Trend Micro™ Cloud Edge

July 2023

Administrator's Guide

Document Part No.: APEM09742/230620

Release Date: July 2023

Protected by U.S. Patent No.: Patents pending.

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

https://www.trendmicro.com/download/documentation/rating.asp

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that Cloud Edge collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Notice:

https://www.trendmicro.com/privacy

Table of Contents

Preface

Chapter 1: Cloud Edge Introduction

Chapter 2: Best Practices for Cloud Edge Deployments

Chapter 6: Cloud Edge Cloud Console

Chapter 7: Cloud Edge On-Premises

Chapter 8: Technical Support

Index

Preface

Welcome to the Trend Micro™ Cloud Edge Administrator's Guide. This guide introduces Cloud Edge and explains how to use Trend Micro™ Remote Manager, register gateways and synchronize accounts in Cloud Edge Cloud Console, and deploy the Cloud Edge gateway at consumer office locations.

Documentation

The documentation set for Cloud Edge includes the following:

TABLE 1. Product Documentation

DOCUMENT	DESCRIPTION
Online Help	The Online Help contains explanations of Cloud Edge components and features, as well as procedures needed to configure Cloud Edge. Cloud Edge Cloud Console provides embedded, context-sensitive help on the right-side of each screen.
Administrator's Guide	The Administrator's Guide is a PDF document that introduces Cloud Edge and explains how to use Trend Micro™ Remote Manager, how to register gateways and synchronize accounts in Cloud Edge Cloud Console, and how to deploy the Cloud Edge gateway at consumer office locations.
What's New	The What's New file contains a description of new features.
Support Portal	The Support Portal is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Support Portal, go to the following website: https://success.trendmicro.com

View and download the documentation at:

http://docs.trendmicro.com/en-us/smb/cloud-edge.aspx

Audience

The Cloud Edge documentation is written for IT administrators and security analysts. The documentation assumes that the reader has an in-depth knowledge of networking and information security, including the following topics:

- Network topologies
- Database management

- Policy management and enforcement

The documentation does not assume the reader has any knowledge of threat event correlation.

Document Conventions

The documentation uses the following conventions:

TABLE 2. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documents
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
Navigation > **Path**	The navigation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface
 **Note**	Configuration notes
 **Tip**	Recommendations or suggestions
 **Important**	Information regarding required or default configuration settings and product limitations

Convention	Description
 **WARNING!**	Critical actions and configuration options

Requirements

Cloud Edge utilizes Amazon Elastic Compute Cloud™ and is subject to the requirements provided by Amazon Web Services. Learn more at http://aws.amazon.com/ec2/.

Table 3. Supported Web Browsers

Browser	Version
Mozilla Firefox™	80 or later
Google Chrome™	83 or later
Microsoft Edge™ (Chromium)	85 or later

Chapter 1

Cloud Edge Introduction

Cloud Edge Overview

Trend Micro Cloud Edge brings together the benefits of a next-generation on-premises firewall and the convenience of security as a service for MSPs (Managed Service Providers). Cloud Edge intelligently combines application control with user and port identification for multilayer protection. URL filtering, bandwidth control, intrusion protection, anti-malware scanning, email security, and web reputation security provide additional protection from network breaches and business disruptions. By deeply scanning and filtering network packets on-premises or through the cloud, Cloud Edge stops threats at the gateway. Virtual Private Network (VPN) support also secures connections from mobile devices, corporate sites, and remote employees.

Deploy the Cloud Edge gateway to customer offices and use Cloud Edge Cloud Console to centrally control user access and security policies. Optionally, you can use single sign-on to access Cloud Edge Cloud Console through Trend Micro Remote Manager. Remote Manager works with Cloud Edge by providing a single point of entry to access graphical reports and summarized dashboard data for supported gateways and Trend Micro products. Remote Manager also helps you to manage licensing and billing of multiple customers.

The following illustration shows how Cloud Edge works.

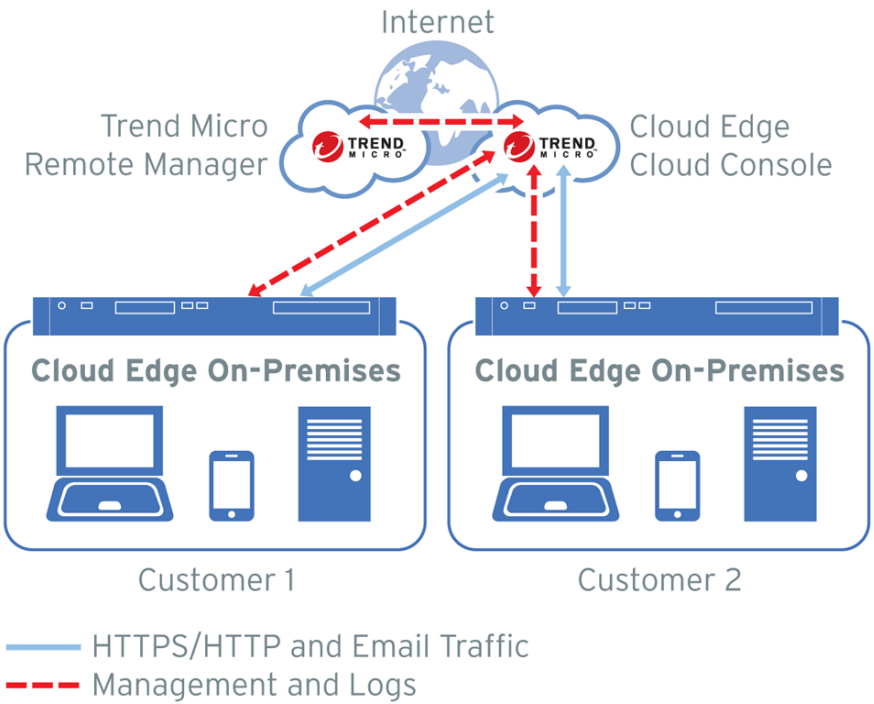


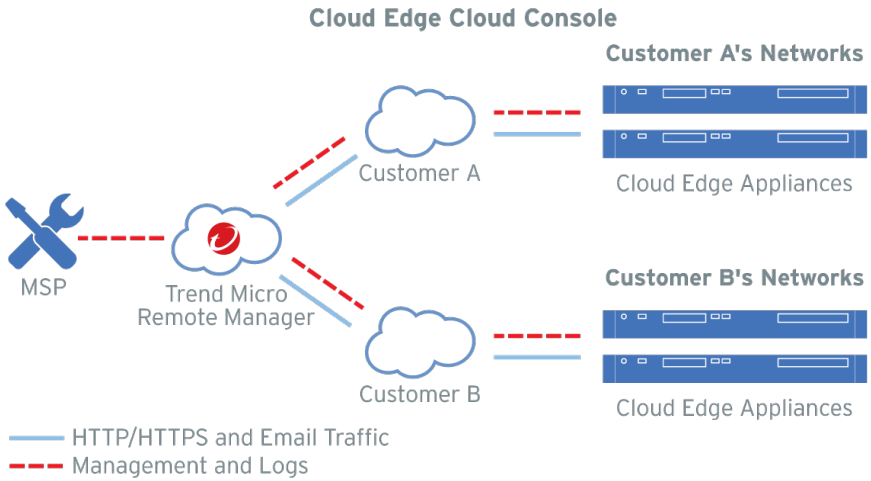
TABLE 1-1. Cloud Edge Components

COMPONENT	DESCRIPTION
Cloud Edge Cloud Console	Cloud Edge Cloud Console is a Security-as-a-Service management console hosted in the AWS (Amazon Web Services) cloud. Cloud Edge Cloud Console controls user access and security policies on Cloud Edge gateways geographically distributed across any number of networks. Access Cloud Edge Cloud Console dynamically in the cloud, anytime.

Component	Description
Cloud Edge gateways	Cloud Edge gateways are cloud-powered UTM (Unified Threat Management) devices engineered to provide network security. Cloud Edge gateways enforce next-generation security at customer locations by scanning and blocking malicious content as on-premises firewalls or by invisibly monitoring for security threats as network bridges.
Trend Micro Remote Manager	Trend Micro Remote Manager is a single pane of glass management console for Trend Micro channel partners and MSPs, providing a real-time security dashboard and reporting across all customers as well as license management. Remote Manager provides access to graphical reports and summarized dashboard data for supported gateways and Trend Micro products. Remote Manager also manages licensing and billing of multiple customers. Optionally, you can use single sign-on to access Cloud Edge Cloud Console through Remote Manager.

How Cloud Edge Works

The following illustration shows how a typical Cloud Edge customer deployment is implemented.



1. Deploy Cloud Edge gateways to customer offices.
2. Use Cloud Edge Cloud Console to centrally manage user access and security policies.
3. Single sign-on to Cloud Edge Cloud Console through Trend Micro Remote Manager.
4. Use Remote Manager as a single point of entry to access graphical reports and summarized dashboard data for supported gateways and Trend Micro products. Remote Manager also helps you to manage licensing and billing of multiple customers.
5. Logs are sent from the Cloud Edge gateways to Cloud Edge Cloud Console and Remote Manager.

After customers deploy Cloud Edge on-premises, the customers configure each gateway as a firewall at the gateway or as a network bridge invisibly scanning and blocking malicious content. With deep content inspection, the Cloud Edge gateway examines the entire traffic as it passes through the gateway, searching for signature matching, behavioral analysis, regulatory and compliance analysis, and session correlation to previous session history.

MSPs use Cloud Edge Cloud Console to manages policies on all traffic passing through registered Cloud Edge gateways geographically distributed across any number of networks. Secure traffic forwarding through the cloud initiates after the MSP registers the Cloud Edge gateway to Cloud Edge Cloud Console.

When email security is set to cloud scan (the default), all email requests are routed directly through the cloud for inspection. When routed through the cloud, a Cloud Edge cloud back-end service inspects, analyzes, and filters the request based on policies set by the managed service provider. If the request is allowed, traffic routes to the user. If the request is not allowed, for example a request to a forbidden URL category, the request is blocked and the user is notified.

MSPs can use Remote Manager to manage licensing and billing of multiple customers leveraging Trend Micro services: LMP (Licensing Management Portal) or CLP (Customer Licensing Portal). License changes or updates synchronize on the back end and display in Cloud Edge Cloud Console and Remote Manager.

Main Features

The following table describes Cloud Edge Cloud Console key features. Technology components are designed to integrate and optimize performance for gateway management through the cloud.

TABLE 1-2. Cloud Edge Cloud Console Features

FEATURE	DESCRIPTION
Gateway management	Centrally manage multiple Cloud Edge gateways through one cloud console. Manage intranet security modes for Cloud Edge gateways with hardware switch chipset. Manage wireless network access control and manage wireless client connections for Cloud Edge wireless gateways. Use Cloud Edge Cloud Console to create and manage HA groups. You can create an HA group from two registered gateways to provide high availability access. If one gateway is down, then the other gateway will take over and ensure that the network traffic continues.
Multilayer Protection	Cloud Edge identifies when users and user groups access the network, which port they used, and what web-based applications were accessed to protect against network infiltration. Enforcing security policies based on these multiple layers of identification fight against emerging, sophisticated threats that may bypass traditional security solutions.
Policy management and deployment	Deploy policies across any number of managed gateways. Policy management options include: • Creating policies for specific gateways, interface groups, users/ user groups, IP addresses, FQDNs, geolocations, services, application groups, URL category groups, schedules, and security profiles • Creating security profiles for advanced policy functionality including Intrusion Prevention System (IPS), anti-malware, email security, Web Reputation Service, HTTPS inspection, anti-denial-of-service, and endpoint identification • Approving or blocking URLs that override policy rules • Sending notifications when a policy event occurs
Plug–and–Play Deployment	Send the Cloud Edge gateway to customer locations without opening the package. Your customers can unpack the box and follow the instructions in the provided documentation. After the gateway is manually registered and is online, the gateway receives your custom security policy configuration.

Feature	Description
Intelligent dashboard	View activity occurring within the network and spanning across one or more gateways. Widgets represent the core components of the dashboard and contain visual charts and graphs that allow you to track threats and associate them with accumulated log data.
Log analysis and reports	View and analyze aggregated log and event data about traffic bandwidth consumption, threat detections, Web 2.0 application usage, web browsing activity, and policy enforcement. Save log query filters as log favorites to reference later or generate custom reports for further investigation. View usage date for policy rules (only available if customer is running all Cloud Edge 6.0 or later gateways).
Quality of Service	Control bandwidth consumption to reduce network congestion by controlling communications, blocking unwanted traffic, and allocating critical traffic or services the appropriate bandwidth.
URL filtering	Configure URL filtering policies to deny or allow web domain access. You can configure a policy to scan traffic for specific URL categories (for example, “Adult” and “Gambling”) to filter traffic. When a user requests a URL, the gateway first looks up the category for that URL and then controls access based on policy settings.
Application control	Control more than 3400 application types running across any port, including applications using specific clients (Skype, BitTorrent, P2P) or Web 2.0 technologies within websites (social networking, web mail, streaming media).
Security profiles	Perform advanced policy configurations targeting security profiles. • Intrusion prevention • Malware protection • Email security protection • Web reputation • HTTPS inspection • Denial of Service attack prevention • Endpoint identification

Feature	Description
User management	Synchronize user information across gateways.
User VPN	User Virtual Private Networking (VPN) extends VPN functionality to remote users, enabling users to securely communicate sensitive information to networks and servers over the IPv4 VPN tunnel, using dial-up (including broadband), LAN, and mobile connections. Not available for Cloud Edge gateway models that do not support VPN.
Site–to–Site VPN	A Site–to–Site Virtual Private Network (VPN) allows offices in multiple fixed locations to establish secure IPv4 connections with each other over a public network such as the Internet. Not available for Cloud Edge gateway models that do not support VPN.
Log Forwarding Service	The Log Forwarding Service is a licensable service that enables Cloud Edge Cloud Console to forward logs for licensed gateways to external applications. Managed Service Providers can assign the Log Forwarding Service service plan to a customer.
Gateway System Status and Events/ Logs	For each gateway, you can view information about the gateway's system status. You can also view events/logs for network, system, and VPN events (if available), and for policy enforcement logs. VPN events are not displayed for Cloud Edge gateway models that do not support VPN.
Gateway Troubleshooting Tools	You can use ping, traceroute, and ARP to troubleshoot gateway network IPv4 connectivity issues.
Integration with Worry Free Business Security Services	Cloud Edge WFBSS Endpoint Protection integrates with WFBSS to provide a compliance check for WFBSS endpoints who have an out-of-date WFBSS Security Agent pattern or who do not have the WFBSS Security Agent installed. Cloud Edge can provide network access control for out-of-compliance endpoints.
Network access control for suspicious endpoints	Cloud Edge provides security services by providing compliance checks for endpoints to see if C&C callbacks above the configured threshold have been detected. Cloud Edge can provide network access control for endpoints who have exceeded the threshold.

