# Trend Micro™ Cloud Edge 5.5 Cloud-Powered UTM

## Best Practice Guide

Anti-Spyware Anti-Spam Antivirus Anti-Phishing Content & URL Filtering

**Released:** August 2019

# Preface

Welcome to the *Trend Micro Cloud Edge 5.5 Best Practices Guide*. This document is designed to help partners develop a set of best practices when deploying and managing Cloud Edge security solutions.

Trend Micro Cloud Edge is a Cloud-Powered UTM (Unified Threat Management) device. It brings together the benefits of a next-generation on-premises firewall and the convenience of Security-as-a-Service delivered from the cloud. Through the combined capabilities, Cloud Edge inspects and filters your network packets to stop sophisticated threats at the gateway.

This document covers the best practices for ease of deployment, superior security and performance, plus monitoring and reporting. It was written for administrator who have the need to deploy Cloud Edge devices and manage the operation regularly. It is not meant to be a replacement for the complete set of user manuals, which can be found at: http://docs.trendmicro.com/en-us/smb/cloud-edge.aspx:

- Deployment Guide (for Managed Service Providers)
- License Provision Quick Start Card (for Managed Service Providers)
- Cloud Edge Quick Start Card (for on-premises customers)
- Cloud Edge Cloud Console Online Help
- Readme

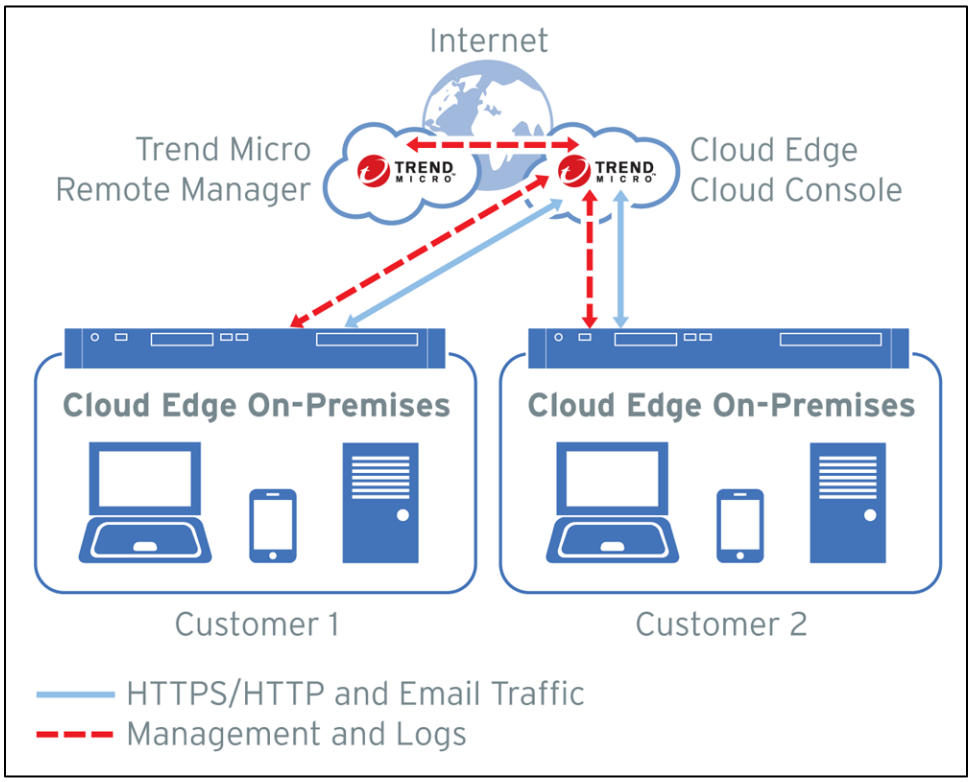
At the time of writing this guide, the latest Cloud Edge version is 5.5. Other versions may have different features or default values that users should pay attention to and adjust the best practices accordingly.

