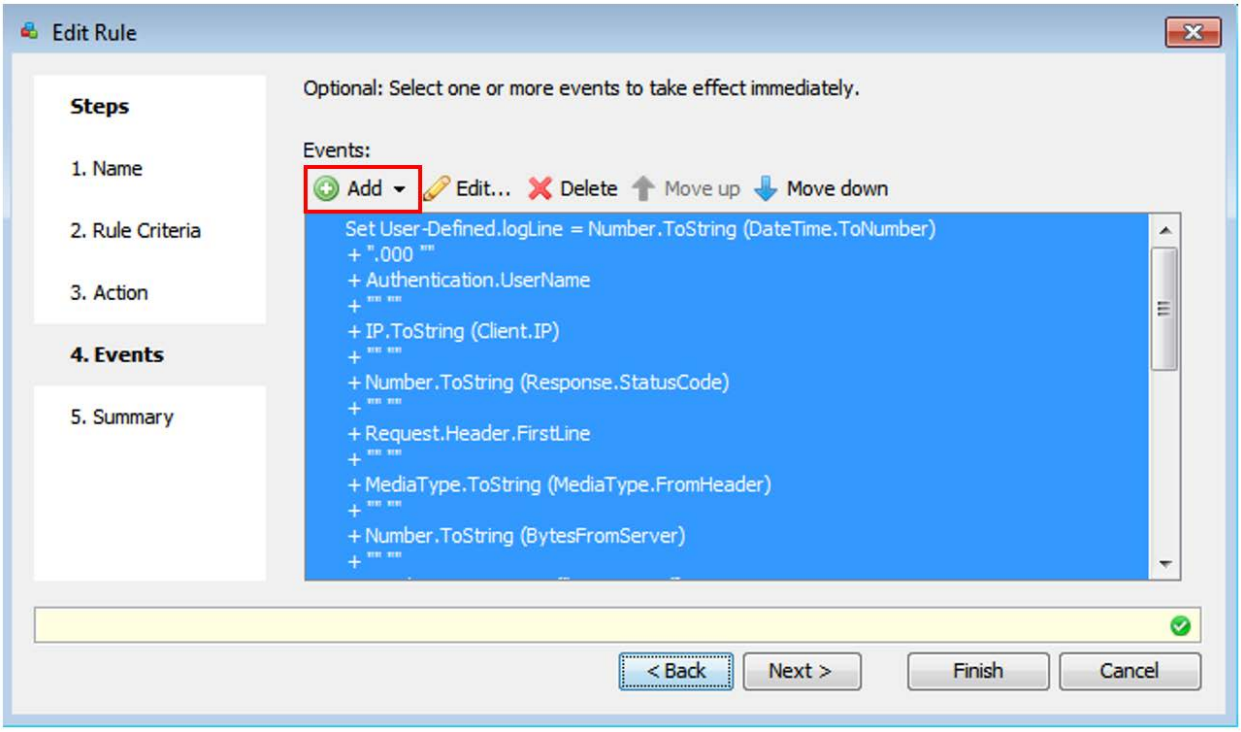


19. Most items on the list are Parameter properties and are searched for. Only the underlined items are added as Parameter values which results in quotes being added to them:

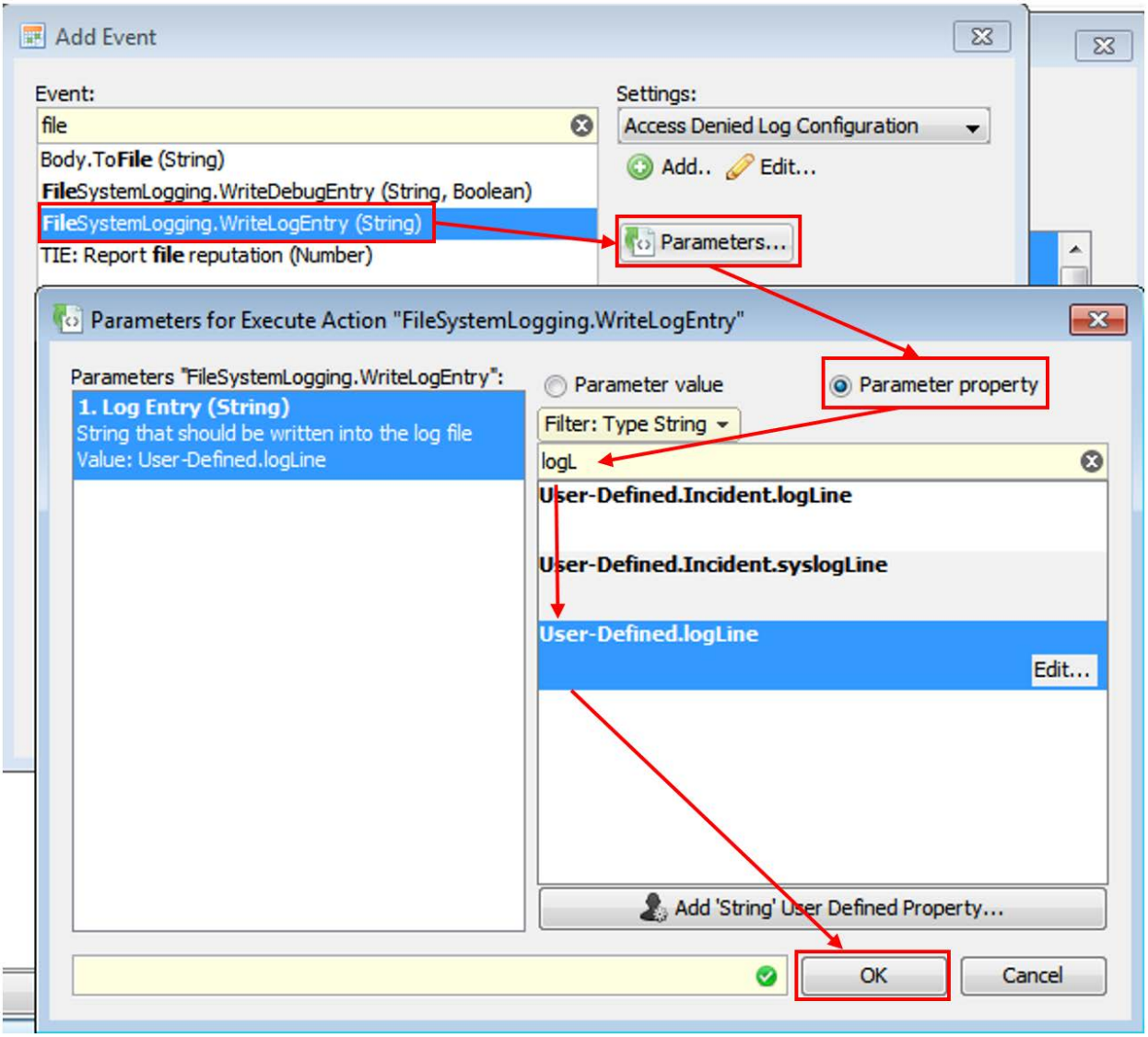
```
Number.ToString(DateTime.ToNumber)
.000 "
Authentication.UserName
" "
IP.ToString(Client.IP)
" "
Number.ToString(Response.StatusCode)
" "
Request.Header.FirstLine
" "
MediaType.ToString(MediaType.FromHeader)
" "
```

```
Number.ToString(BytesFromServer)
" "
Header.Request.Get(User-Agent)
" "
Number.ToString(Connection.RunTime)
000" "
Number.ToString(BytesFromClient)
" "
Header.Request.Get(Referer)
" "
IP.ToString(URL.Destination.IP)
" "
Number.ToString(Body.Size)
" "
Header.Response.Get(Location)
" "
Cache.Status
"
```