Hybrid Security

Cloud Edge distributes security features on-premises and in the cloud to improve quality of service for network bandwidth and to efficiently enforce policies where needed. Only specific traffic forwards to the cloud for analysis and control based on policies. Management capabilities are available on-premises through the Cloud Edge on-premises console and in the cloud through Cloud Edge Cloud Console. The following table explains the distribution of on-premises and in-the-cloud security capabilities.

TABLE 1-3. Cloud Edge Distributed Security

FEATURE	ON-PREMISES	IN-THE-CLOUD
High Availability (HA) Groups		●
Advanced Firewall Protection	●	
Application Control	●	
Endpoint Management	●	●
Gateway Management		●
Intrusion Prevention System (IPS)	●	
Licensing Management Platform Integration		●
Remote Manager Integration		●
Spam Scanning	●	●
Switch: Software Switch	●	
Switch: Hardware Switch Chipset	●	●
URL Filtering	●	
Virtual Private Networking	●	
Virus and Malware Scanning	●	●

Feature	On-Premises	In-the-Cloud
Advanced Malware Protection with Virtual Analyzer		●
Advanced Malware Protection with Predictive Machine Learning		●
Web Reputation Service	●	●
Wireless Network	●	●

On-Premises Capabilities

The following table explains the Cloud Edge capabilities available on-premises.

For more information about IPv6 support for on-premises capabilities, see *Support for IPv6 on page 1-20*.

Table 1-4. Cloud Edge On-Premises Capabilities

Feature	Description
High Availability (HA) Groups	You can configure two registered gateways as an HA Group to provide high availability access. If one gateway is down, then the other gateway will take over and ensure that the network traffic is not down. An HA Group can also increase network traffic efficiency.
Advanced Firewall	Easily deploy and manage the next-generation firewall by blocking attacks while allowing good application traffic to pass.
Antivirus	Leverage multiple security components and antivirus protection based on application content scanning for better protection with lower latency and improved user experience.

Feature	Description
Spam and Anti-Malware scanning	When email security is set to local scan, Cloud Edge locally manages and provides spam and anti-malware protection. **Note** The default setting for email security is cloud scan. Cloud Edge can automatically change the setting to local scan in certain cases, including if there are network issues.
Email Reputation Services	Use Trend Micro Email Reputation Services (ERS) to detect and block email messages based on the reputation of the mail sender.
IPS	Identify and stop many active threats, exploits, back-door programs, and other attacks, including denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, passing through the device. An intrusion prevention system (IPS) bolsters a firewall's security policy by ensuring that traffic allowed by the firewall is further inspected to make sure it does not contain unwanted threats.
Application control	Automatically discover popular Internet applications and control access to them using policies.
Network configuration	View and edit detected network interfaces, or modify physical L2 and L3 port configurations. The following IPv4 configurations are supported for L3 ports: • Dynamic Host Configuration Protocol (DHCP) • Static route configurations by IP address and netmask • Point-to-point Protocol over Ethernet (PPPoE)
Bridging	Transparently bridge two interfaces and filter network traffic to protect endpoints and servers with minimal impact to the existing network environment. Spanning Tree Protocol (STP) ensures a loop-free topology for any bridged Ethernet local area network. Bridge Mode deployments support IPv6 functionality.

Feature	Description
Software Switch	Configure a Cloud Edge gateway to function as a Software Switch (a variation of Bridge Mode), which eliminates the need for a separate switch in small business environments. Cloud Edge still provides security scanning according to configured policies while configured as a switch. Software Switch deployments support IPv6 functionality.
Hardware Switch Chipset	The Cloud Edge gateway with hardware switch chipset is both a security gateway and a hardware switch. In Bridge Mode, the gateway provides seven LAN switch ports that connect directly to endpoints, which eliminates the need for a separate switch in many business environments. You can also deploy the gateway in Routing Mode if desired. Eight LAN ports are available for internal networks when deployed in Routing Mode. Whether deployed in Routing Mode or in Bridge Mode as a hardware switch, Cloud Edge gateways with hardware switch chipset still provide security scanning according to configured policies. Bridge Mode deployments support IPv6 functionality.
Routing	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. The Cloud Edge gateway locally manages all IPv4 static routes. Routing Mode deployments do not support IPv6 functionality.
Bandwidth control	Reduce network congestion by controlling communications, reducing unwanted traffic and allowing critical traffic or services the appropriate bandwidth allocation.
URL filtering	Create and configure unique URL filtering procedures for different profiles. URL filtering, along with WRS, is part of the multi-layered, multi-threat protection solution.
NAT	Configure Network Address Translation (NAT) policies to specify whether source or destination IPv4 addresses and ports are converted between public and private addresses and ports.

Feature	Description
Services	Configure the following services: • Dynamic Host Configuration Protocol (DHCP) servers
VPN	Configure IPv4 VPNs. • User VPN Configure Virtual Private Network (VPN) with the Layer 2 Tunneling Protocol (L2TP) or Secure Sockets Layer Virtual Private Network (SSL VPN). Allow iOS and Android mobile device users to easily and securely connect back to the corporate environment by utilizing the built-in IPsec VPN clients. No agent installation is required for the mobile devices. • Site–to–Site VPN Create encrypted L3 tunnels by using the Internet Key Exchange (IKE) and IP Security (IPsec) protocols. You can create a single peer-to-peer VPN tunnel, a star VPN topology with one central hub device and up to four spoke devices, or a full-mesh VPN topology of up to five devices. You cannot configure VPNs for Cloud Edge gateway models that do not support VPN.
Logs	View and analyze audit logs, system events, and VPN logs (if available).
Gateway System Status and Events/ Logs	For each gateway, you can view information about the gateway's system status. You can also view information about network events, system events, VPN events (if available), and policy enforcement logs. You cannot view information about VPNs for Cloud Edge gateway models that do not support VPN.
Gateway Troubleshooting Tools	You can use ping, traceroute, and ARP to troubleshoot gateway IPv4 network connectivity issues.

Feature	Description
Integration with Worry Free Business Security Services	Cloud Edge WFBSS Endpoint Protection integrates with WFBSS to provide a compliance check for WFBSS endpoints who have an out-of-date WFBSS Security Agent pattern or who do not have the WFBSS Security Agent installed. Cloud Edge can provide network access control for out-of-compliance endpoints.
Network access control for suspicious endpoints	Cloud Edge provides security services by providing compliance checks for endpoints to see if C&C callbacks above the configured threshold have been detected. Cloud Edge can provide network access control for endpoints who have exceeded the threshold.
Wireless Networks	For Cloud Edge gateways with wireless network functionality, you can configure wireless network access for a main network and a guest network, while controlling access by using MAC address filtering. Cloud Edge provides full security services to both the main and guest networks. You can configure other networking services on the wireless networks including DHCP services, bandwidth control, NAT, VPN access, and network access control for suspicious endpoints.

In–the–Cloud Capabilities

The following table explains the Cloud Edge capabilities available in the cloud.

Table 1-5. Cloud Edge In–the–Cloud Capabilities

Feature	Description
Gateway management	Centrally manage multiple Cloud Edge on-premises gateways through one cloud console. Use Cloud Edge Cloud Console to configure two registered gateways as an HA Group to provide high availability access. Manage existing HA groups, including modifying the configuration, enable or disable the HA group, force takeover, or remove the HA group.
Web Reputation	Control the level of protection against malicious websites with Trend Micro Web Reputation technology.

Feature	Description
Malware and virus scanning	Leverage multiple security components and antivirus protection based on application content scanning for better protection with lower latency and improved user experience. Use cloud-based Virtual Analyzer and Predictive Machine Learning for advanced protection from email-based malware.
Spam scanning	Use cloud-based spam scanning to detect and block or tag spam email messages based on the email content.
Reports	Generate reports about detected malware and malicious code, blocked files, and accessed URLs to optimize program settings and fine tune security policies.
Log analysis	View and analyze aggregated log and event data about traffic bandwidth consumption, threat detections, Web 2.0 application usage, web browsing activity, and policy enforcement. If the customer is running all Cloud Edge 6.0 or later gateways, view usage data for policy rules. Save log query filters as log favorites to reference later or generate custom reports for further investigation.

Enhancing in-the-cloud capabilities, security profiles provide a mechanism to control specific security threats that may affect the gateway. Configure advanced policy controls for Intrusion Prevention System (IPS), anti-malware security, email security, web reputation, denial of service attacks, and endpoint identification. The following table describes the available security profiles.

For more information about support for IPv6 with security profiles, see *Support for IPv6 on page 1-20*.

Table 1-6. Cloud Edge Security Profiles

Feature	Description
IPS profiles	Each security profile can specify an intrusion protection profile that determines the level of protection against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities. The default profile protects clients and servers from known threats.

Feature	Description
Anti-malware profiles	Take default intelligent actions on web-based anti-malware or customize the actions setting for the organization or specify which file extensions specified in URLs to allow or block. Enable Smart Scan for enhanced malware scanning. Smart Scan is a next-generation, cloud-based protection solution. At the core of this solution is an advanced scanning architecture that leverages the Smart Scan server to perform threat scanning using signatures that are stored in the cloud.

Feature	Description
Email security profiles	Take default intelligent actions on email security or customize the actions setting for the organization. Email security profiles scan and take action on IPv4 email traffic. **Anti-Malware** Enable anti-malware scanning and define the tag used in the subject line and body of an email with malware attachments. You can configure advanced cloud-based scanning and protection from email-based malware by enabling Virtual Analyzer and Predictive Machine Learning. If enabled, Cloud Edge sends suspicious file attachments to Virtual Analyzer and Predictive Machine Learning when a file exhibits suspicious characteristics and signature-based scanning technologies cannot find an unknown threat. Tag emails that contain encrypted attachments and define the tag used in the body of the email. **Anti–Spam** Enable anti-spam scanning and optionally enable Cloud Edge to use Trend Micro ERS (Email Reputation Services) to determine spam based on the reputation of the source address. Set the spam "sensitivity" level or catch rate. Enable BEC (Business Email Compromise) scanning. BEC scams target companies to compromise legitimate business email accounts through social engineering for the purpose of conducting unauthorized transfers of funds. Define the action to take when an email is determined to be spam and BEC and, if the action is tag, define the tag used in the subject line and body of a spam or BEC email message. **Content Filtering** and **Exception Lists** Configure content filters or create exception lists to block or approve emails based on the sender or on attachment file types (true file types for cloud scan and file extensions for local scan). **Advanced Settings**

Feature	Description
	You can configure which email protocols are enabled, custom SSL ports, and SMTP server settings.
Web reputation profiles	Each security policy can select the web reputation sensitivity level to block sites. Web Reputation technology assigns reputation scores to URLs. For each accessed URL, Cloud Edge queries Web Reputation for a reputation score and then takes the necessary action, based on whether this score is below or above the user-specified sensitivity level.
HTTPS profiles	Each security policy can select URL category and source IPv4 address exceptions to exclude from HTTPS inspections. Secure Socket Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols widely adopted and deployed in network communication today. The traffic over SSL/TLS is encrypted and signed to ensure security, hence HTTPS. Because encrypted HTTPS connections can carry the same risks as unencrypted HTTP connections, Cloud Edge scans all IPv4 traffic for potential risks and threats. Customize the HTTPS profile by specifying up to five HTTPS ports to scan.
Anti-DoS profiles	Each security policy can specify flood protection and address exceptions for Denial of Service attacks. A denial-of-service (DoS) or a distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to users, and is intended to temporarily or indefinitely interrupt or suspend services to a host connected to the Internet. Typical attacks involve saturating the target machine with external communication requests, such that the machine can no longer respond to legitimate traffic, or responds so slowly it is rendered unavailable. Such attacks usually lead to server overload.

Feature	Description
Endpoint identification profiles	Each security policy can specify IPv4 address objects for Captive Portal to use to identify which IPv4 address belongs to which user. Endpoint identification provides a method of user identification using an IPv4 address-to-user mapping cache for policy matching. By default, endpoint identification cannot automatically identify IP addresses. You must define which IPv4 address objects can be used for endpoint identification. If a source IPv4 address is not in the defined ranges within the selected IPv4 address objects, the IPv4 address will not work for endpoint identification. You cannot use IPv6 addresses for endpoint identification.

Support for IPv6

Cloud Edge provides support for IPv6 in Bridge Mode and Software Switch deployments.

Important

IPv6 is not supported in Routing Mode.

The following table explains which features and capabilities provide IPv6 support in Bridge Mode and Software Switch deployments. In addition to the support specified in the table, Cloud Edge can forward traffic over IPv6 through the Cloud Edge gateway, including to an IPv6 router, which can provide access to the Internet.

Table 1-7. Cloud Edge IPv6 Support in Bridge Mode and Software Switch Deployments

Feature	Category	Support for IPv6	Not Supported for IPv6
Dashboard		●	
	Cloud Edge supports displaying IPv6 addresses in the dashboard.		
Gateway—Registration			●

Feature	Category	Support for IPv6	Not Supported for IPv6
	Cloud Edge uses IPv4 to connect to Cloud Edge Cloud Console.		
Gateways — Network	Interfaces		●
	Administrative access		●
	DHCP		●
	Dynamic DNS		●
	Routing table		●
	Static Routes		●
	NAT		●
	Cloud Edge gateways do not support IPv6 for network configurations (any mode). However, Cloud Edge can forward requests such as DNS for IPv6 and DHCPv6 through to end points.		
Gateways — Bandwidth control		●	
Gateways — VPN	User VPN		●
	Site–to–Site VPN		●
Gateways — End User Management — General settings			●
	Functionality dependent on user accounts is not supported for IPv6.		
Gateways — Updates			●
	Cloud Edge uses IPv4 to connect to ActiveUpdate.		
Gateways — Network Access Control			●
	Cloud Edge does not support network access control for IPv6 endpoints, even if the endpoint is dual-stack with both an IPv4 and IPv6 address.		
Policies — Policies	Source IP	●	

Feature	Category	Support for IPv6	Not Supported for IPv6
	Source FQDN	●	
	Users / User Groups		●
	Destination IP	●	
	Destination FQDN	●	
	Traffic — Applications and URL categories	●	
	Policies based on users or user groups are not supported for IPv6. That policy will not be applied to IPv6 traffic.		
Policies — Objects	IP Address/FQDN	●	
	MAC Addresses	●	
	Services	●	
	Applications and application groups	●	
	URL categories	●	
	Cloud Edge supports ICMPv6.		
Policies — Approved Blocked List	IPv6 addresses	●	
	FQDNs	●	
	URLs	●	
Policies — Security Profiles	IPS	●	
	Anti-Malware	●	
	Email Security — Local Scan		●
	Email Security — Cloud Scan		●