# Table of Contents

# Chapter 1: Deployment

## 1.1 > Provision Licenses by MSPs

MSP partners can follow the **Deployment Guide** or the **License Provision Quick Start Card** for proper licensing and deployment of Cloud Edge appliances to their customers. As a quick recap, **Trend Micro Remote Manager** is the starting point where all relevant tools can be launched from.




### 1.1.1 Create Service Plans

Access Trend Micro **Licensing Management Platform** (LMP) to create the **Service Plans** for Cloud Edge. Create the Cloud Edge service plan, this may include the following components:

1. **Cloud Edge** – required license for appliance firmware

2. **Virtual Analyzer** – license for sandbox emulation
3. **Log Forwarding Service** – license for forwarding logs to a 3rd party log management system

Take note of the following:

- For **Version type**, **'Full'** is recommended since Cloud Edge is an appliance.
- For **Data Center** location, select one that is closest to your physical location.
- For **Managing product/service**, check [✓] **Remote Manager** to allow remote management.
- The **Initial license period** can be either Monthly or Yearly, according to your marketing strategy.
- Enable license **Auto-renewal** based on your marketing setup

### 1.1.2 Create Customers

On LMP, create **Customers** and fill out the required information like **Company**, **address**, **city**, **state**, **account name**, **contact person's name** and **email addresses**. You will want to **Send account creation email 'immediately upon creation'** of a customer. And finally, it is easier to **Assign Service Plan** as you create a Customer. Set **Unit per license** based on the number of Cloud Edge appliance you will deploy for the customer created.

### 1.1.3 Add New Gateways

On **Remote Manager**, select the new Customer and launch the **Cloud Edge Cloud Console**. This is where a Cloud Edge gateway appliance can be registered using its serial number. It is recommended you test register first a new gateway locally before actually deploying the appliance to the customer site. This way you can troubleshoot the registration process easily in case there are any issues. Once the test is complete you can de-register the gateway if needed. Reset the box back to factory default before shipping it out to the end customer so the network configuration can be configured locally.

# 1.2 > Deploying Appliances On-Premises and Cloud Activation

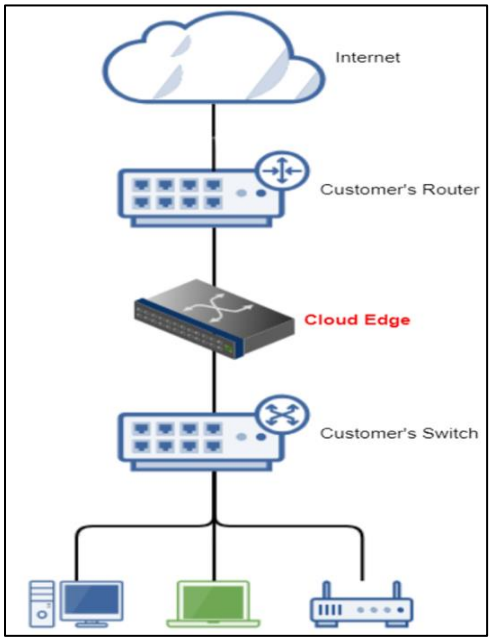
Refer to the **Quick Start Card** for deploying appliances at customer sites.

## 1.2.1 Deployment Mode

Bridge mode vs. Routing mode recommendation:

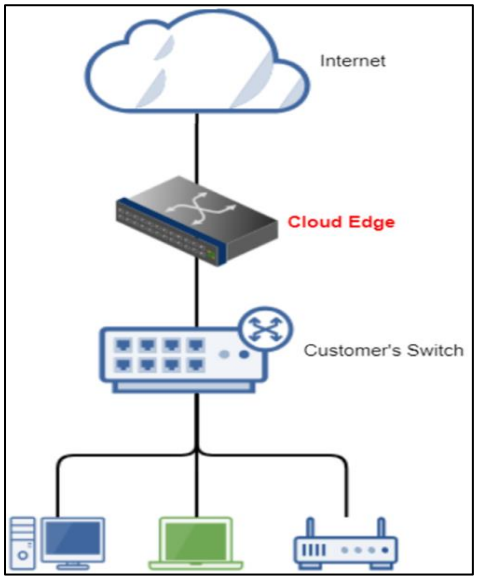
### Cloud Edge Bridge Mode

Choose **Bridge Mode** whenever possible, you would typically use a Bridge Mode deployment on a private network behind a router and in front of a switch. This is set by toggling the physical switch at the back of the Cloud Edge appliance, which is also set on Bridge as default.
Bridge mode allows for drop-in deployment of the Cloud Edge box without modifying the existing network, Cloud Edge can add superior scan and threat protection.



### Cloud Edge Routing Mode

Configure a Cloud Edge gateway to function as a router while in Routing Mode. The gateway is visible on the network and acts as a layer 3 routing device with security scanning and control capabilities. You normally replace existing Router on the network with Cloud Edge appliance in this mode or deploy the appliance between router and switch. Necessary configuration changes is needed on the router and the Cloud Edge appliance.




## 1.2.2 Quick Setup

From the On-Premises Console > Quick Setup page:

- **Uplink configuration** – Choose **DHCP** when possible, if not assign a static IPv4 address, subnet and DNS on the bridge interface. PPPoE is also available on Routing mode. [**Start Configuration Test**] should be used to check if the appliance can access DNS and connect to the Cloud Edge Cloud.
- **System settings – Enable NTP server** is recommended for setting the appliance clock automatically.
- **Serial number** is available on the **Cloud Edge On-Premise Console>Administration>Device Management page.**
  It's also located under the Cloud Edge Appliance.

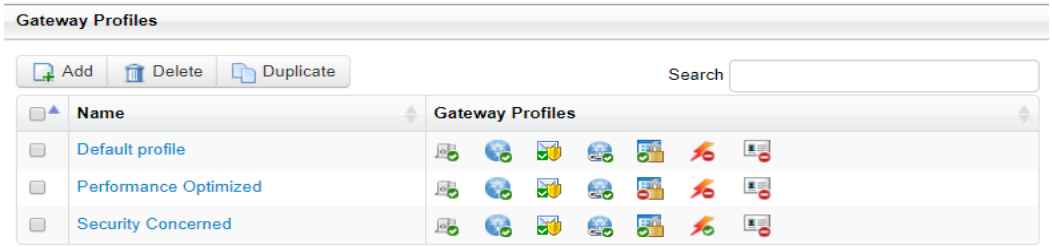
- DHCP service is also available under **On-Premises Console > Network > Services**: Enabling DHCP service for the LAN interface is recommended
  (Note: After device is registered, DHCP for LAN2,LAN3,MGMT can only be edited in Cloud Edge Cloud Console.)
- Register the gateway by accessing the **Cloud Edge Cloud Console**, Go to **Gateways >Register New Gateway**

# Chapter 2: Security Configuration

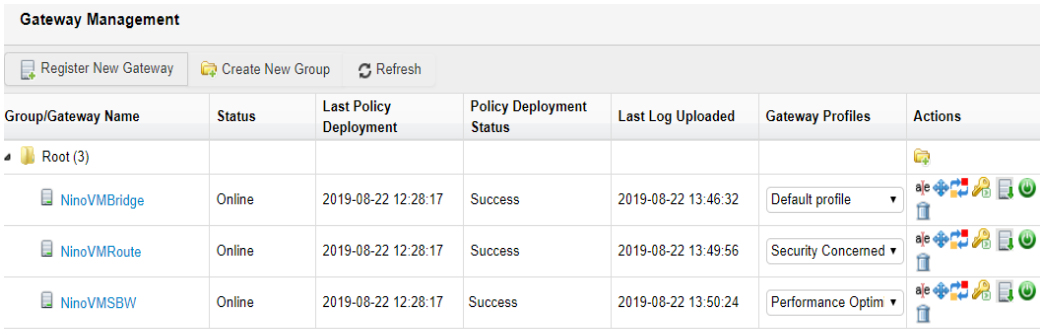
After successful registration, Cloud Edge appliances can be centrally configured and managed from the Cloud Edge Cloud Console. You can configure each gateway for its unique network settings and set up **Policy Rules** and **Gateway Profiles** for common security settings that are to be shared across multiple gateways.

