Zscaler Internet Access (ZIA) and McAfee MVISION Cloud (formerly Skyhigh Networks) Deployment Guide

July 2020

Version 1.1
# Table of Contents

1 Document Overview .............................................................................................................. 5  
   1.1 Document Audience ........................................................................................................ 5  
   1.2 Software Revisions ......................................................................................................... 6  
   1.3 Document Prerequisites ............................................................................................... 6  
   1.4 Request for Comments ................................................................................................. 6  

2 Configuring Log Processing ................................................................................................. 7  
   2.1 Configuring Zscaler NSS Feed ..................................................................................... 7  
   2.2 Configuring Zscaler NSS Server and McAfee MVISION Cloud (Skyhigh) ............... 8  

3 Configuring Automated Closed Loop Remediation (CLR) ............................................. 10  
   3.1 Closed Loop Remediation (CLR) Overview .............................................................. 10  
   3.2 Configuring Closed Loop Remediation (CLR) ......................................................... 11  

4 Appendix A: Zscaler Resources ......................................................................................... 27  

5 Appendix B: McAfee Resources ......................................................................................... 28
## Terms and Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS</td>
<td>Amazon Web Services (Amazon)</td>
</tr>
<tr>
<td>CASB</td>
<td>Cloud Access Security Broker</td>
</tr>
<tr>
<td>CLR</td>
<td>Closed Loop Remediation</td>
</tr>
<tr>
<td>EC</td>
<td>Enterprise Connector (McAfee MVISION Cloud)</td>
</tr>
<tr>
<td>ESX</td>
<td>VMware Hypervisor</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>NSS</td>
<td>Nanolog Streaming Service (Zscaler)</td>
</tr>
<tr>
<td>SIEM</td>
<td>Security Information and Event Management</td>
</tr>
<tr>
<td>Skyhigh</td>
<td>McAfee MVISION Cloud</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>ZIA</td>
<td>Zscaler Internet Access (Zscaler)</td>
</tr>
</tbody>
</table>
# Document Revision Control

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Change Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>November 2018</td>
<td>Initial document by Zscaler and McAfee</td>
</tr>
<tr>
<td>1.1</td>
<td>July 2020</td>
<td>Zscaler product name changes – Zscaler App to Zscaler Client Connector</td>
</tr>
</tbody>
</table>
1 Document Overview

This Deployment Guide document will provide GUI examples for configuring Zscaler Internet Access (ZIA) and McAfee MVISION Cloud (formerly Skyhigh). All examples in this guide presumes the reader has a basic comprehension of Cloud Security, including CASB concepts.

The solution deployment described in this guide can be summarized with following architecture.

1.1 Document Audience

This document was designed for Security Architects and Engineers. For additional product and company resources, please refer to the Appendix section.
1.2 Software Revisions

This document was written using Zscaler Internet Access v5.6 and McAfee MVISION Cloud v3.7.0 or later.

1.3 Document Prerequisites

Zscaler Internet Access (ZIA)

- A working instance of ZIA 5.6 (or newer)
- An active subscription to Nanolog Streaming Service (NSS)
- Administrator login credentials to ZIA

McAfee MVISION Cloud (Skyhigh)

- A working subscription to McAfee MVISION Cloud’s Shadow IT Service

1.4 Request for Comments

We value the opinions and experiences of our readers. To offer feedback or corrections for this guide, please contact partner-doc-support@zscaler.com.
2 Configuring Log Processing

2.1 Configuring Zscaler NSS Feed

1. In the Zscaler Admin Portal, navigate to Administration->Cloud Configuration->Nanolog Streaming Service-> NSS Feeds
2. Add a new NSS Feed with the following options:
   a. **Feed Name.** Skyhigh Log Feed
   b. **SIEM IP Address.** Enter the IP Address of McAfee MVISION Cloud (Skyhigh) Log Processor (for example, 10.1.1.3).
   c. **SIEM TCP Port.** Enter the port number of Skyhigh Syslog Server on the Log Processor server (for example, 514).
   d. **Log Type.** Web Log.
   e. **Status.** Enabled.
   f. **Feed Output Type.** Tab-Separated.
   g. **Feed Output Format.** Enter the following line. (You can also download this as a text file to easily copy and paste: zScalerNSSFormat.txt)