Feature	Category	Support for IPv6	Not Supported for IPv6
	Anti-DOS	●	
	HTTPS		●
	Web Reputation	●	
	Endpoint Identification		●
	Both email local scan and cloud scan do not support IPv6. IPv6 email traffic will pass through the Cloud Edge gateway without scanning. HTTPS IPv6 traffic will pass through the Cloud Edge gateway without scanning. Cloud Edge does not trigger Endpoint Identification for IPv6 traffic. If Captive Portal is enabled, the Captive Portal window will not open; IPv6 traffic will pass through the Cloud Edge gateway.		
Policies — Web Reputation Service		●	
Policies — User Notifications		●	
	Cloud Edge supports displaying user notifications to IPv6 clients.		
Analysis & Reports — Reports		●	
	Cloud Edge supports displaying IPv6 addresses in reports.		
Analysis & Reports — Log Analysis	Application bandwidth	●	
	Policy Enforcement	●	
	Internet Access	●	
	Internet Security	●	
	Cloud Edge supports displaying IPv6 addresses in the logs.		
Administration — Users & Accounts			●

Feature	Category	Support for IPv6	Not Supported for IPv6
	Functionality dependent on user accounts is not supported for IPv6.		
Administration — User Authentication			●
	Functionality dependent on user accounts is not supported for IPv6.		
Administration — Audit Log		●	
Administration — Administrator Alerts	Gateway status change	●	
	Mail security status change	●	
	C&C Callbacks	●	
Administration — Scheduled Updates			●
	Cloud Edge uses IPv4 to connect to ActiveUpdate.		
Administration — Maintenance			●
	Cloud Edge uses IPv4 to connect to external servers.		
Administration — Certificate Management			●

Chapter 2

Best Practices for Cloud Edge Deployments

This chapter 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) gateway 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 chapter covers the best practices for ease of deployment, superior security and performance, and monitoring and reporting. It was written for administrators who deploy Cloud Edge gateways and manage the operation regularly. It is not meant to be a replacement for the complete set of information in this deployment guide and in other user manuals, which can be found at: http://docs.trendmicro.com/en-us/smb/cloud-edge.aspx, including:

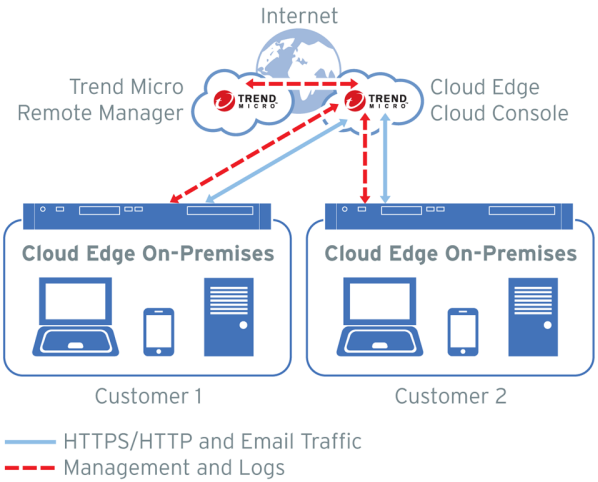
- License Provision Quick Start Card (for Managed Service Providers)
- Cloud Edge Quick Start Card (for on-premises customers)
- Cloud Edge Cloud Console Online Help

- Readme

Deployment Best Practices

Provision Licenses by MSPs

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



Creating Service Plans

Access Trend Micro Licensing Management Platform (LMP) to create the service plans for Cloud Edge.

Procedure

1. Create the Cloud Edge service plan, which might include the following components:

   a. **Cloud Edge** — required license for appliance firmware

b. **Virtual Analyzer** — license for sandbox emulation

c. **Log Forwarding Service** — license for forwarding logs to a third party log management system

2. For best practices, take note of the following:

   - For **Version type**, **Full** is recommended since Cloud Edge is an appliance.
   - For **Data Center** location, select the 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.

Creating Customers

Use Licensing Management Platform (LMP) to create the **Customer**.

Procedure

1. Create the **Customer** by filling out the required information including:

   a. **Company**

   b. **Address**

   c. **City**

   d. **State** and **Postal code**

   e. **Account name**

   f. **Contact person** name and **Email address**

2. For best practices, take note of the following:

   - You will want to set **Send account creation email** to **immediately upon creation** of a customer.

- And finally, it is easier to assign a service plan as you create a customer.
- Set **Units per license** based on the number of Cloud Edge gateways that you will deploy for the customer that you are creating.

Adding New Gateways

After creating service plans and customers, you can add new gateways to Cloud Edge Cloud Console.

Procedure

1. On Remote Manager, select the new customer and launch Cloud Edge Cloud Console.

   This is where a Cloud Edge gateway can be registered using its serial number.

2. For best practices, take note of the following:

   a. It is recommended you first test register a new gateway locally before actually deploying it 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 unregister the gateway if needed.

   b. Reset the gateway back to factory defaults before shipping it out to the end customer so that the network settings can be configured locally.

Deploying Gateways On-Premise

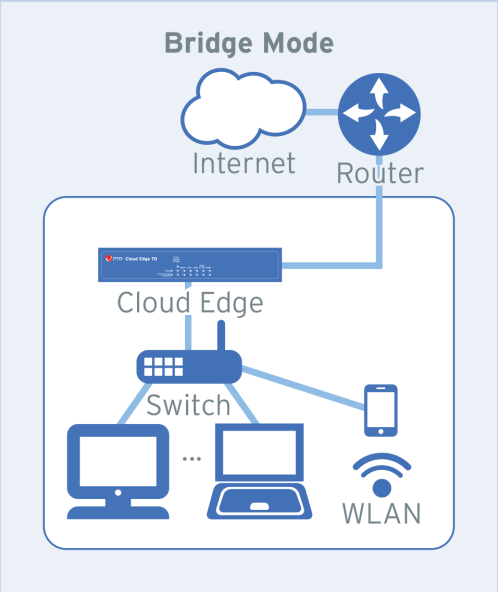
Refer to the *Quick Start Card* for deploying gateways at customer sites.

Recommendations for Choosing Deployment Mode

You should keep the following Bridge Mode vs. Routing Mode recommendations in mind.

Cloud Edge Bridge Mode

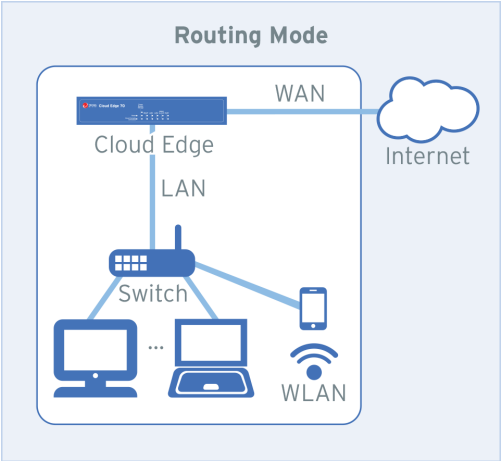
Choose Bridge Mode whenever possible. You would typically use a Bridge Mode deployment on a private network behind a router and in front of a switch. This is set by toggling the physical switch at the back of the Cloud Edge gateway. The gateway is set to Bridge as the default. Bridge Mode allows for drop-in deployment of the Cloud Edge gateway without modifying the existing network. Cloud Edge can add superior scan and threat protection.



Cloud Edge Routing Mode

Configure Routing Mode when you want the Cloud Edge gateway to function as a router as well as providing security and threat protection. The gateway is visible on the network and acts as a layer 3 routing device with security scanning and control capabilities. In Routing Mode, you normally replace an existing router on the network with the Cloud Edge gateway or deploy the

gateway between the router and switch. Necessary configuration changes are needed on the router and the Cloud Edge gateway.



Using Quick Setup

Use **Quick Setup** to configure basic settings on the Cloud Edge gateway.

Procedure

1. From the on-premises console, go to the **Quick Setup** page.
2. For best practices, take note of the following:
   - **Uplink configuration** — Choose **DHCP** whenever possible; if not possible, assign a static IPv4 address and subnet and configure DNS on the bridge interface. PPPoE is also available when deploying Routing Mode.
   - **Start Configuration Test** should be used to check if the gateway can access DNS and connect to Cloud Edge Cloud Console.
   - **System settings** — **Enable NTP server** is recommended for setting the gateway clock automatically.

- You can find the **Serial number** using the Cloud Edge on-premise console on the **Administration** > **Device Management** page. It's also located on the bottom of the Cloud Edge device.
- You can configure DHCP services on an interface using the on-premises console on the **Network** > **Services** page.

  Enabling DHCP service for the LAN interface is recommended.

  Note

  After the device is registered, DHCP for LAN2, LAN3, and MGMT can only be edited using Cloud Edge Cloud Console.

- To register the gateway, access Cloud Edge Cloud Console and then go to **Gateways** > **Register New Gateway**.

Security Configuration Best Practices

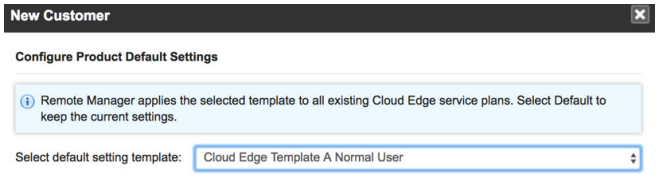
After successful registration, Cloud Edge gateways can be centrally configured and managed from Cloud Edge Cloud Console or you can use Trend Micro Remote Manager to set up and deploy policy rules and security profiles for common security settings that are to be shared across multiple gateways. You can then configure each gateway for its unique network settings.

Remote Manager Security Templates

You can configure security settings using Cloud Edge Cloud Console.

As a convenience, Remote Manager features **Default Settings Templates**, which contain the same security settings you can configure through Cloud Edge Cloud Console. Remote Manager allows you to assign them to gateways to become the default settings associated with customer companies. This

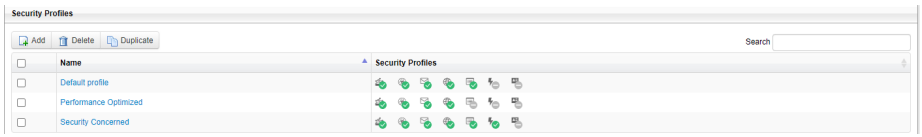
makes it easier to ensure customers are using the same settings when deploying their gateways.



Creating Security Templates

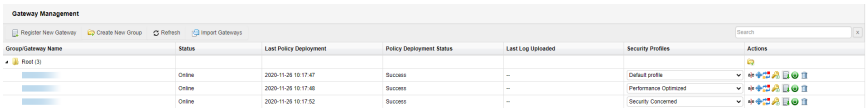
You can create additional security templates as needed. When creating additional templates, consider at least three scenarios:

- Cloud Edge Template A — Normal User (the default template)
- Cloud Edge Template B — Security Concerned User
- Cloud Edge Template C — Performance Optimized User



Procedure

1. Create additional security templates.
2. Assign the Security Profiles as desired by going to **Gateways** on the default template page or from Cloud Edge Cloud Console.



Creating a Security Template for Normal Users

Security Profile A — Normal User: You can use the default security template for normal users. All settings are left at their default values. This gives you the best balance between security and performance.

Procedure

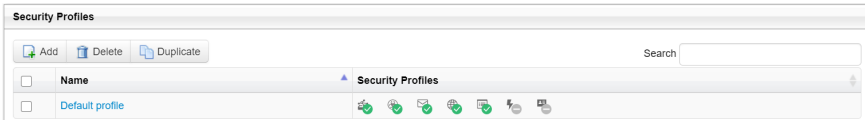
1. Perform the appropriate action:
   - From Remote Manager, go to **Administration** > **Configure default setting templates**.
   - From Cloud Edge Cloud Console, go to **Polices** > **Security Profiles** > **Default Profile**.
2. Verify that all values are at their default values.

Creating a Template for the Security-Concerned User

Gateway Profile B — Security-Concerned User: You can use this security template when security is the primary goal. Enhance security by inspecting more in depth and block potentially malicious traffic.

Procedure

1. Perform the appropriate action:
   - From Remote Manager, go to **Administration** > **Configure default setting templates**.
   - Log on to Cloud Edge Cloud Console.
2. Enable the following settings at **Polices** > **Security Profiles** > **Default Profile**.



a. **IPS**:

   1. Change the IPS action from **Monitor** to **Block**.
   2. **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`.

b. **Anti-Malware**: In addition to **Enable Smart Scan**, also **Enable Enable Predictive Machine Learning**.

   Doing this leverages the Smart Scan real-time signature server in the cloud.

c. **Email Security**:

   1. **Enable Virtual Analyzer** for leveraging the cloud sandbox to analyze suspicious files (license required).
   2. **Enable Predictive Machine Learning** to leverage AI in detecting previously unknown threats; also change the **Action** from **Monitor** to **Block** or **Add Tags**.
   3. Turn on **Tag emails with encrypted attachments** to notify users that the attached file could not be scanned.
   4. Under **Anti-Spam**, **Enable Email Reputation** and **Enable Business Email Compromise (BEC)**.

d. **Web Reputation**: Choose **Medium** for sensitivity level.

e. **HTTPS**: Turn **On** HTTPS Scanning and uncheck **All URL Category** under the **Exceptions** list.

3. Remember to **Save** and **Deploy** the gateway profile.
4. For added security, you can define additional **Policy Rules** to block unwanted Applications or URL Categories at the firewall level.

   - From the Remote Manager Security Template screen, go to **Policies** > **Policy Rules**.
   - From Cloud Edge Cloud Console, go to **Policies** > **Policy Rules**.

a. Add a **Policy Rule** named “Block Internet Security URLs”.

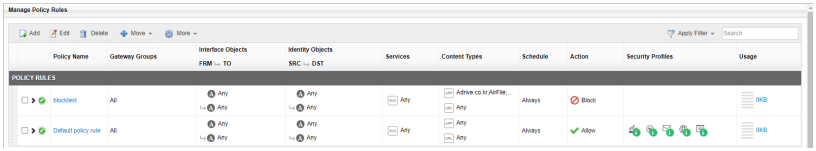
   Under **Traffic Type**, select **Selected applications / URL categories** > **URL Categories** > **Internet Security**, then set the **Action** to **Block**.

b. Add a **Policy Rule** named “Block Gaming Applications”.

   Under **Traffic Type**, select **Selected applications / URL categories** > **Applications** > **Game**, then set the **Action** to **Block**.

c. The newly added policy rules should come before the “Default policy rule”.

   The result might look something like the following:



5. Configure Network Access Control under **Gateways** > **<Selected Gateway>**.

   - **WFBSS Endpoint Protection**: Enable when customer is also using Worry Free Business Security Services

     This feature blocks internet access on devices that are out of compliance.

     a. Turn feature **On** because it is disabled by default.

     b. Choose **Block** for both of the criteria:

        - Clients without Agents
        - Clients with Agents using out-of-date patterns

     c. Under the **Protection list**, add the IP address pool of your network.

        This ensures that traffic from unknown devices on your network will be blocked.

d. Under the **Exception list**, add the IP addresses of devices on which you cannot install Worry Free Services Security Agent.

e. Click **Apply**.