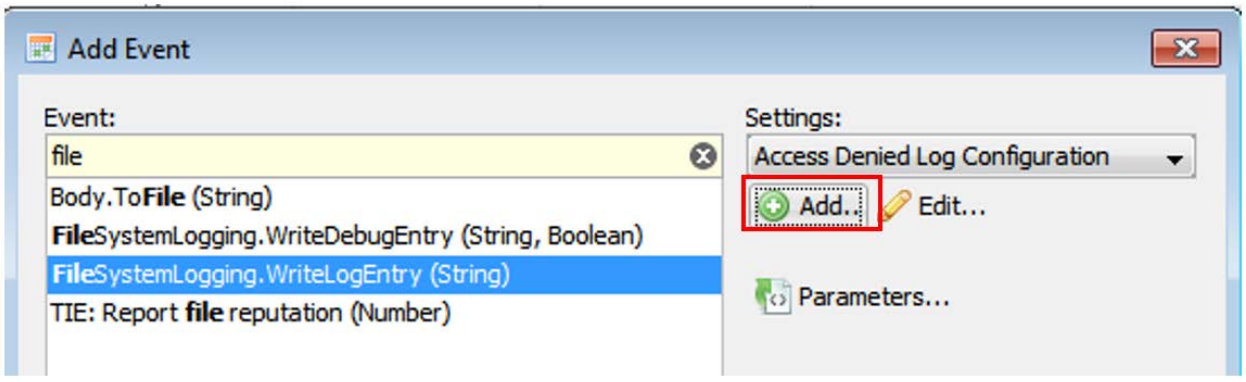
20. Once the last line is configured, click **OK**.
21. Send your newly created log line to a file system logging engine. Click **Add > Event**.



22. Search for **FileSystemLogging.WriteLogEntry**.
23. Click **Parameters...**
24. In the pop-up, select **Parameter property**, and search for **User-Defined.logLine**.
25. Select **User-Defined.logLine** and click **OK**.



26. Set up system logging engine by clicking **Add**...



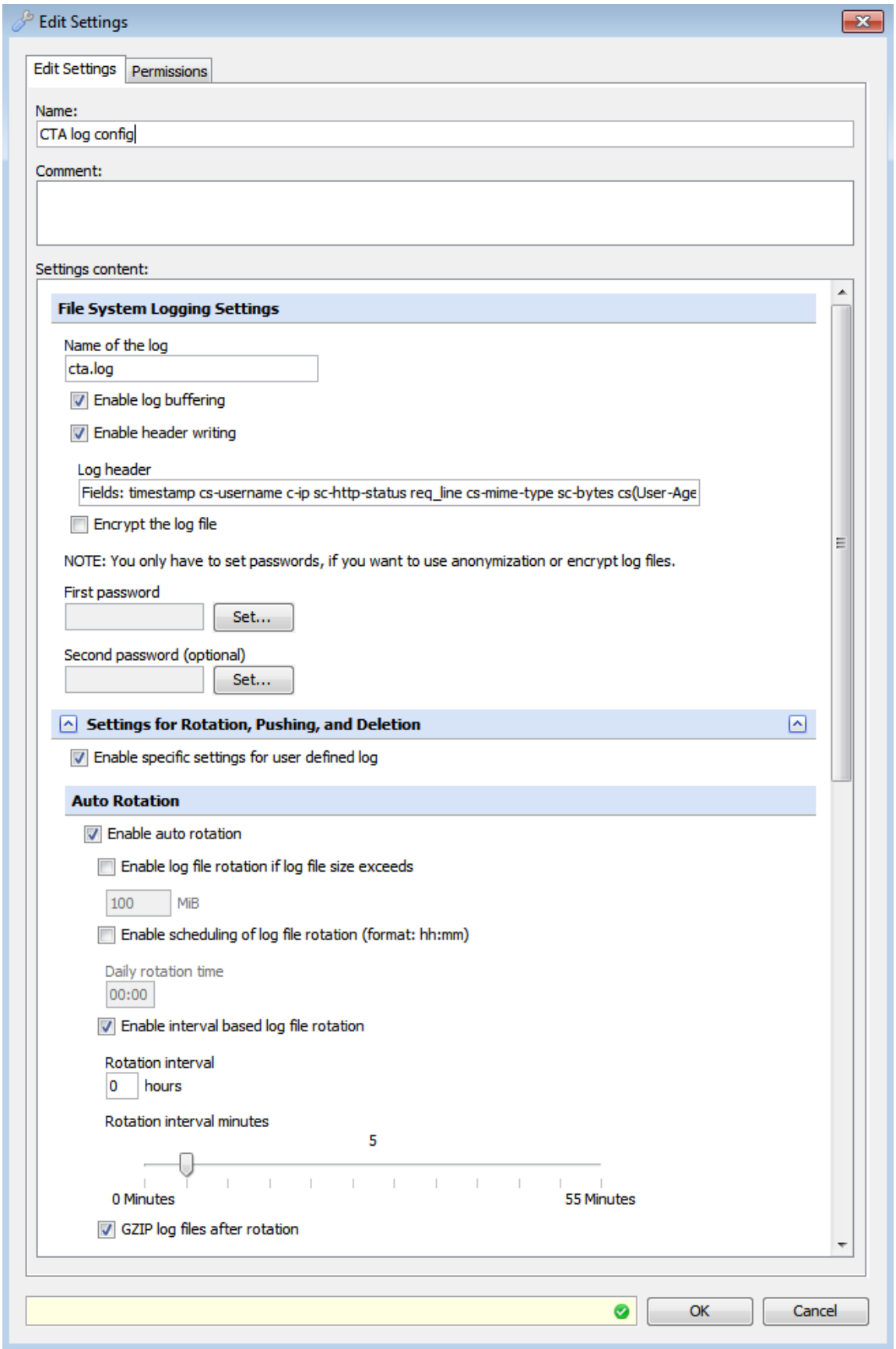
27. Set up the following:
    a. Name: **CTA log config**
    b. Name of the log: **cta.log**
    c. Enable log buffering