   ```
   "%02d{mth}/%02d{dd}/%d{yyyy}t%02d{hh}:%02d{mm}:%02d{ss}t%s{action}\t
t%s{host}\t%s{proto}\t%s{sip}\t%s{filetype}\t%s{urlcat}\t%s{cip}\t%s{login}\t%s{ologin}\t%s{dept}\t%s{bwthrottle}\t%s{location}\t%d{ctime}\t
t%d{reqdatasize}\t%s{reqmethod}\t%d{reqsize}\t%s{respcode}\t%d{respsize}\t%d{totalsize}\t%s{ua}\t%s{eurl}\t%s{referer}\t
t%s{filename}\t%s{nsssvcip}\t%s{productversion}"
   ```

   **IMPORTANT:** Make sure this field does not contain any line breaks or empty lines.

3. **Click Save.**
2.2 Configuring Zscaler NSS Server and McAfee MVISION Cloud (Skyhigh)

Setup on the Zscaler side

1. The McAfee MVISION Cloud Enterprise Connector (EC) should be in the same location where the logs are delivered. This can be on the customers’ premises or the same VM. A link to configure and deploy a NSS Server on ESX, AWS, and Azure can be found here [LINK].

Setup on the McAfee MVISION Cloud side

2. The Enterprise Connector (EC) is a lightweight on-premise application that runs on a virtual machine to ingest and process logs from egress devices (such as proxies or firewalls) and identifies relevant log entries, while tokenizing confidential information, enhancing the value of your existing infrastructure investments. It compresses the data and securely uploads it to the McAfee cloud service for discovery and analysis. Sensitive log data is tokenized on-premise, ensuring no personally identifiable information or confidential data (such as usernames and IP addresses) leave your organization. Enterprise Connector also integrates with Edge devices (proxies and firewalls) for Closed-Loop Remediation, Active Directory, SIEM, and SMTP.

   a. Install EC on customer premises (collocated with the location of delivery of logs)
      i. Need a VM or any local server
      ii. Download EC from this McAfee link
         1. Enterprise Connector runs on a virtual machine and is available for download and install on Windows or Unix environments.
         2. Before installing, please review Enterprise Connector Prerequisites
      iii. Install EC on VM
   b. After installation, configure the EC
      i. Connect EC to McAfee Cloud (link to steps)
      ii. Whitelist the required URLs so that EC can function properly (link to URL list)
   c. Configure EC in customer VM
      i. Configure syslog so that EC can receive log files (link)
      ii. Enable syslog service on EC interface
      iii. EC will capture syslog feeds and create log files
   d. Send a sample of these log files to McAfee support
      i. McAfee analyzes these log files and then creates a log parsing rule (or format)
   e. McAfee support team will enter the parsing rule on the customer admin tenant
f. Log processor (within EC) will pull this parsing rule and apply it on the log files in the customer VM

g. Logs are processed by EC and uploaded to McAfee MVISION Cloud

h. Customer can see cloud usage data on the McAfee MVISION Cloud dashboard
3 Configuring Automated Closed Loop Remediation (CLR)

3.1 Closed Loop Remediation (CLR) Overview

McAfee MVISION Cloud (Skyhigh) integrates with Zscaler to define and enforce granular governance policies on employees’ cloud usage. IT admin can define policies within McAfee based on several risk, compliance, or security attributes by creating a Service Group and then sync the URLs in this Service Group to Zscaler via an API integration. A Custom Category is created within Zscaler with these URLs and app control policies can be applied to control access to all URLs in this category.