- **Suspicious Endpoint**: Configuring Suspicious Endpoints provides network access control for endpoints on which C&C callbacks above a configured threshold are detected

  a. Turn feature **On**, because it is disabled by default.

  b. Use the default threshold, which is **50** C&C callback events in **1 hour**.

  c. Set action to **Block**.

  d. Click **Apply**.

Creating a Security Template for Performance-Optimized User

Security Profile C — Performance-Optimized User: You can use this security template when performance is the primary goal. This profile uses various techniques to speed up the traffic for specified users and groups.

Procedure

1. Perform the appropriate action:

   - From Remote Manager, go to **Administration** > **Configure default setting templates**.
   - From Cloud Edge Cloud Console, go to **Polices** > **Policy Rules**.

2. Configure the following settings:

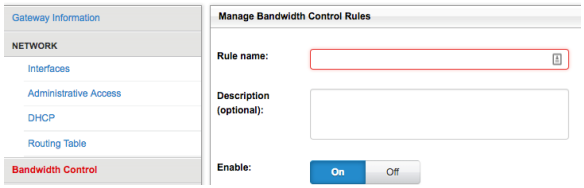
   - Add a **Policy Rule** named “Bypass Trusted Sources” — define specific policy **Sources** for trusted IP addresses or users/groups and set the **Action** to **Bypass**, which will bypass threat scanning for traffic coming from these sources.
   - Alternatively, set a bypass policy rule for local to local network traffic.

- HTTPS — Leave HTTPS scanning at the default **Off** setting under **Security Profiles**.

3. You can also set up gateway-specific **Bandwidth Control** rules, which can be used to prioritize traffic among critical versus noncritical applications.

   This feature must be configured from Cloud Edge Cloud Console.

   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, which causes other applications to suffer.



Miscellaneous Best Practices

You should keep the following recommendations in mind when deploying Cloud Edge gateways.

Monitoring Cloud Edge Gateways

You can monitor Cloud Edge activity and view threat analysis using the **Dashboard** and **Analysis & Reports**.

Using the Dashboard

Consider the following when using the dashboard to monitor Cloud Edge activity:

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

Using Analysis and 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. It is really a time-saving feature to send report notifications via email so that a summary report can always be ready in your in-box when you start a new day, a new week, or when you need to generate a month-end report for management.

Managing Administrative Tasks

You should keep the following recommendations in mind when managing administrative tasks.

Creating User Accounts

Consider the following when creating user accounts using Cloud Edge Cloud Console.

Procedure

1. Go to **Administration** > **User & Accounts**.
2. Create **Read only** accounts for people who need access to Cloud Edge Cloud Console to view logs and reports, but do not need the privilege to modify configurations.

Managing Administrative Alerts

Consider the following when managing administrative alerts.

Procedure

- Configure administrative alerts through Cloud Edge Cloud Console.
- Go to **Administration** > **Administrative Alerts** and set **Enable** to **On**.
- Set the following alert types:
  - Select: **C&C Callbacks** with [50] events occur in [1 hour]
  - Select: **Gateway status change** & **Mail security status change**
- Log on to Remote Manager and go to **Administration** > **Configure notifications** to fine tune **Event Notification** settings with adjustable **Alert Thresholds**.

Configuring Scheduled Updates

Consider the following when configuring scheduled updates:

Procedure

- Normally, the **Daily** component (patterns/engines) update setting is sufficient. However, during a malware outbreak, changing the update period to **Hourly** might be desirable.
- Weekly firmware updates is advised; choose the default or set the update to occur during off-business hours.

Configuring Administrative Access

Consider the following when configuring administrative access.

Procedure

- Configure the different types of management services through Cloud Edge Cloud Console.

- Go to **Gateways** > **<Select Gateway>** > **Administrative Access** and specify the IP range or IP address that will need access to the Cloud Edge gateway using the on-premise console, ping, or SSH.

Certificate Management

Consider the following when managing certificates.

Procedure

- Go to **Administration** > **Certificate Management** to manage Cloud Edge certificates.
- Import your own certificate or export the certificate that Cloud Edge uses to decrypt SSL traffic and then install the exported certificate into end users' trusted certificate store.

  This helps end users' avoid receiving certificate warnings that are displayed on their browsers when accessing HTTPS websites.

Chapter 3

Getting Started

Getting Started Tasks

The following procedure explains the necessary steps to get started with Remote Manager and Cloud Edge Cloud Console. After completing these steps, supply the Cloud Edge on-premises gateway to the customer. The customer must configure network settings based on their network environment.

Tip

You can use Licensing Management Platform (LMP) to manage your service plans and companies. You can access LMP directly or you can single sign-on (SSO) to LMP through Trend Micro Remote Manager. Trend Micro recommends accessing LMP through Remote Manager for better access to daily monitoring and other resources.

Procedure

1. Access LMP directly or through Remote Manager.

   See *Accessing LMP on page 4-3*.

2. Create a service plan.

   See *Creating a Service Plan on page 4-4*.

3. Create a company and assign the service plan.

   See *Creating a Company and Assigning the Service Plan on page 4-5*.

4. View Cloud Edge Cloud Console widgets through Remote Manager.

   See *Daily Monitoring on page 5-8*.

   The **Getting Started** screen appears after logging on. This screen helps you navigate Cloud Edge Cloud Console and register gateways.

   See *Getting Started Screen on page 6-3*.

5. Register all gateways that Cloud Edge Cloud Console will manage.

   See *Registering Gateways on page 7-44*.

6. Optionally create user accounts to access Cloud Edge Cloud Console.

   See *Adding Cloud Console Administrator Accounts on page 6-184*.

7. Begin managing registered gateways.

   After providing the Cloud Edge on-premises gateway to the customer, the customer must configure some deployment settings based on the deployment mode that you select for their network.

Deployment Tasks

The following procedure explains all mandatory and optional steps to configure the Cloud Edge gateway.

Procedure

1. Decide which mode to deploy the Cloud Edge gateway.

   See *Deployment Modes on page 7-2*.

2. Toggle the deployment switch depending on the selected deployment mode. The deployment switch is located on the back panel of the Cloud Edge gateway.

   Note

   Toggle the deployment switch to **Bridge**:

   - For Software Switch deployments
   - For Bridge Mode deployments on Cloud Edge gateways with hardware switch chipset

3. Gather the materials listed in the pre-deployment checklist.

   See *Pre-deployment Checklist on page 7-19*.

4. Perform the installation and initial configuration.

   See *Performing the Initial Configuration on page 7-25*.

   This step consists of the following sub-steps:

a. *Setting up the Hardware on page 7-22* (includes cabling the network).

b. *Logging on the On-Premises Console from the MGMT Port on page 7-24*.

c. *Performing the Initial Configuration on page 7-25* (includes procedures for Bridge Mode, Bridge Mode (With Switch Chipset), Software Switch, and Routing Mode).

   For Cloud Edge gateways with wireless functionality, includes a procedure for Routing Mode.

d. *Registering Gateways on page 7-44* (if not already registered).

e. *Performing additional configuration on page 7-46* (optional).

Chapter 4

Licensing Management Platform

Trend Micro™ Licensing Management Platform™

The Trend Micro™ Licensing Management Platform™ enables service providers and other partners to manage and issue licenses for Trend Micro products with ease. It includes branding settings you can use to customize the platform.

Trend Micro Licensing Management Platform makes use of service plans with different licensing details to satisfy the needs of your customers. You can create company accounts for your customers and then assign service plans to those company accounts.

Features and Benefits

With Licensing Management Platform, you can customize product offerings and services. These are some of the key features:

TABLE 4-1. Key Features

FEATURE	DETAILS
Service plans	Set up service plans to create subscription terms for your customers.
Customer accounts	Set up company accounts for your customers and add service plans to the company accounts.
License information	View and manage licenses purchased by your customers.
Customized notification emails	Set up different notification emails for your customers.
Create Registration keys	Generate licenses and assign the licenses to service plans.
Branding settings	Customize branding settings for your business purposes. This includes contact information, the log on page, and banners visible on the platform.

To learn more about managing your customers, service plans, and licenses through LMP, see the supporting documentation at:

http://docs.trendmicro.com/en-us/smb/trend-micro-licensing-management-platform.aspx

Accessing Licensing Management Platform

You can use Licensing Management Platform (LMP) to manage your service plans and companies. You can access LMP directly or you can single sign-on (SSO) to LMP through Trend Micro Remote Manager. Trend Micro recommends accessing LMP through Remote Manager for better access to daily monitoring and other resources.

Procedure

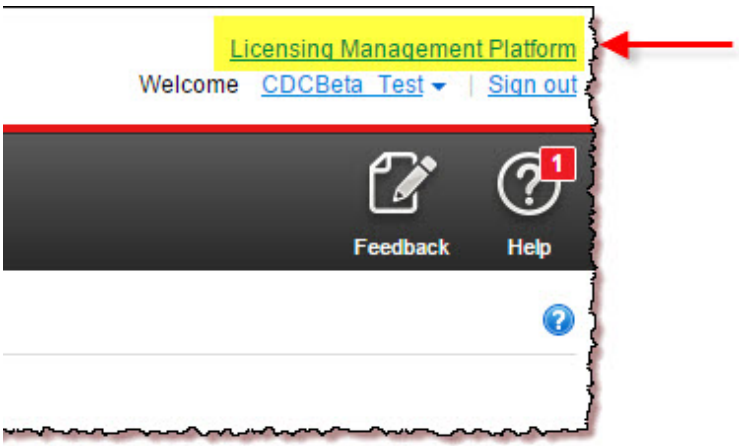
- Access LMP directly.

  The LMP URL is unique to each managed service provider. Trend Micro provides the URL in an email message after you create the LMP account.

- Single sign-on to LMP through Remote Manager.

  a. Log on to Remote Manager.

  b. At the top-right corner, click **Licensing Management Platform**.



The LMP dashboard appears. Click **Trend Micro Remote Manager** at the top-right corner to return to Remote Manager.

Note

To learn more about managing your customers, service plans, and licenses through LMP, see the supporting documentation at:

http://docs.trendmicro.com/en-us/smb/trend-micro-licensing-management-platform.aspx

Creating a Service Plan

Use service plans to issue licenses to customers and set up different licensing plans for your products/services and customers. You must use the Licensing Management Platform (LMP) to create service plans.

Procedure

1. Single sign-on to LMP through Remote Manager.
2. Go to **Users & Licenses** > **Service Plans**.
3. Click **Create Service Plan**.
4. Specify service plan settings.

Option	Description
Service plan name	Specify a name for the service plan that appears in LMP and Remote Manager.
Product/Service	Select the relevant Cloud Edge product or service. Licensing types include licenses for Cloud Edge gateway models, Virtual Analyzer for Cloud Edge, and Log Forwarding Service for Cloud Edge.
Version type	Select **Trial** or **Full**.
Trial form	Optionally enable the trial form for this service plan.
Unit	Select **Seat(s)**.
Data center	Select the country for customer locations.

Option	Description
Activation policy	Configure when the service plan activates.
Managing product/service	Select this option to allow Remote Manager to control Cloud Edge. **Important** Remote Manager requires this setting to manage Cloud Edge.

5. Specify the subscription policy settings.

Option	Description
Initial license period	Configure the initial period during which the subscription is valid. After this period, the subscription must be renewed or it will expire.
Auto-renewal	Select to renew the subscription automatically.
Expiration notification	Select the number of days before the subscription expires to send customers an expiration notification. The license status is visible in the table when you click **Users & Licenses** > **Customers** and then click a customer.

6. Click **OK**.
7. At the confirmation message, click **Yes**.

Creating a Company and Assigning the Service Plan

Procedure

1. Single sign-on to LMP through Remote Manager.
2. Go to **Users & Licenses** > **Customers**.
3. Click **Create customer**.
4. Specify **Company Profile** information.

Option	Description
Company and **Address**	Specify the customer's company name and optionally specify the customer address.
City, **State**, and **Postal code**	Specify the customer's city, state, and postal code.
Country/Area	Select the customer's country.
Notes	Optionally enter notes.

5. Specify **User Account(s)** information.

Option	Description
Account name	Specify the account name for your customer.
User role	Set to “Administrator” (not configurable).
Contact person	Specify the contact person's name.
Email address	Specify an email address for the account.
Time zone	Select the customer's time zone.
Language	Select the preferred language that appears on Cloud Edge Cloud Console and in which the customer will receive reports and notifications.
Send account creation email	Select when to send the account creation email message to the customer.

6. Click **Assign Service Plan**.
7. Select one or more service plans created at *Creating a Service Plan on page 4-4*.
8. For each selected service plan, select the **License start date**.
9. For each selected service plan, set **Units per license** to the maximum seats allowed by your product license.
10. Click **Save**.
11. Verify the following:

- The company has been added to the **Customers** list at **Users & Licenses** > **Customers**.
- The company shows the correct service plans.

12. Return to Remote Manager by clicking **Trend Micro Remote Manager** at the top-right corner.

Chapter 5

Trend Micro Remote Manager

Trend Micro™ Remote Manager™

Trend Micro™ Remote Manager™ is a robust console that works in parallel with Trend Micro Licensing Management Platform™ to provide managed security services to small and medium businesses.

Remote Manager enables you to monitor the health of multiple managed networks through multiple, managed products and services. Remote Manager allows reseller administrators to issue commands to manage critical aspects of network security.

Remote Manager is hosted on regional Trend Micro Data Center servers where resellers obtain an account. Resellers can use Remote Manager to establish customer accounts, monitor customer networks, and manage security using the Remote Manager web console.

Remote Manager monitors the following products:

- Trend Micro Cloud Edge
- Trend Micro Cloud App Security
- Trend Micro Hosted Email Security™
- Trend Micro InterScan Web Security as a Service (IWSaaS)
- Trend Micro Worry-Free Business Security™ Standard
- Trend Micro Worry-Free Business Security Advanced
- Trend Micro Worry-Free Business Security Services

Remote Manager has a monitoring dashboard that allows resellers to look into the following aspects of Cloud Edge network security with the following widgets:

- Cloud Edge Devices with the Most Threats
- Cloud Edge Customers with the Most Threats

Remote Manager provides a number of widgets with cumulative information from all supported products includes information about ransomware detections, threat management, customers needing the most attention,

license management and usage, managed customers and products, and system management.

Note

For detailed information on Cloud App Security, IWSaaS, Hosted Email Security, Worry-Free Business Security (all), and Cloud Edge, see the documentation for those products and services available at: http://www.docs.trendmicro.com.

Remote Manager offers a structured view of customer networks and allows resellers to issue commands and manage the following aspects of network security:

- Component updates and updates to the managed server
- Vulnerability assessment
- Damage cleanup
- Automatic outbreak response
- Firewall and Real-time Scan settings
- Manual scans
- Single sign-on

Remote Manager also supports comprehensive reporting features and allows resellers to subscribe individuals to automatically generated reports.