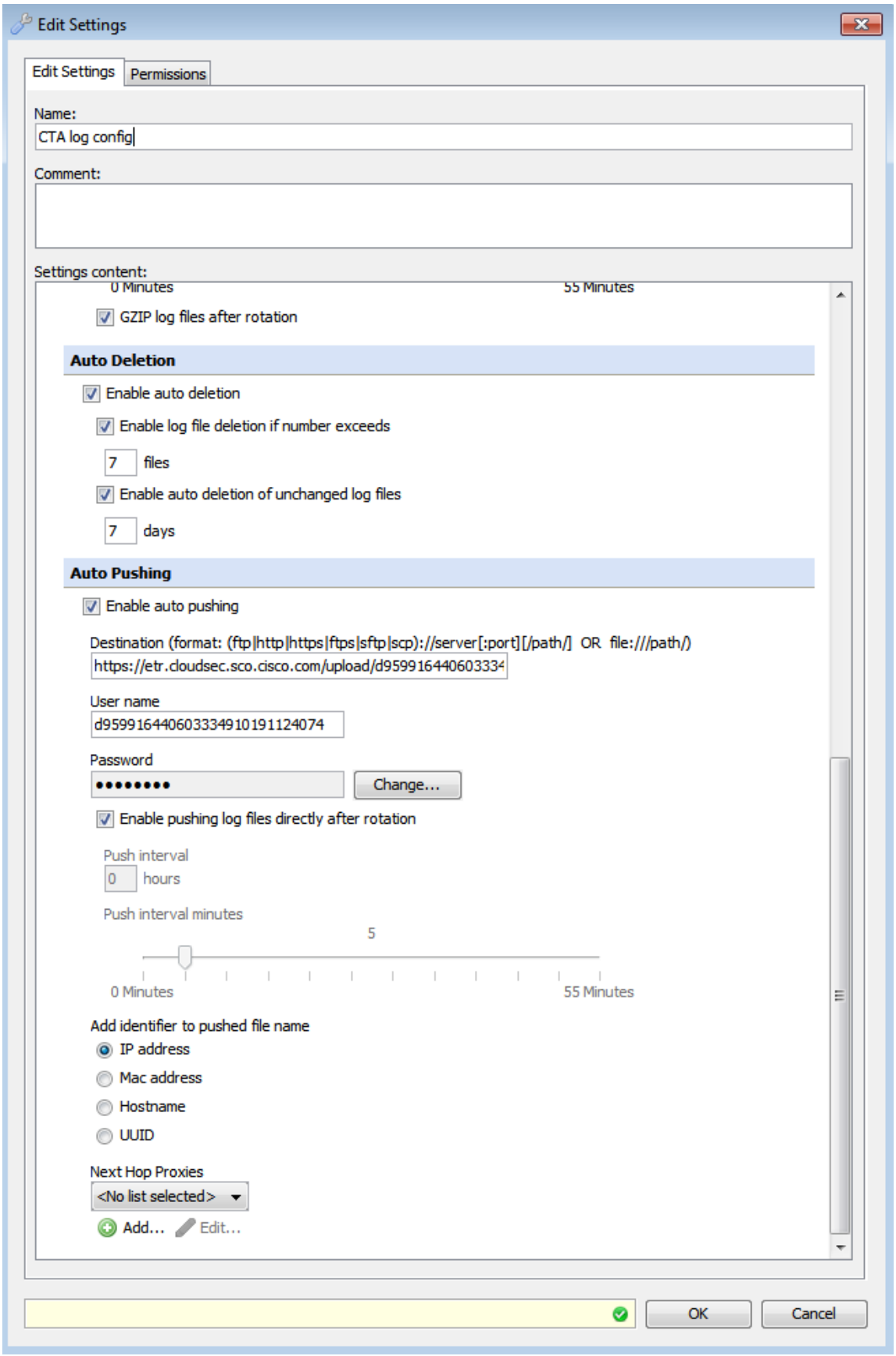
d. Enable header writing
e. Log header:
   `Fields: timestamp cs-username c-ip sc-http-status req_line cs-mime-type sc-bytes cs(User-Agent) x-elapsed-time cs-bytes cs(Referer) s-ip ma-bodylength sc(Location) sc-result-code`
f. Expand section **Settings for Rotation, Pushing, Deletion**
g. Enable specific settings for user-defined log
h. Enable auto rotation
i. Enable interval based log file rotation and disable the other file rotation methods
j. Rotation interval: 0 hours
k. Set Rotation interval minutes based on the following table:

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

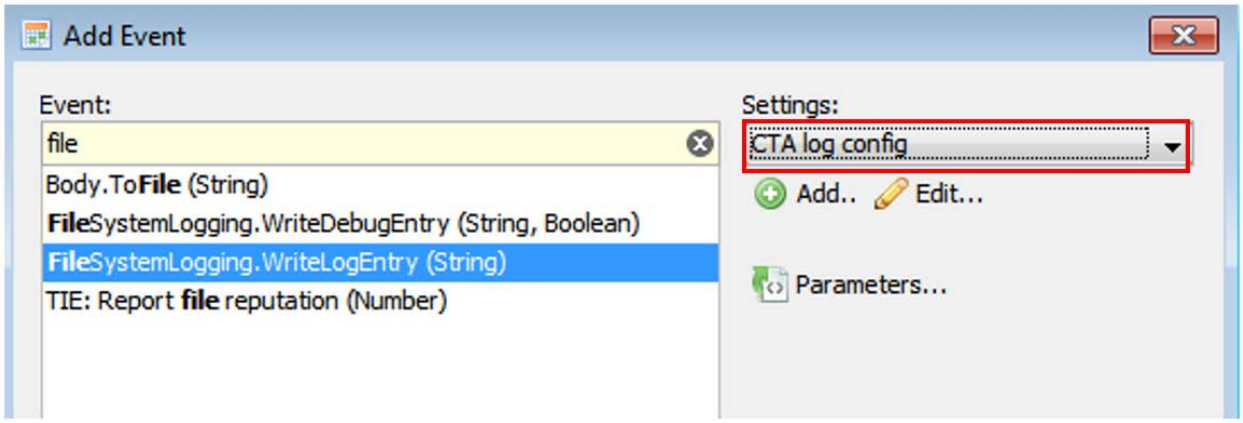
l. Enable GZIP log files after rotation
m. Enable Auto Pushing
n. In the Destination field, enter
   i. the path followed by the device username provided by device name provided by CTA:
      https://etr.cloudsec.sco.cisco.com/upload/*device_username*
   ii. User name: [Device username generated by CTA]
   iii. Password: [Device password generated by CTA]
o. Enable pushing log files directly after rotation