By using CLR, IT or security administrators can control access to risky websites. McAfee uses Zscaler APIs to automatically sync changes from McAfee Service Groups and updates relevant McAfee Custom URL Category within Zscaler. For example, a Service Group is created within Skyhigh for malware and ransomware websites. This Service Group is synced to Zscaler and a custom URL category control policy is applied to block all URLs in this category. If a new threat is added to Skyhigh’s Registry that satisfies the criteria for a malware or ransomware, then the Service Group is updated with the associated URLs. These changes are automatically synced to Zscaler and all access to URLs associated with the new threat are blocked.
3.2 **Configuring Closed Loop Remediation (CLR)**

1. To setup the CLR integration with the Zscaler edge device, go to the ‘Integration’ option on the Navigation bar.

2. If the Zscaler integration is already configured, you will have to enter the API credentials to sync service groups with the Zscaler Cloud. Click on ‘Provide API Credentials’. 
3. Enter the Zscaler tenant credentials. You are required to enter the 'User Name', 'Password', and 'API Key' (see screenshot for #4). Then, check the box that acknowledges that McAfee will store these credentials for continuous sync with Zscaler.
4. Download API key from Zscaler Admin Console.
   
a. Navigate to Administration > API Key Management. The API key has been blanked out in the below screenshots for privacy purposes.
b. Zscaler recommends creating an Administrator account with restricted Functional scope to associate with Zscaler-McAfee Closed Loop Integration.

5. After the credentials are entered, McAfee establishes a connection with Zscaler via APIs. When the connection has been established, you can see the ‘Status’ shows ‘Connected’.
6. To sync service groups with Zscaler, click on the ‘Edit Integration’ button.

7. Make sure that Zscaler is included in the list of appliances. Also, if you want the custom categories in Zscaler to have an SHN- prefix, select that option here. This allows you to identify the custom categories that are synced with McAfee without having to open them.
8. Choose the Service Groups you want to sync with Zscaler. Check the ‘Require Approvals’ option if you want to approve all changes that are synced to Zscaler.
9. Select the recipients who will receive an email summary of URL changes that are pending approval, were automatically applied to a device, or need to be downloaded and applied manually.
10. Review the integration summary and hit ‘Save’ to configure the integration with Zscaler. All Service Groups for which ‘Require Approvals’ is not selected will be synced with Zscaler at this time. If ‘Require Approvals’ is selected then, the pending changes need to be Approved after the integration is configured.
11. You can see the sync status of the Service Groups and the number of URLs that are synced with Zscaler.
12. In the Zcaler tenant, the synced service groups can be found under Administration>Access Control>URL Categories and in the 'User Defined' section.
13. When you edit the Custom Category, you can see that the number of items matches the number of URLs in the Service Group. You can also see a comment in the ‘Description’ section that says that this custom category is integrated with a McAfee Service Group.

14. Now, you can apply app control policies within Zscaler to allow/block/caution access to URLs in the Custom Category. If there a change in the changes in McAfee Service Group, the change is being automatically synced to the Zscaler Custom URL Category.
15. Now, you can apply app control policies within Zscaler to allow/block/caution access to URLs in the Custom Category. The changes in McAfee Service Group are automatically synced to the Zscaler Custom URL Category.

16. On the Zscaler admin console, Go to Policy > URL & Cloud App Control
17. Create a URL filtering policy by selecting the URL category and the associated action.
Appendix A: Zscaler Resources

Zscaler: Getting Started
https://help.zscaler.com/zia/getting-started

Zscaler Knowledge Base:
https://support.zscaler.com/hc/en-us/?filter=documentation

Zscaler Tools:
https://www.zscaler.com/tools

Zscaler Training and Certification:
https://www.zscaler.com/resources/training-certification-overview

Zscaler Submit a Ticket:
https://help.zscaler.com/submit-ticket

ZIA Test Page
http://ip.zscaler.com/

Zscaler and McAfee SkyHigh Security Cloud Solution Brief
5 Appendix B: McAfee Resources

McAfee MVISION Cloud (Skyhigh Networks)
https://www.skyhighnetworks.com/

McAfee Cloud Security University
https://www.skyhighnetworks.com/cloud-security-university/

McAfee MVISION Cloud Submit a Ticket:
https://skyhighnetworks-support.secure.force.com/Webtcase