Configuring Default Setting Templates

Note

Default Setting Templates are only available if you integrated with Licensing Management Platform.

Default setting templates are templates that already have the preconfigured settings for a customer. This makes it easier to ensure that customers are using the same settings.

For more information on the settings that you can configure from this template, refer to Trend Micro Remote Manager documentation at:

http://docs.trendmicro.com/en-us/smb/trend-micro-remote-manager.aspx

---

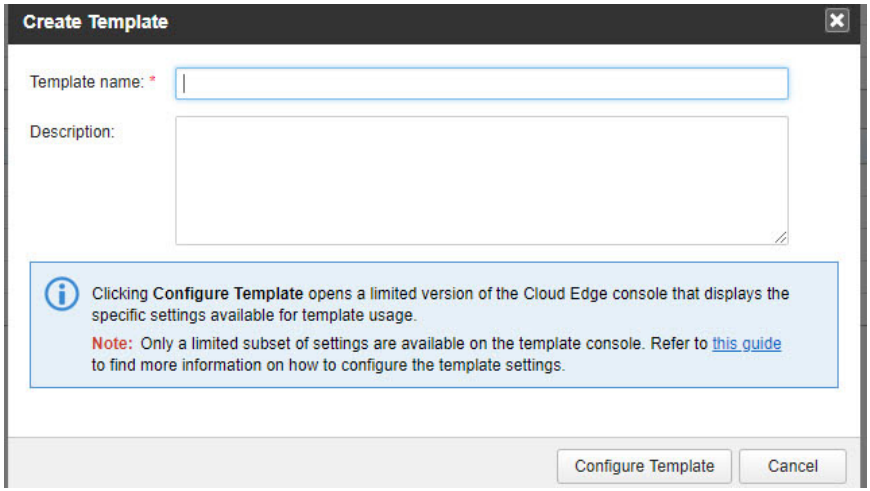
Procedure

1. Log on Remote Manager.
2. Go to **Administration** > **Configure default setting templates**.

   The **Configure default setting templates** screen opens. The **Cloud Edge** section contains a list of five templates. All are initially empty. From this list, you can create five templates or you can edit existing templates.
3. In the **Cloud Edge** section, click **Create** beside one of the unconfigured templates to create a new template.

   You can alternatively click **Edit** to modify a configured template.

   The **Create Template** screen appears.



4. Specify the template name and optionally add a description. A description helps to identify the template's purpose.

5. Click **Configure Template**.

   A console similar to Cloud Edge Cloud Console opens with three menus displayed in the navigation bar: **Policies**, **Alerts & Reports**, and **Administration**

   Note

   Any changes to this site are saved as a template and do not affect any registered product.

6. Configure relevant policy and schedule settings.

   You can configure the following settings:

   - Policies
     Rules, Objects, Approved/Blocked List, Gateway Profiles, User Notifications

     Note

     You cannot configure and use the new interface object when configuring policy security templates. You must user Cloud Edge Cloud Console after the templates are deployed to configure and use interface objects for a policy rule.

     You can configure the new security profile section for the policy rule template. The security profile settings will take effect only on Cloud Edge 6.0 and later gateways.

   - Analysis & Reports
     Reports, Summary Report
   - Administration
     Captive Portal, Audit Log, Scheduled Updates, and Administrative Alerts

   Learn about configuring policies in the Online Help available at:

   http://docs.trendmicro.com/en-us/smb/cloud-edge.aspx

Creating a Company and Assigning the Service Plan

This procedure explains how to create a company and assign a service plan through Remote Manager. You must use the Licensing Management Platform (LMP) to create service plans. For instructions on using LMP, see *Creating a Company and Assigning the Service Plan on page 4-5*.

Procedure

1. Log on Remote Manager.
2. Go to **Customers**.
3. Click **New Customer**.
4. Specify **Company profile** information.

Option	Description
Company name and **Address**	Specify the customer's company name and optionally specify the customer address.
City, **State/Province**, and **Postal code**	Specify the customer's city, state/province, and postal code.
Country	Select the customer's country.

5. Specify **User account** information.

Option	Description
Account ID	Specify the account ID for your customer.
Contact person	Specify the contact person's name.
Contact number	Specify an area code, telephone number, and optional extension.
Email	Specify an email address for the account.
Time zone	Select the customer's time zone.

Option	Description
Language	Select the preferred language that appears on Cloud Edge Cloud Console and in which the customer will receive reports and notifications.

6. Click **Next**.
7. Select the **Service plan**.

Note

You cannot create a service plan through Remote Manager. To create the service plan, either access LMP directly or single sign-on to LMP through Remote Manager. For details, see *Creating a Service Plan on page 4-4*.

8. Select a **Start date** by clicking the calendar.
9. Set **License** to the maximum units allowed by your product license.
10. Click **Add device** to specify a device name and serial number.
11. Click **Next**.

    The **Configure Product Default Setting** window appears.
12. Select a previously created policy template.

    For details, see *Configuring Default Setting Templates on page 5-3*.
13. Optionally enter information about the selected template in **Comments**.
14. Click **Save**.
15. Verify the following:
    - The company has been added to the **Customers** list at **Customers**.
    - The company shows the correct service plan.

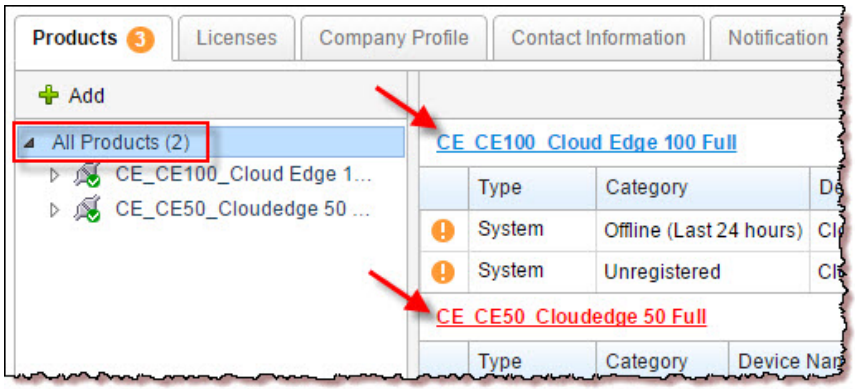
Using SSO to Cloud Edge Cloud Console

This procedure explains how to single sign-on (SSO) to Cloud Edge Cloud Console through Remote Manager.

Procedure

1. Log on Remote Manager.
2. Go to **Customers**.
3. Click the customer's name.

   The **Products** tab appears by default.
4. Select **All Products**.
5. Click the name of the product that appears.
6. Click the Cloud Edge service plan name.



Cloud Edge Cloud Console appears.

Daily Monitoring

Procedure

1. Log on to Remote Manager.

   The Remote Manager dashboard appears at the **Home** screen.

2. Add Cloud Edge widgets to your dashboard.
   a. Select the appropriate tab.
   b. Click **Add Widgets**.
   c. Select the Cloud Edge widgets.
      - **Cloud Edge Devices with the Most Threats**
      - **Cloud Edge Customers with the Most Threats**
   d. Click **Add**.
3. View the Cloud Edge widgets.
   - *Cloud Edge Devices with the Most Threats Widget on page 5-11*
   - *Cloud Edge Customers with the Most Threats Widget on page 5-13*
4. Optionally single sign-on to Cloud Edge Cloud Console.

   See *Using SSO to Cloud Console on page 5-7*.

Reports Overview

Cloud Edge lets you generate, download, and automatically send out reports. Reports provide an overview of license status, assessment results, threat incidents, major threats, and the most affected computers, files and email addresses in your customers' networks.

Reports include many statistics from supported Trend Micro products managed by Remote Manager. Configure report profiles and one-time and periodic reports during certain date ranges and then send reports to multiple email recipients. Remote Manager saves the 30 most recent daily reports, ten

most recent weekly reports, and five most recent monthly reports. General reports are suitable for resellers and customers.

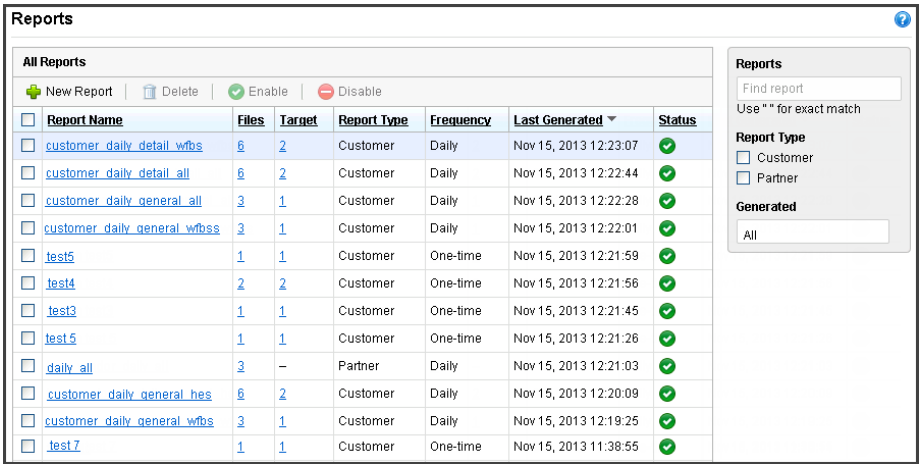


FIGURE 5-1. Reports Page

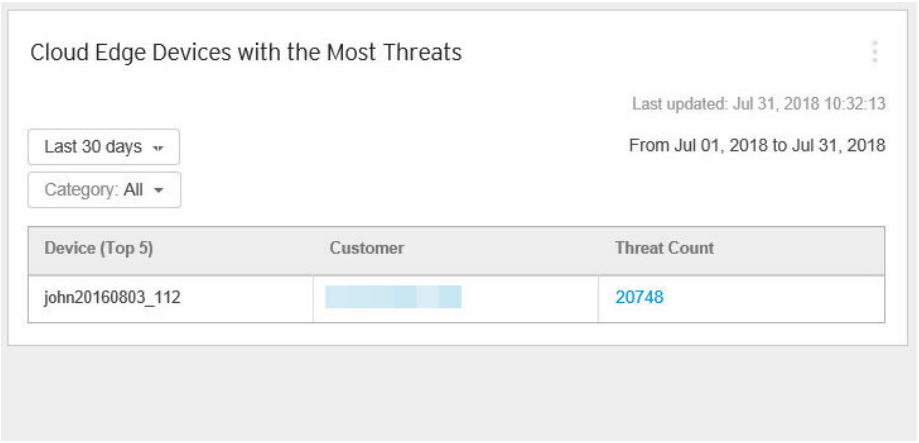
Report profiles enable you to create multiple reports from a single profile. For example, create a one-time report today, generate that report, and tomorrow, change some options and regenerate without having to recreate the entire report.

For more information about Remote Manager reports, review the Remote Manager Online Help:

http://docs.trendmicro.com/en-us/smb/trend-micro-remote-manager.aspx

Cloud Edge Devices with the Most Threats Widget

Shows the Cloud Edge devices with the highest number of threat events.



- You can change the time range for the data shown by selecting from:
  - Last hour
  - Last 24 hours
  - Last 7 days
  - Last 30 days (default)
- You can change the threat type for the data shown by selecting from:
  - All
  - Botnet
  - Intrusion Prevention System (IPS)
  - Spam
  - Web Reputation
  - Virus

- Ransomware
- C&C

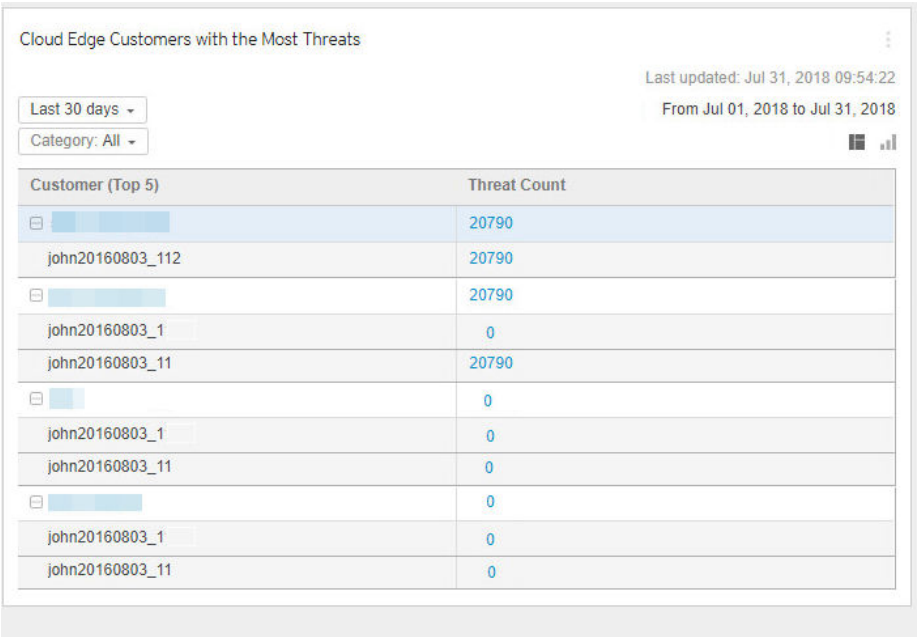
- Click the customer name to view the customer information.
- Click the threat count to open the threat information from Cloud Edge Cloud Console.

Note

Cloud Edge widgets do not appear on the Remote Manager dashboard by default.

Cloud Edge Customers with the Most Threats Widget

Shows the Cloud Edge customers with the highest number of threat events. Data displays in a table and pie chart. You can switch between the table and pie chart by clicking the display icons ( ).



- You can change the time range for the data shown by selecting from:
  - Last hour
  - Last 24 hours
  - Last 7 days
  - Last 30 days (default)
- You can change the threat type for the data shown by selecting from:
  - All

- Botnet
- Intrusion Prevention System (IPS)
- Spam
- Web Reputation
- Virus
- Ransomware
- C&C

- Click the customer name to view the customer information.
- Click the threat count to open the threat information from Cloud Edge Cloud Console.

Note

Cloud Edge widgets do not appear on the Remote Manager dashboard by default.

Managing Gateway Devices

Manage your gateway devices through the **Customer** screen in Remote Manager. After selecting the service plan, manage your gateway devices to:

- View recent gateway events
- Immediately update a gateway device's firmware
- Register additional gateway devices to a customer

Procedure

1. Log on to Remote Manager.

   The Remote Manager dashboard appears at the **Home** screen.

2. Click **Customers**.

3. In the **Company** column, select the customer's name.
4. From the left navigation, expand **All Products** and then select a service plan.
5. Do the following:

Option	Description
View violation and system events	Click the **Events** tab.
Update firmware	Click the **Firmware Updates** tab, select the devices that are outdated or were unable to update, and then click **Update**. After clicking **Update**, the updates for the selected gateway devices are performed immediately.
Register additional gateways	Click the **Devices** tab and then click **Register**.

