# Table of Content

1. Introduction .......................................................................................................................... 2
2. Advanced Malware Prevention ............................................................................................ 2
3. Intelligence Intrusion Detection & Prevention ................................................................. 2
4. Web Filter ............................................................................................................................. 2
2. Supported AP Models ........................................................................................................... 3
3. Getting Started .................................................................................................................... 3
4. Enabling Wedge Security Service Add-on ........................................................................... 4
4.1. Applying voucher .............................................................................................................. 4
4.2. License control for APs ................................................................................................... 6
4.3. Preparing for SSL/TLS Traffic Scan .............................................................................. 8
5. Checking License Status ..................................................................................................... 12
7. Remark ................................................................................................................................ 13
1. Introduction

This document is to provide an instruction for setting up the Wedge Security Service add-on on ecCLOUD. Wedge Security Service Add-on is ecCLOUD’s real-time threat prevention service, provided by Wedge Networks' Cloud Network Defense (WedgeCND). After subscribing to this service, the add-on software will be installed on your device to establish a fast VPN tunnel to connect to WedgeCND in the cloud. Security functions are applied to network traffic routed through the tunnel to protect the device and the endpoints connected to it.

Wedge Security Service Add-on provides the following security functions. In addition to these security inspections, it also provides security event reports.

1.1. Advanced Malware Prevention

Blocks any malware from reaching endpoints in the network.

- **Antivirus**: Signature and heuristic based antivirus with dual antivirus engines to detect most of known malware, such as Viruses, Trojans, Worms, Backdoors, etc.
- **AI Anti-Malware**: Artificial intelligence machine learning based malware detection for unknown and never-seen-before malware, such as APT, Zero-day, and Ransomware.
- **Malware Analyzer**: Sandbox based malware detection for greyware and suspicious code, data and files.

1.2. Intelligence Intrusion Detection & Prevention

Mainly protects the hosts and servers in the network from external attacks.

- **Exploit**: Prevent from exploits on different applications, including PDF readers, Microsoft RDP, Windows Media Player, VNC Server, Java-based programs, JavaScript, etc.
- **BOT Command & Control**: Inspect traffic from a list of botnet command and control servers.
- **SQL Injection**: Prevent from compromising SQL-based RDBMS.
- **DoS**: Detect and block Denial-of-Service attack.
- **Critical Infrastructure Protection**: Inspect insecure data transfer methods and known vulnerabilities of various SCADA software packages, such as PcVue, Sunway ForceControl, Siemens FactoryLink, etc.

1.3. Web Filter

Provides a safe Internet usage environment by detecting and blocking all categorized websites and URLs containing malicious content, spam, phishing, fraud, spyware, adware, and more.

- **Malware sites**
- **SPAM URLs**
- **Confirmed SPAM sources**
• Unconfirmed SPAM sources
• Phishing and other frauds
• Spyware and adware

2. Supported AP Models

For the time being, Wedge Security Service add-on is supported on the AP listed below.

<table>
<thead>
<tr>
<th>Model</th>
<th>Supported versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP101</td>
<td>11.6.5</td>
</tr>
</tbody>
</table>

3. Getting Started

Before subscribing to the security service, please make sure the AP is on the support list and managed by ecCLOUD. For how to register an AP to ecCLOUD, please check the instructions in the Edgecore Help Center (https://support.edge-core.com/hc/en-us/sections/900000350566-ecCloud) or the ecCLOUD user manual (https://wifi.edge-core.com/assets/Document/UserManual/EC_ecCLOUD_UserManual.pdf).

Note:
• In current version, only router mode SSID is supported for Wedge Security Service.
4. **Enabling Wedge Security Service Add-on**

4.1. **Applying voucher**

   i. Go to “Add-ons” page. Find Wedge Security Service add-on and click the “SUBSCRIBE / REDEEM” button to get to the add-on subscription page.

   ![Add-on subscription page](image1)

   ii. In the subscription page for Wedge Security Service add-on, click the “APPLY VOUCHERS” button. A modal will pop-up for filling the voucher codes.

   ![Modal for filling voucher codes](image2)
iii. Get a voucher code from Edge-core team. Enter the voucher code and click the “ADD” button. The voucher code is valid, the voucher value will be listed below. After inputting all of your valid voucher codes, click the “APPLY” button. A dialog box will be popped-out for your confirmation. Click “CONFIRM” button if you would like to apply the vouchers.