## 2.1 > Security Gateway Profiles

From Cloud Edge Cloud Console, go to: **Policies > Gateway Profles**.
Consider at least three scenarios when creating additional Gateway Profiles:




You can then assign the Gateway Profiles under **Gateways** of the Cloud Edge Cloud Console:




### 2.1.1 Normal User

**Gateway Profile A – Normal User** - All settings are left at their default values. This gives you the best balance between security and performance.

### 2.1.2 Security-Concerned User

**Gateway Profile B – Security-Concerned User** – Enhance security by inspecting more in depth and block potentially malicious traffic. Enable the following settings at **Polices>Gateway Profiles > Default Profile**:


- **IPS** – Change IPS action from [Monitor] to [**Block**], and [**Enable**] **Advanced Settings**, then use **Rule Filter** to set the **Minimum severity** to '4-high'. Doing this will block IPS detections with severity '4-high' and '5-critical'.
- **Anti-Malware** – In addition to [**Enable Cloud Scan]**, also [**Enable Smart Scan]** for leveraging the Smart Scan real-time signature server in the cloud.
- **Email Security**
  - **[Enable] Virtual Analyzer** for leveraging the cloud sandbox to analyze suspicious files (license required).
  - [**Enable**] **Predictive Machine Learning** to leverage AI in detecting previously unknown threats, also change the **Action** from [Monitor] to [**Block**] or [**Add Tags**].
  - Under Anti-Spam, **[Enable] Email Reputation** and [**Enable**] **Business Email Compromise (BEC)** detection.
- **Web Reputation** – choose **Medium** for sensitivity level
- **HTTPS** – Turn [**On**] HTTPS Scanning , uncheck all URL Category under Exceptions list
- Remember to [**Save**] and [**Deploy**] the gateway profile

For added security, you can also define additional **Policy Rules** to block unwanted Applications or URL Categories at the firewall level, for example:

- Add a Policy Rule named "Block Internet Security URLs" > **Select Traffic Type > URL Category > Internet Security**, and set the Action to [**Block**]
- Add a Policy Rule named "Block Gaming Applications" > **Select Traffic Type > Application Group > Game**, and set the Action to [**Block**]
- The newly added Policy Rules should come before the "Default policy rule". The result may look something like this:


Configure Network Access Control under **Gateways>Select Gateway**:

- **WFBSS Endpoint Protection:**
  Enable when client is also using Worry Free Business Security Services, this feature blocks internet access on devices that are out of compliance.
  - Turn **On** feature as it's disabled by default
  - Choose **[Block]** for both of the criteria:
    - Clients without Agents
    - Clients with Agents using out-of-date patterns
  - Add the IP pool of your network on the **Protection list**, this would ensure traffic from unknown devices on your network will be blocked
  - Add IP address of devices which you cannot install Worry Free Services Security Agent under **Exception list**
  - Click **Apply**
- **Suspicious Endpoint:**
  Configuring Suspicious Endpoints provides network access control for endpoints on which C&C callbacks above a configured threshold are detected.
  - Turn feature **On**, as it's disabled by default

- Use default threshold, which is 50 C&C callback events in 1 hour
- Set action to **Block**
- Click **Apply**