6. Perform additional gateway tasks.
   a. Select any registered gateway device from the left navigation.
   b. Click the **Events** tab to view violation and system events over the last one hour.
   c. Click the **Components** tab to view the current and latest version of each product component.
   d. Click the **Network** tab to view recent user activity over the last 24 hours.
   e. Click the **VPN** tab to view recent VPN activity.

Note

You cannot view information about VPNs for Cloud Edge gateway models that do not support VPN.

Learning More about Remote Manager

For more information about Remote Manager, see the Online Help available at:

http://docs.trendmicro.com/en-us/smb/trend-micro-remote-manager.aspx

Chapter 6

Cloud Edge Cloud Console

This chapter explains how to use Cloud Edge Cloud Console to register and manage gateways.

Logging on the Cloud Console

Log on to Cloud Edge Cloud Console directly or single sign-on through Remote Manager.

Procedure

- Log on to Cloud Edge Cloud Console directly.
  - **a.** Go to the Cloud Edge Cloud Console URL provided by Trend Micro.
  - **b.** Specify your user name and password.

Note

Before you can log on to Cloud Edge Cloud Console directly, you must first log on to Cloud Edge Cloud Console from Remote Manager using single sign-on and create an administrator account.

See *Adding Cloud Console Administrator Accounts on page 6-184*.

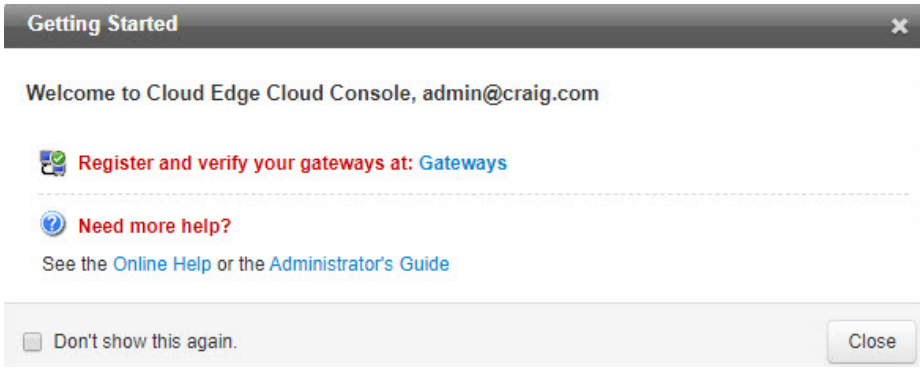
Contact Trend Micro if you cannot access Cloud Edge Cloud Console.

- Log on to Cloud Edge Cloud Console through Remote Manager.

  See *Using SSO to Cloud Console on page 5-7*.

Getting Started Screen

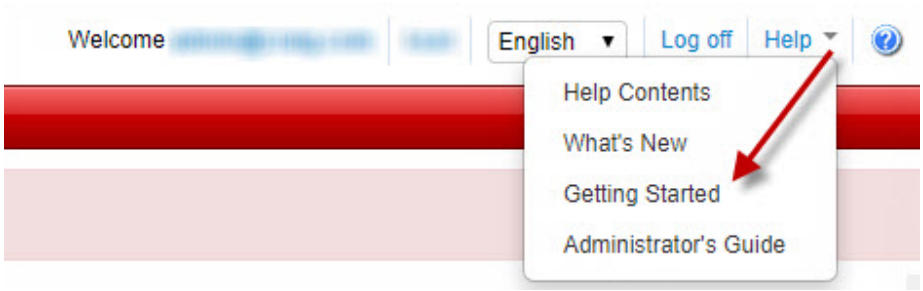
When you first log on to Cloud Edge Cloud Console, the **Dashboard** loads and the **Getting Started** screen appears.



The **Getting Started** screen consolidates information to quickly get started using Cloud Edge Cloud Console. The **Getting Started** screen also provides links to Cloud Edge user assistance.

Select **Don't show this again** to hide the **Getting Started** screen the next time you log on to Cloud Edge Cloud Console.

Display the **Getting Started** screen at any time by clicking the arrow next to **Help** and then selecting **Getting Started**.



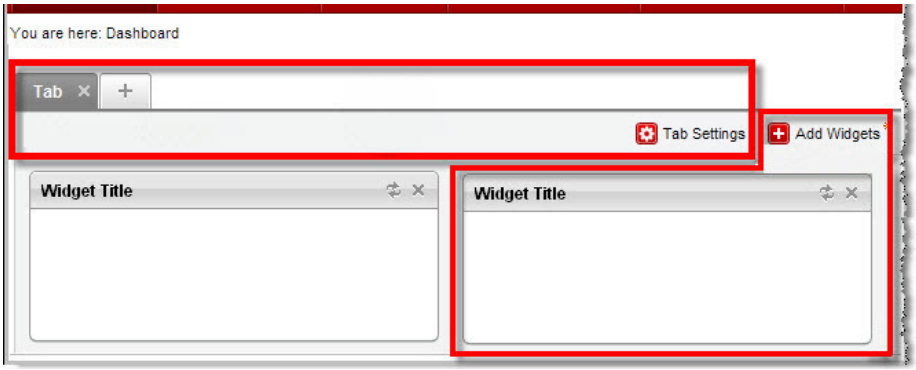
Cloud Edge Cloud Console Overview

This section provides a basic overview of Cloud Edge Cloud Console features. View the Cloud Edge Online Help for more detailed information.

About the Dashboard

From the dashboard, monitor your network integrity through various widgets. Each user account has an independent dashboard. Changes made to one user account dashboard do not affect other user account dashboards.

The dashboard consists of the following user interface elements:



About Gateways

You can deploy Cloud Edge gateways to customer locations and register the gateway as a gateway with Cloud Edge Cloud Console for remote management through the cloud.

From the **Gateways** tab, depending on the gateway model and deployment mode, you can do the following:

- View hardware and policy status information
- View gateway status for CPU temperature, CPU usage, disk partition usage, and memory usage

- View gateway network events, system events, VPN events, and policy enforcement logs
- Use the ping, traceroute, and ARP network tools to troubleshoot gateway IPv4 network connectivity issues
- Configure how the Cloud Edge gateway behaves when the traffic load is high
- Update the firmware or product components
- Configure and view network information
- Configure intranet security mode settings for gateways with hardware switch chipset
- Configure wireless network access control settings and manage wireless client connections for gateways that support wireless networking
- Configure User Virtual Private Network (VPN) settings with Secure Sockets Layer VPN (SSL VPN) or Layer 2 Tunneling Protocol (L2TP) VPN
- Configure bandwidth control rules to improve quality of service by saving bandwidth for network traffic that support business goals
- Configure Site-to-Site VPN
- Configure static routes and NAT
- Configure end-user management
- Configure LDAP settings for authentication (not supported in Japan)
- Configure WFBSS Endpoint Protection, an integrated solution with Worry Free Business Security Services (WFBSS) to control whether WFBSS endpoints with out-of-date WFBSS Security Agent patterns or endpoints without the WFBSS Security Agent installed can access the Internet
- Configure Suspicious Endpoints to provide network access control for endpoints on which Cloud Edge detects C&C callbacks above a configured threshold
- View a list of endpoint devices and vulnerabilities discovered in you network by Suspicious Endpoints.

- Configure Suspicious Endpoints to scan endpoint devices for vulnerabilities, weak passwords, and open ports.

Note

You cannot configure or view information about VPNs for Cloud Edge gateway models that do not support VPN.

About Log Analysis

From the **Analysis & Reports** tab, you can view interactive charts and graphs about log statistics uploaded from registered gateways and aggregated by Cloud Edge Cloud Console. You can track detailed information that might not appear in the dashboard or drill down to investigate raw logs.

- **Application Bandwidth**

  View and analyze bandwidth consumption across IP addresses, users, and applications on the network. After reviewing the logs, adjust policies to control communications, block unwanted traffic, and allocate bandwidth to critical traffic or services.

  If a customer uses only Cloud Edge 50G2 gateways running Cloud Edge 6.0 or later, view usage data for policy rules.

- **Policy Enforcement**

  View and analyze how policies control network traffic. After reviewing the logs, adjust policy rules to allow or block certain traffic and to troubleshoot improperly configured policies.

  The following events are included in **Policy Enforcement**:

  - Policy rules (application control, URL filtering, firewall)
  - Blocked lists

- **Internet Access**

  View and analyze the websites and domains accessed by specific users. After reviewing the logs, add URL category groups to filter certain types of traffic and approve or block specific URLs beyond those categories, as necessary.

If a customer uses only Cloud Edge 50G2 gateways running Cloud Edge 6.0 or later, view usage data for policy rules.

- **Internet Security**

  View and analyze how scan engines protect users from malware, network threats, and other potential harm. After reviewing the logs, enable or disable security features and adjust actions, schedules, or user policies to better protect the network.

  The following events are included in **Internet Security**:

  - Intrusion prevention
  - Malware protection
  - Email security protection
  - Web reputation
  - Botnet detection

After configuring a particular log query, click **Save** and select ⭐ **Save As Favorite** to record those settings for later viewing. Go to **Analysis & Reports** > **Log Favorites** to access the **Log Favorites** screen.

About Policies

From the **Policies** screen, you can manage Cloud Edge Cloud Console policy rules, policy objects, the approved and blocked lists, security profiles, user notifications, and the suspicious objects list and block action. Cloud Edge Cloud Console can enforce policies to some or all registered gateways.

You can create policy objects to customize options for the policy rules. The policy objects include interface groups, users/user groups, IP addresses/ FQDNs, MAC addresses, or geolocations to which the policies apply, what types of services, application groups, or URL group categories the policies affect, and the schedule for enforcing the policy rules.

You can fine-tune policy controls by configuring security profiles for IPS, anti-malware security, web reputation, email security, HTTPS inspection,

denial of service attacks, and endpoint identification. Optionally, you can add approved and blocked URLs that override the defined policy rules.

About Reports

From the **Analysis & Reports** tab, you can view and download scheduled or on-demand reports. Cloud Edge Cloud Console aggregates log information from all registered gateways. From these logs, you can generate reports about detected virus and malicious code, blocked files, and accessed URLs. You can use this information about network events to optimize settings and fine-tune security policies.

Gateway Management

MSPs use Cloud Edge Cloud Console to register new Cloud Edge gateways. After a customer powers on the Cloud Edge gateway and connects to the network, policies deploy, and MSPs can view related dashboard, log, and report statistics.

Managing Gateways

Purpose: Manage gateways from Cloud Edge Cloud Console.

Location: Gateways

Procedure

1. To manage gateways from Cloud Edge Cloud Console, you can do the following:
   - View information about the registered gateways.
   - Register a new gateway.
   - Import multiple gateways.
   - Create a new gateway group.
   - Search for a Cloud Edge device in the search box.
   - Choose the default security profile for a listed gateway.

If a gateway is a member of an HA group, the primary gateway's security profile is used for both the primary and secondary gateway.

- Perform select actions on a gateway.

Note

You cannot perform certain actions on gateways that are part of an HA group.

See *Gateway Actions on page 6-11*.

- Click a gateway name to manage that gateway.

  Gateways can be either a standard/G3 gateway or a Cloud Edge 50G2 gateway.

  -  : Standard/G3 gateway
  -  : Cloud Edge 50G2 gateway

    The Cloud Edge 50G2 gateway is a second-generation model with higher hardware and performance that runs on Cloud Edge 6.0 and later releases.

  The gateways that you can modify from the Cloud Edge Cloud Console vary and available management tasks are dependent on the gateway model and deployment mode.

2. Manage High Availability configurations for Cloud Edge gateways.

   - View information about existing HA groups.
   - Create one or more new HA groups.

     To create an HA group, you must have at least two gateways that support HA groups.

   - Enable an HA group.
   - Disable an HA group.

- When disabled, the two Cloud Edge gateways are still paired to each other. You cannot use either of the gateways to create a new HA group.
- End-user traffic might be down for a time depending on the user's network topology while the HA group is disabled.

- Edit an existing HA group.
- Perform a manual fail over (force takeover) for an existing HA group.
- Remove an existing HA group.

Note

All management actions generate an audit log.

Registration

The number of gateways available to register with Cloud Edge Cloud Console depends on your maintenance agreement with Trend Micro.

After registering a gateway, click the name to do the following:

- View general information about the gateway
- View information about the gateway's system status
- Use the ping, traceroute, and ARP network tools to troubleshoot gateway IPv4 network connectivity issues
- View gateway network events, system events, VPN events, and policy enforcement logs
- Configure how the Cloud Edge gateway behaves when the traffic load is high
- Configure network settings
- Configure intranet security mode settings for gateways with hardware switch chipset

- View wireless network settings for gateways that support wireless networking
- Configure wireless network access control settings and manage wireless client connections for gateways that support wireless networking
- Configure bandwidth control
- Configure User VPN
- Configure Site-to-Site VPN
- Configure end user authentication and TTL cache settings
- Configure LDAP settings for authentication (not supported in Japan)
- Update the Cloud Edge gateway
- Configure WFBSS Endpoint Protection, an integrated solution with Worry Free Business Security Services (WFBSS)
- Configure Suspicious Endpoints to provide network access control for endpoints on which C&C callbacks above a configured threshold are detected

Note

You cannot configure or view information about VPNs for Cloud Edge gateway models that do not support VPN.

Gateway Actions

Action	Description
	Add a new gateway group.
	Change the display name that appears for the gateway.
	Move the gateway to a different gateway group. You cannot move a gateway if it is in an HA group.

Action	Description
	Replace the gateway hardware by providing a new gateway serial number. You must replace a gateway that is part of an HA group with the same model as the original gateway. You must apply patches that were applied to the original gateway to the replacement gateway. Also reapply engine/pattern updates to the replacement gateway.
	Change the gateway's on-premises console password. For gateways that are part of an HA group, change password for each gateway independently.
	Update gateway components to stay protected from the latest security threats.
	Remotely restart the gateway.
	Delete the gateway from Cloud Edge Cloud Console. This gateway still scans for security threats on-premises but cannot receive remote commands or updates. You cannot delete a gateway if it is in an HA group.

Registering Gateways

Purpose: Register gateways to control policies and view log statistics through Cloud Edge Cloud Console.

Location: Gateways

Procedure

1. Click **Register New Gateway**.
2. Specify the gateway settings.
   - **Display name**

     Specify the name that appears in the cloud console for the new gateway.
   - **Model**

     Specify the Cloud Edge gateway hardware model.

- **Serial number**

  Specify the Cloud Edge gateway serial number. Find the serial number on the gateway itself or on the gateway packaging. The serial number is alphanumeric with 12 digits separated by hyphens (example: 4C80-9315-3A0B).

3. Click **Save**.

   It may take a few minutes for registration to complete.

   After registration, Cloud Edge Cloud Console deploys policies to the gateway. View log statistics through dashboard widgets, log analysis, and reports based on live traffic sent by the Cloud Edge gateway.