28. Check the fields once more using the following screenshots:

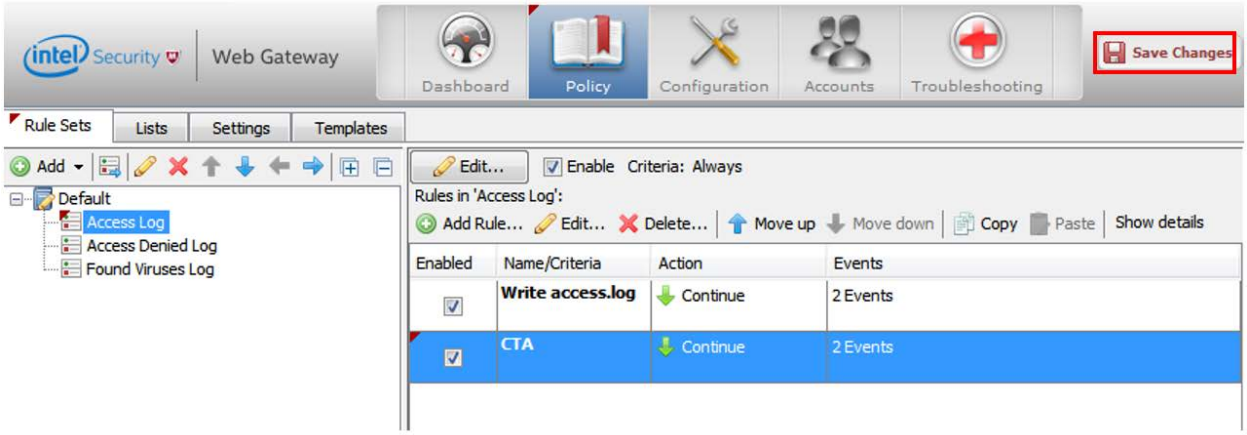

Edit Settings
Edit Settings
Permissions
Name:
CTA log config
Comment:
Settings content:
File System Logging Settings
Name of the log
cta.log
Enable log buffering
Enable header writing
Log header
Fields: timestamp cs-username c-ip sc-http-status req_line cs-mime-type sc-bytes cs(User-Age
Encrypt the log file
NOTE: You only have to set passwords, if you want to use anonymization or encrypt log files.
First password
Set...
Second password (optional)
Set...
Settings for Rotation, Pushing, and Deletion
Enable specific settings for user defined log
Auto Rotation
Enable auto rotation
Enable log file rotation if log file size exceeds
100
MiB
Enable scheduling of log file rotation (format: hh:mm)
Daily rotation time
00:00
Enable interval based log file rotation
Rotation interval
0
hours
Rotation interval minutes
5
0 Minutes
55 Minutes
GZIP log files after rotation
OK
Cancel


Edit Settings
Edit Settings
Permissions
Name:
CTA log config
Comment:
Settings content:
0 Minutes
55 Minutes
GZIP log files after rotation
Auto Deletion
Enable auto deletion
Enable log file deletion if number exceeds
7
files
Enable auto deletion of unchanged log files
7
days
Auto Pushing
Enable auto pushing
Destination (format: (ftp|http|https|ftps|sftp|scp)://server[:port][/path/] OR file:///path/)
https://etr.cloudsec.sco.cisco.com/upload/d95991644060333
User name
d9599164406033349101911240 74
Password
Change...
Enable pushing log files directly after rotation
Push interval
0
hours
Push interval minutes
5
0 Minutes
55 Minutes
Add identifier to pushed file name
IP address
Mac address
Hostname
UUID
Next Hop Proxies
<No list selected>
Add...
Edit...
OK
Cancel

29. Click **OK** twice and the Settings selector gets automatically populated with the new settings.



30. Click **Finish**.
31. Click **Save Changes**.



Next Steps

Sign in to the Cisco CTA portal, and check the Device Accounts page to verify that the uploading is successful. When you browse the web from devices behind your McAfee Web Gateway, the telemetry data logged in the files is uploaded to the CTA system for analysis and displayed in the CTA portal.

Additional Resources

- https://community.mcafee.com/docs/DOC-4812
- https://community.mcafee.com/docs/DOC-4928
- https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/26000/PD26527/en_US/mwg_762_ig_installation_0a00_en-us.pdf

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.