### 2.1.3 Performance-Optimized User

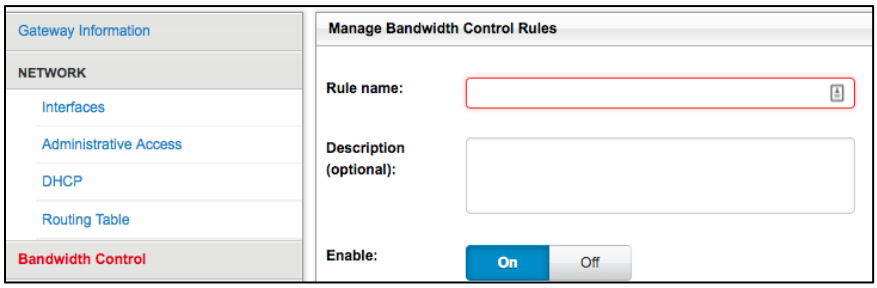
**Gateway Profile C – Performance-Optimized** – Uses various techniques to speed up the traffic for specified users/groups.

- Add a Policy Rule named "Bypass Trusted Sources" – define specific **Policy Rules** for trusted IP's and users/groups and set the Action to [**Bypass**], which will bypass threat scanning for traffic coming from these sources.
- Or set a bypass policy rule for local to local network traffic
- **HTTPS** – Leave HTTPS Scanning at the default [**Off**] setting under Gateway Profiles

You can also set up gateway-specific **Bandwidth Control Rules** which can be used to prioritize traffic among critical vs. non-critical applications. This feature must be configured from the Cloud Console:

**Gateways > [gateway name] > Bandwidth Control**

- Bandwidth Control – create specific **Bandwidth Control Rules** for selected application groups and/or network services. Specify rules with **Guaranteed bandwidth** when you want minimal bandwidth allocated for certain speed-sensitive applications; on the other hand, specify rules with **Maximum bandwidth** to limit the bandwidth-hungry applications from hogging all the bandwidth and cause other applications to suffer.



# Chapter 3: Miscellaneous

## 3.1 > Monitoring and Reporting

### 3.1.1 Dashboard

From the **Cloud Edge Cloud Console > Dashboard** page, you can see the Security Status and Traffic Status at a glance.

### 3.1.2 Analysis & Reports

From the **Cloud Edge Cloud Console > Analysis & Reports** page, you can view predefined log statistics or set up your own queries and save them as favorites.

Scheduled reports can also be defined to run on a daily, weekly, or monthly interval. This is a time-saving feature to send report notifications via email so a summary report can always be ready at your inbox when you start a new day, a new week, or when you need to generate a month-end report for the management.

## 3.2 > Administration

### 3.2.1 User & Accounts

**Cloud Console > Administration > Accounts Management**:

Create **[Read only]** accounts for people who need access to Cloud Console to view logs/reports, but do not need the privilege to modify configurations.

### 3.2.2 Administrator Alerts

**Cloud Edge Cloud Console > Administration > Administrator Alerts**: set **Enable** to [**On**]

Alert Type:

- [**Check**] C&C Callbacks [50] events occur in [1 hour]

- [**Check**] Gateway status change & Mail security status change

  **Remote Manager > Administration > Configure notifications**

Fine-tune Event Notification Settings with adjustable Alert Thresholds.

### 3.2.3 Scheduled Updates

Normally, **Daily** component (patterns/engines) update is sufficient. However, during a malware outbreak, changing the update period to **Hourly** may be desired.

Weekly firmware updates is advised, choose the default or set this during business off hours.

### 3.2.4 Administrative Access

Configure different type of management services thru the Cloud Edge Cloud Console.
Access **Gateways>Select Gateway>Administrative Access** and specify the IP range or IP address that will need access to the Cloud Edge Appliance via On-premise console, ping and SSH.

### 3.2.5 Certificate Management

Navigate to **Administration>Certificate Management.**
Import your own certificate or export the certificate that Cloud Edge use to decrypt SSL traffic, install the exported certificate into end user trusted certificate store.
This would help avoid certificate warning displayed on browsers when accessing HTTPS website.