Importing Multiple Gateways

Purpose: It allows customers to upload a CSV file (with designated format) to register gateways in bulk.

Location: Gateways > Gateway Management

Procedure

1. Click the **Import Gateways** button.
2. In the Import Gateways popup, select a gateway model in the **Model** dropdown.
3. Click **Browse** to navigate to a CSV file on your local drive (click **Download Template** to download a .CSV file).

Note

In the .CSV file, customers should fill these 2 values of each gateway. Each gateway in a line. The Gateway Name field can be left empty so the system will automatically generate names for such gateways. The automatically generated gateway names are like "Cloudedge_01", "CloudEdge_02", etc. Do not delete the head row of the CSV file.

4. Click **Import**.

   On the Gateway Management page, the imported gateways will show in the Root group list. The Import Summary banner will show the number of successfully imported gateways and the number of gateways failed to import. Click **Fix the errors** to view the details of the gateways failed to import in a popup, which shows the failure details.

5. Click **OK** or click **Export Errors** to export the .CSV file to a local drive.

Verifying the Registration

Trend Micro recommends verifying each gateway after registration. The following procedure explains how to check that your gateway correctly registered with Cloud Edge Cloud Console.

Procedure

1. Log on to Cloud Edge Cloud Console.
2. Go to **Gateways**.
3. Confirm that the gateway appears in the **Gateway Management** list.
4. Confirm that the status in the **Policy Deploy Status** column is “Success”.
5. Click the name of the gateway.
6. Check the gateway information in the **Gateway Information** window that appears.

Viewing Information for All Gateways

Purpose: View gateway and HA group information for all gateways.

Location: Gateways

Procedure

1. View the information for all gateways.

- **Group/Gateway Name**: The group or gateway's name.
- **Status**: Current status in Cloud Edge Cloud Console for the gateway.
- **Last policy deployment**: Time stamp for the most recent policy deployment from Cloud Edge Cloud Console to the gateway.
- **Policy deployment status**: Last policy deployment result.
- **Last Log Uploaded**: Time stamp for the most recent logs uploaded from the gateway to Cloud Edge Cloud Console.
- **Security Profiles**: The Cloud Edge security profile applied to this gateway.
- **Actions**: Actions available for this gateway.

  You cannot move or delete a gateway if it is in an HA group. These action icons are not available for gateways that are part of an HA pair.

2. View the information about HA groups:

   - **HA Name**: The name for each HA group. Under each HA group name are the names of the two member Cloud Edge gateways.
   - **Enable**: Whether the HA group is **On** or **Off** .
   - **HA Role**: Role can be **Primary** or **Secondary**.
   - **Priority**: List the priority for the primary and secondary gateways.
   - **Heartbeat Interface**: List the heartbeat interface for the primary and secondary gateways.

     The interface must be the same for both the primary and secondary gateway.
   - **IPv4 Address/Netmask**: List the IPv4 address and netmask for the primary and secondary gateways.
   - **Version**: List the version for the primary and secondary gateways.

     Generally, version will be the same for both gateways, but might differ for a short time during upgrades.

- **HA states**: Status for the primary and secondary gateways.

  Possible statuses include:

- **Actions**: List of actions you can perform on the HA group: Edit, Remove, Force Takeover, Enable, Disable.

  To perform an action, click on the desired action.

Creating an HA Group

Purpose: You can create an HA group from Cloud Edge Cloud Console. An HA group consists of two Cloud Edge gateways. A gateway can belong to only one HA Group.

Location: Gateways

Procedure

1. Review information about HA Groups as needed.

   HA Groups on page 6-20

2. Connect an Ethernet cable directly between the heartbeat interfaces for each gateway that will be a member of the HA group.

   For the Cloud Edge 50G2 gateway, you can use only LAN2 or LAN3 for the heartbeat L3 interface. Moreover, you must use the same interface on each gateway (LAN2-to-LAN2 or LAN3-to-LAN3).

3. In the **High Availability Management** section, click **Create HA Group**.

   The **Create HA Group** wizard opens.

4. In the **Create HA Group and Choose Operation Mode** page, specify the following details:

Option	Description
HA group name	Name must be between 1 to 32 characters long and can contain letters, numbers, or the underline symbol.

Option	Description
Operation mode	Preset to **Active-Passive**, which is the only available mode.
Authentication method	Select one of the following: • **None** • **Simple** and then enter the password to use for simple authentication • **HMAC** and then enter the password to use for HMAC authentication
Enable	Select one of the following: • **On** • **Off**

5. Click **Next**.

6. In the **Configure Primary Gateway** page, configure settings for the Cloud Edge gateway that will be the primary gateway in the HA group.

Option	Description
Primary HA gateway	Select the gateway from the drop-down list that you want to designate as the HA primary gateway. Only gateways that support an HA group configuration are listed.
Role	A read-only field set to **Primary**, which is the role that will be assigned to this gateway.
Priority	Enter a priority number for this gateway (1-253). Default is 253. The gateway with the higher the priority is active.

Option	Description
Heartbeat interface	Select the L3 interface from the drop-down that Cloud Edge uses for communicating with the peer HA gateway. For the Cloud Edge 50G2 gateway, only LAN2 or LAN3 can be selected as the heartbeat interface.
Heartbeat interface IP / **Netmask**	If not already configured, you must enter an IPv4 address and netmask for the heartbeat interface. The heartbeat interface's IPv4 address for the primary and secondary gateways must be on the same subnet. After adding an interface to an HA pair, you cannot change the primary or secondary gateways for that interface.

7. Click **Next**.

8. In the **Configure Secondary Gateway** page, configure settings for the Cloud Edge gateway that will be the secondary gateway in the HA group.

Option	Description
Secondary HA gateway	Select the gateway from the drop down list that you want to designate as the HA secondary gateway. Only gateways that support an HA group configuration are listed.
Role	A read-only field set to **Secondary**, which is the role that will be assigned to this gateway.
Priority	Enter a priority number for this gateway (1-253). Default is 100. The gateway with the higher the priority is active.
Heartbeat interface	The L3 interface is preselected from the drop-down and is the same interface selected for the primary HA gateway. Cloud Edge uses the interface for communicating with the peer HA gateway.

Option	Description
Heartbeat interface IP / **Netmask**	If not already configured, you must enter an IPv4 address and netmask for the heartbeat interface. It must be on the same subnet as the heartbeat IP address configured for the primary.

9. Click **Next**.

10. In the **Configure Takeover When Failure Occurs** page, configure settings for the Cloud Edge HA group when a failure happens and takeover occurs.

Option	Description
Preemption	Select one of the following: • **On** (default): Primary gateway will return to active role after it recovers from a previous failure • **Off**: Primary gateway does not automatically resume the active role after recovery from a failure. User must perform manual failover.
Monitor interface	Select one or more interfaces to monitor. Cloud Edge monitors only physical interfaces. It is recommended to monitor all physical interfaces with traffic.
Monitor IP/FQDN	For each monitor interface, enter up to two IP addresses or FQDNs to use as monitor hosts.
Takeover triggers	You must enter values for the following: • **Heartbeat failure times**: Indicates the number of heartbeat failures before the passive gateway takes over from the failed gateway (default is 3, range is 3-9) • **Ping failure times**: Indicates the number of ping failures before the passive gateway takes over from the failed gateway (default is 3, range is 1-5)

11. In the **Configure Virtual Router Redundancy Protocol (VRRP) Group** page, add one or more VRRP groups.

a. Click **Add**.

b. Select an interface and enter the virtual IPv4 Address and netmask for the VRRP group.

You can select either an L3 physical interface or a static L3 VLAN interface, depending on the configuration.

See *HA Group – VRRP Groups on page 6-27* configuration requirements.

c. Save the VRRP group by clicking on the check mark to the right of the **IP Address/Mask** field.

You must add and save at least one VRRP group before clicking **Next**.

Note

You can delete a VRRP group by clicking on the "X" to the right of the VRRP group that you want to delete.

After clicking **Next**, the summary page opens.

12. Review the summary of the HA group settings.

Note

The primary HA gateway is active and the secondary HA gateway is passive when you first create an HA group.

13. Click **Save**.

HA Groups

You can configure two gateways as an HA Group to provide high availability access. One gateway is configured as the primary and one as the secondary. When first created, the primary HA gateway is active and the secondary is passive. If one gateway is down, then the other gateway will take over (becomes active) and ensures that network traffic is not down.

An HA Group can increase network traffic efficiency in addition to providing redundancy when a fatal error is encountered.

Basic Information

- You can use registered or unregistered gateways when creating an HA group.
    - **Unregistered**:

      Cloud Edge Cloud Console checks only the hardware model for each gateway chosen for the HA group. If they do not match, an error displays and the HA group is not saved.
    - **Registered**:

      Cloud Edge Cloud Console performs the following checks:
        - Checks hardware model, software version, and deployment mode for each gateway — if they do not match, an error displays and the HA group is not saved.
        - Checks the heartbeat interfaces — if they are not in the same subnet, an error displays and the HA group is not saved.
        - Checks the VRRP interfaces — if they are not in the same subnet, an error displays and the HA group is not saved.
        - Checks whether the gateways are online — both Cloud Edge gateways must be online to successfully save the HA group.
- A gateway can belong to only one HA Group.
- Only active–passive mode is supported.
- The active node is designated the master.
- The HA group can function in either preemption or non-preemption mode
    - **Preemption** (check box, default): Primary gateway will return to active role after it recovers from a previous failure.

- **Non-preemption**: Primary gateway does not automatically resume the active role after recovery from a failure. User must perform manual failover.

- Before creating an HA group, ensure that the following items are addressed
  - Gateways in an HA group must be deployed in routing mode.
  - Gateways in an HA group must be the same model.
  - Gateways in an HA group must have the same firmware version.

    Note

    When the firmware version is updated or rolled back on one gateway in an HA group, the firmware must be updated or rolled back to the same version on the other gateway in the HA group.

  - Gateways in an HA group must have the same timezone configuration and the time difference must be within 5 minutes.
  - The factory default interface settings for gateways must be configured before creating an HA group.
- Cloud Edge Cloud Console pushes configurations for the gateways in an HA group to the gateways; however, if configuration updates are not possible, nodes from an HA group can synchronize using the heartbeat connection.
- In the dashboard, logs, and reports, queries are supported for the primary, secondary and HA group.
- Since policy templates configured on Trend Micro Remote Manager are deployed before an HA group is set up, there is no impact to HA groups. To Remote Manager, an HA group appears to be two stand-along gateways.

Additional HA Group Information

- *HA Group - WAN Topologies on page 6-23*

Supported Models for HA Groups

The following models are supported for HA Groups:

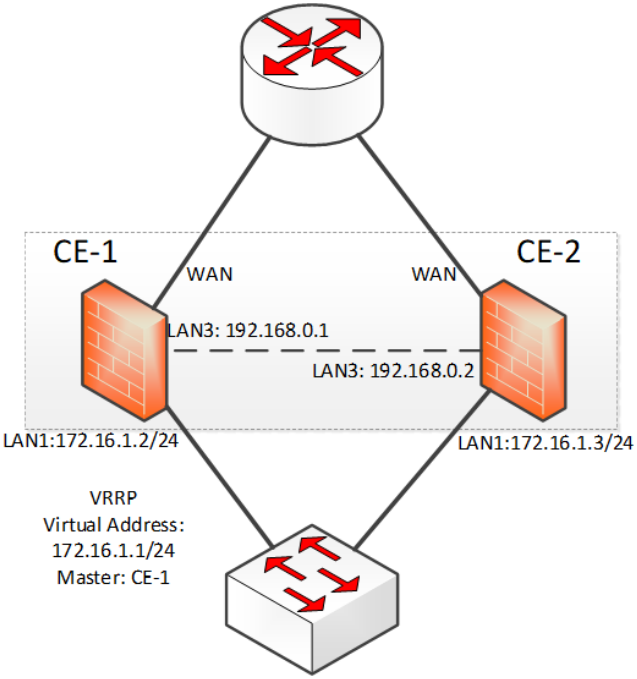
- Cloud Edge 50G2 gateway

HA Group - WAN Topologies

One Route Next Hop

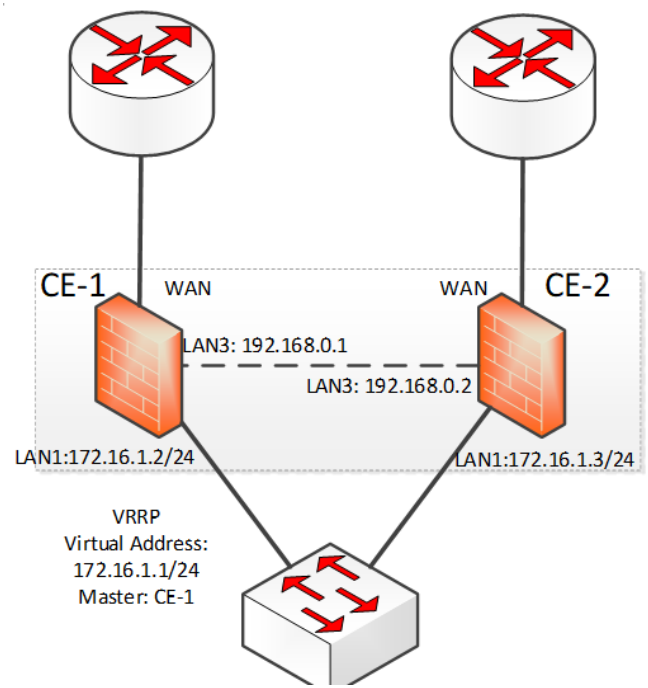
In this scenario, because CE-1 and CE-2 are connected to a single router, the packets coming through the WAN interface of CE1 cannot be in the same

subnet of packets coming from CE-2. In such a scenario, NAT must be enabled.



Router Is Two Hops

There is no issues for this scenario.



HA Group – Failover Conditions

When using Cloud Edge HA groups, you should understand under what conditions an HA group failover occurs, which include the following:

- One or more of the monitor interfaces are down
- Heartbeat or ping takeover thresholds reached
- Active gateway does firmware update
- Replacing an active gateway
- Force takeover

If the HA group is in an abnormal state, force takeover will not happen.

When force takeover is triggered, the primary will become standby and the secondary will become active.

HA Group – Heartbeat Interfaces

When creating a Cloud Edge HA group, one interface on each HA peer is designated as the heartbeat interface. This interface is chosen during HA group creation.

- The heartbeat interface must be an L3 interface.
- The heartbeat interface must use the same interface on each gateway (for example: LAN2-to-LAN2 or LAN3-to-LAN3).
- The two heartbeat interfaces must be connected directly to each other (not through a switch).
- Heartbeat interfaces cannot be used for other purposes, such as LAN traffic interfaces.
- You must configure IPv4 addresses and netmasks for the heartbeat interfaces and the IPv4 addresses must be on the same subnet.
- After an interface has been selected as a heartbeat interface, you cannot change the configuration of that interface, including gateway IP addresses.