Note that the voucher code will be consumed after click “CONFIRM” button. The applied voucher cannot be recovered or transferred to another cloud.
4.2. License control for APs

i. Go to the subscription page for Wedge Security Service add-on. Click “MANAGE LICENSE” button to check the device list.

![Image of Wedge Security Service subscription page]

ii. Select the AP you would like to apply the license, open the “ACTIONS” menu and click “Apply License”.

![Image of Wedge Security Service license management page]
iii. A dialog box will pop-up for your confirmation to apply the license. First, you may filter the licenses by the available duration. For example, inputting 360 and click “SUBMIT” button, the licenses with more than 360 days of available duration will be counted in. After filtering the license duration, clicking “APPLY” button then the system will automatically select a license from the pool and apply to the selected APs.

![License Application](image)

iv. After the license is applied to an AP, the “ACTIVATED AT” and “EXPIRED AT” will be shown. Note that the license is for 1 year from the time it is applied to an AP.

![License Application](image)

v. Check the Activity page. There should an Addon Management activity to update the add-on license to the AP. Initially, the status would be “Scheduled”, which means this task is scheduled to be executed. If the status becomes “Running”, it means that the installation of the related packages is in progress. When the status becomes “Completed”, the AP is ready to provide service.

![Manage Licenses](image)

![Activity Page](image)
4.3. Preparing for SSL/TLS Traffic Scan

To allow Wedge Security Service to scan SSL/TLS traffic for providing further protection, it is required to download and import the Wedge certificate on your devices. The steps below shows an example to import the Wedge certificate on a Windows 10 device.

**Note:** With the steps below, the SSL/TLS traffic via **Microsoft Edge**, **Google Chrome**, or command prompt will be scanned. For those using **Mozilla Firefox** browsers, you will need to install the Wedge Security certificate separately as it does not use the Microsoft Certificate key store.

i. Download and save the Wedge certificate from [https://wedgenetworks.com/Certificates/wedgearp-ca.cer](https://wedgenetworks.com/Certificates/wedgearp-ca.cer).

ii. Once downloaded, double click on the file "wedgearp-ca.cer". Press Open once the following dialog box appears.

![Open File - Security Warning](image)

iii. The Certificate dialog box will appear. Click on "Install Certificate" to install.
iv. The "Certificate Import Wizard" dialog box will appear. Click on the radio button "Local Machine" and click Next to continue.

v. Windows will flash another screen asking for permission to make changes. Click on Yes.

vi. Choose the radio button "Place all certificates in the following store" and then click on the Browse button.

vii. The following "Select Certificate Store" dialog box will appear. Click on "Trusted Root Certificate" and then OK.
viii. Then, click Next as shown:

ix. The following dialog box will appear. Click on Finish to complete the installation.

x. To verify that the certificate was properly installed, go to the Start menu and type in "Internet Options" and click on Open.
xi. Once the Internet Properties dialog box comes up, navigate to the Content tab and click on Certificates to get the Certificates dialog box.

xii. Click on the "Trusted Root Certification Authorities" tab.

xiii. Scroll down until you see the WedgeARP Certificate for verification.
5. Checking License Status

The summary of the license information is listed in the add-on subscription page. The number of available licenses and the number of in-use licenses are listed based on the length of the license duration.

By clicking the “DETAIL” button, you can check the details of all the licenses. In the license details page, you can check whether the license is activated or not, and even check which AP on which site the license is applied to. The original license duration and the available license duration for each license are also shown in the details.

<table>
<thead>
<tr>
<th>License Duration</th>
<th>Available</th>
<th>In Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>12 Months</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>24 Months</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>


i. Go to the subscription page for Wedge Security Service add-on and scroll down to the “Report” section. Select the start date and the end date, and then click “CREATE REPORT” button to generate the security report for the selected period.
ii. After clicking the “CREATE REPORT” button, a hint message will pop out. As the message described, it may take some time for the report to be generated. You may refresh the page and check whether the download link is ready.

![Report Generator](image)

iii. The download link will appear once it is ready. Click the “DOWNLOAD” link to get the report in PDF format.

![Report](image)

**Note:**
- At most 6 reports can be displayed. Any additional reports will overwrite the oldest one.

7. **Remark**

For more information, please submit a ticket at [https://support.edge-core.com/hc/en-us](https://support.edge-core.com/hc/en-us), or just send an email to ecwifi@edge-core.com.