Managing a Split-brain Condition

- Because Cloud Edge uses only one interface for the HA group heartbeat, issues with the heartbeat connection might cause an condition known as the split-brain problem. Cloud Edge must be able to handle this condition.
- *Split-brain*: A split-brain condition is the result of a cluster partition, where each side believes the other is dead, and then proceeds to take over resources as though the other side no longer owns any resources.

HA Group – VRRP Groups

When creating a Cloud Edge HA group, Virtual Router Redundancy Protocol (VRRP) groups are created as part of the HA Group configuration.

- Due to the fact that the WAN side might connect to a router directly, Cloud Edge only supports LAN–side virtual IP addressing. The primary and secondary gateways each have their own WAN configuration.
- You can select either an L3 physical interface or a static L3 VLAN interface, depending on the configuration:
  - Both gateways unregistered: Only physical interface can be selected
  - Both gateways registered: Either physical interface or VLAN interface can be selected

    The VLAN interface must exist in both gateways.
  - Primary gateway registered, secondary unregistered: Only physical interface can be selected
  - A physical interface/VLAN interface can be used in only one VRRP group.
  - WAN interface cannot be used in VRRP group.
- Only IPv4 virtual IP addresses are supported for the VRRP groups.

HA Group - Endpoint Network Access

To provide network access to endpoints through an HA group, use one of the following methods:

- Dynamic addressing
  1. In the Cloud Console or on-premises console, configure the DHCP service on the VRRP group interface for both the primary and secondary gateways in the HA group.

Note

The gateway address of the DHCP service must be the virtual IP address of the VRRP group.

The DHCP settings for the interfaces must be identical on the primary and secondary gateways in the HA group.

For more details, see *DHCP on page 6-70*.

2. On the endpoints, configure the endpoints to obtain an address through DHCP.

- Static addressing

1. On the endpoints, configure the IP address and subnet mask to be in the same subnet as the VRRP group interface.
2. On the endpoints, configure the gateway address to be the same as the virtual IP address of the VRRP group.

HA Group – Monitor Interfaces and Takeover Triggers

When creating Cloud Edge HA groups, you configure monitor interfaces that are used to do basic interface and protocol monitoring to determine if failover conditions are met. You can also configure the takeover thresholds for heartbeat and ping takeover triggers.

- **Monitor interface**: Cloud Edge performs basic target tracking for selected physical interfaces (WAN and some LAN ports). It is recommended that you select all available physical interfaces for monitoring.
- **Monitor IP/FQDN**: You can enter up to two IP addresses or FQDNs to monitor for each of the selected monitor interfaces.
- **Takeover triggers**: Cloud Edge tracks heartbeat and ping thresholds.

  Takeover will be initiated if either takeover trigger is met.

  If two monitor hosts are configured, takeover occurs if pings to both hosts fails. Ping failure to one of the two hosts does not result in

takeover. If there is only one monitor host, failover is triggered if the ping threshold on that host is reached.

HA Groups - Configuration Settings Matrix

The following matrix provides information about how Cloud Edge manages HA Group configuration settings.

The following features are configured on each gateway separately. "Yes" means can do configuration in Cloud Edge Cloud Console.

Feature	Primary	Standby	Detail
Gateway Information – General, Status, Logs/Events, Tools)	Yes	Yes	
Gateway Information – Advanced (Conservative Mode setting)	Yes	Yes	
Interface	Yes	Yes	Heartbeat interface configure only through HA groups, not through interfaces page.
Administrative Access	Yes	Yes	
DHCP	Yes	Yes	
Dynamic DNS	Yes	Yes	
Routing Table	Yes	Yes	
Static Route	Yes	Yes	
NAT	Yes	Yes	
Bandwidth Control	Yes	Yes	
L2TP VPN	Yes	Yes	
SSL VPN	Yes	Yes	

Feature	Primary	Standby	Detail
Site–to–Site VPN	Yes	Yes	
End User Management – General Settings	Yes	Yes	
LDAP Settings	Yes	Yes	
Updates	Yes	Yes	The "Installed Updates" might be different for a short time.
WFBSS Endpoint Protection (General)	Yes	Yes	
WFBSS Endpoint Protection (Troubleshooting)	Yes	Yes	
Suspicious Endpoints (General)	Yes	Yes	
Suspicious Endpoints (Troubleshooting)	Yes	Yes	
Diagnostic Files	Yes	Yes	
Packet Capture	Yes	Yes	
Hidden Page	Yes	Yes	

HA Groups – Policy Settings Matrix

You should understand how policies work with gateways in an HA group.

Policy Setting	Details
Gateways are not part of an HA group when Policy Rules, Interface Groups, or Approved/Blocked List were configured.	The primary's configuration will be applied to the HA pair. The secondary's old policies will not be used.

Policy Setting	Details
Gateways are already part of an HA group prior to setting up Policy Rules, Interface Groups, or Approved/ Blocked List.	Policy Rules and Approved/Blocked list are configured for the HA pair, not for the primary or secondary. If want to select Interface Groups in policy rules, select only one standalone gateway or one HA pair for that rule.
You can configure Interface Groups for gateways in an HA group.	Configure the Interface Group for the primary gateway and it will be used by the HA pair. To do this, primary and secondary must have similar VLAN and VPN configurations. Keep the following consideration in mind: If the primary is registered while the secondary is unregistered and the primary's policy rules use Interface Groups that contain VLANs or VPNs, the those primary rules cannot be applied successfully to the secondary. For this case, you should configure VLANs and VPNs for the secondary after it's registered, then perform policy deployment.
Policies are deployed to both gateways in an HA group.	Keep the following consideration in mind: Policy deployment might be successful to one gateway but failed to another.
You can configure geolocations for policies used by the HA group.	Keep the following consideration in mind: Certain policy rules with geolocations configured in policy rules might not work after failover in an HA group. This is because the gateways might have different versions of the location database.
After destruct of an HA group, both the primary and secondary will use the policies configured for the HA group.	Keep the following consideration in mind: If the policy rule has configured interface groups, it will only be applied to the primary gateway.

HA Group Limitations

You should be aware of certain HA Group limitations.

Limitation	Description
NAT connections	NAT connection tracking will not be synchronized.
Split brain issue	Cloud Edge gateways have limited ports, which means there might be only one port for the heartbeat.

HA Group - Actions

Action	Description
	Edit HA group configuration.
	Force takeover in the HA group. When force takeover is triggered, the primary will become standby and the secondary will become active.
	Enable the HA group. The HA group becomes operational after clicking **Deploy All**.
	Disable the HA group. The HA group becomes non-operational after clicking **Deploy All**.
	Remove the HA group from Cloud Edge Cloud Console.

Replacing a Gateway

Replacing a gateway with a different Cloud Edge gateway maintains all policies, configuration data, and logs on Cloud Edge Cloud Console. Replace a gateway for the following reasons:

- The Cloud Edge gateway is malfunctioning or broken.
- The customer wants to upgrade to a higher performance Cloud Edge gateway.

Once the new Cloud Edge gateway synchronizes log statistics with Cloud Edge Cloud Console, Cloud Edge Cloud Console merges the new log statistics with cached data from the replaced Cloud Edge gateway.

Note

You can replace a gateway that is in an HA Group only with a gateway that is the same model and firmware version as the gateway being replaced.

Before replacing a gateway in an HA Group, remove the Ethernet cable from the heartbeat interface of the gateway that you are replacing and connect the Ethernet cable to the heartbeat interface of the new gateway.

Important

Each gateway has a unique key (serial number) associated with a specific registered Cloud Edge gateway on Cloud Edge Cloud Console. After replacing the gateway, you can no longer use the old Cloud Edge gateway unless you register the Cloud Edge gateway as a new gateway.

Note

After replacing the gateway, only the policy settings are restored.

Procedure

1. Go to **Gateways**.
2. Right-click the gateway to replace, then select **Replace**.
3. Specify the new Cloud Edge gateway serial number.
4. Click **Replace**.
5. Remove the old Cloud Edge gateway from the network.
6. Add the new Cloud Edge gateway to the network.

The new Cloud Edge gateway registers to Cloud Edge Cloud Console and the old Cloud Edge gateway is removed from Cloud Edge Cloud Console.

Gateway Information

Purpose: Click a gateway name to manage that gateway from Cloud Edge Cloud Console.

Location: Gateways > (Selected Gateway)

Procedure

1. To manage a selected gateway from Cloud Edge Cloud Console, you can do the following:
    - View information and perform tasks under the gateway information section.
        - View general information, system status information, and gateway logs and events about the selected gateway.
        - Use tools to troubleshoot network connection issues or enable/disable conservative mode for high traffic conditions.
    - Configure network settings.
        - Interfaces (including VLANS)
        - Administrative access
        - DHCP
        - Dynamic DNS
        - Routing table (viewing only)
        - Static routes
        - NAT
    - Configure bandwidth control.
    - Configure user VPN.

    - L2TP VPN
    - SSL VPN
- Configure Site–to–Site VPN.
- Configure end-user management.
    - General settings
    - LDAP settings
- Configure LDAP
- Manage gateway updates.
- Configure network access control.
    - WFBSS Endpoint Protection
    - Suspicious Endpoints

Viewing General Gateway Information

Purpose: View hardware, network, and registration information for selected gateways.

Location: Gateways > (Selected Gateway) > Gateway Information > General

---

Procedure

1. View the gateway information.

   Gateway Information

   - **Display name**: The gateway's name. You can use gateway actions to rename the gateway.
   - **Status**: Current status in Cloud Edge Cloud Console for the gateway.
   - **Last policy deployment**: Time stamp for the most recent logs uploaded from the gateway to Cloud Edge Cloud Console.
   - **Policy deployment status**: Last policy deployment result.

- **Total users**: The user count of active sessions in the last 15 minutes.

Network Settings

- **Deployment mode**: Whether the Cloud Edge gateway is deployed in Bridge Mode or Routing Mode.

  A Cloud Edge gateway deployed as a Software Switch configuration is listed as a Bridge Mode device.

- **Host name**: The Cloud Edge gateway host name.
- **DNS**: The Cloud Edge gateway DNS settings.
- **WAN**: The Cloud Edge gateway and subnet mask settings.
- **Interface status** (Bridge Mode label: **Virtual Interface status**): The interface link state.

  Hover over an interface to see the following link information: link speed, duplex, MTU, send and receive packets, send and receive bytes

  Hover over a wireless interface to see the nick name assigned to the wireless interface and the MTU.

Hardware and Registration

- **Model**: The Cloud Edge gateway hardware model.
- **Serial number**: The currently registered serial number.
- **Hard disk parameters**
- **Registration date**: The date and time when the Cloud Edge gateway registered with Cloud Edge Cloud Console.
- **Version**: The Cloud Edge gateway build number.
- **Factory reset version**: The factory reset package version of the Cloud Edge gateway.
- **Uptime**: The running time since the Cloud Edge gateway hardware powered on.

- **Mail security status**: The current status of Cloud Edge mail security scanning.
  - Cloud scan is enabled.
  - Local scan is enabled.
  - Cloud scan has failed back to local scan since YYYY-MM-DD hh:mm:ss TZ.

    TZ represents the timezone of the company.
  - Email security is disabled.

Note

"--" is displayed when the Cloud Edge gateway is offline.

Viewing Gateway System Status

Purpose: View CPU temperature, CPU usage, data partition usage, and memory usage information for the selected gateway. You can manually refresh the page to see updated data.

Location: Gateways > (Selected Gateway) > Gateway Information > Status

Procedure

1. View the gateway system status information.

   Temperature

   - View the CPU temperature over the selected time period: Today, Last 1 hour, Last 12 hours, Last 24 hours, Last 7 days

   CPU Usage

   - View the CPU usage over the selected time period: Today, Last 1 hour, Last 12 hours, Last 24 hours, Last 7 days
   - View the current CPU usage.

   Disk Partition Usage

NOTICE

For versions earlier than Cloud Edge 5.2, only system disk information is displayed.

- View the system disk usage over the selected time period: Today, Last 1 hour, Last 12 hours, Last 24 hours, Last 7 days
- View the data disk usage over the selected time period: Today, Last 1 hour, Last 12 hours, Last 24 hours, Last 7 days
- View the current system disk usage.
- View the current data disk usage.

Memory Usage

- View the system memory usage over the selected time period: Today, Last 1 hour, Last 12 hours, Last 24 hours, Last 7 days
- View the current memory usage.

Viewing Gateway Logs and Events

Purpose: View gateway network events, system events, VPN events, and policy enforcement logs. You can manually refresh the page to see updated data.

Location: Gateways > (Selected Gateway) > Gateway Information > Log/Events

Procedure

1. View the gateway event log information.

   A log entry records the following information: Date/Time, Client IP, Sub-category, Event, Message

2. (Optional) Filter results by selecting one of the following categories:

   - **System Events**

- **Network Events**
- **VPN Events**
- **Policy Enforcement Logs**
- **Trust Certificate Events**

System, network, and VPN events display at the bottom of the page.

If **Policy Enforcement Logs** is selected, the **Analysis and Reports - Policy Enforcement** screen opens to display the results.

Note

VPN events display only for Cloud Edge gateway models that support VPN.

3. You can further filter event results using the following:
   - **Period**

     Available time periods: Today, Last 15 Minutes (default), Last 1 hour, Last 12 hours, Last 24 hours, Last 7 days
   - **Client IP**
   - **Sub-category**
   - **Event**

     See *Event Categories and Sub-Categories on page 6-39*.

Event Categories and Sub-Categories

TABLE 6-1. Event Categories and Sub-categories

CATEGORY	SUB-CATEGORY
System Events	Firmware Update
	Engine/Pattern Update
	System Status

Category	Sub-Category
	Service
	Device Access
Network Events	DHCP
	Interface
	PPPOE
VPN Events	L2TP
	SSL VPN
	Site-to-Site VPN
Policy Enforcement Logs	
Trust Certificate Events	Trust Certificate
	Not Trust Certificate
Smart Bypass Events	

Using Tools to Troubleshoot Network Connectivity

Purpose: Use IPv4 network tools to verify the gateway configuration or to troubleshoot gateway connectivity.

Location: Gateways > (Selected Gateway) > Gateway Information > Tools

---

Procedure

1. Perform the appropriate action:
   - *Performing a Ping Test on page 6-41*
   - *Performing a Traceroute Test on page 6-41*

- *Retrieving ARP Results on page 6-42*

Performing a Ping Test

Purpose: Use a ping test to verify the gateway configuration or to troubleshoot gateway connectivity.

Location: Gateways > (Selected Gateway) > Gateway Information > Tools

Procedure

1. Click on the **Ping** tool icon.
2. Enter an IPv4 address or a domain name to ping.
3. Optional: Enter additional parameters for ping.
   - **Select a network interface to send pings**: Default is any interface.
   - **Bytes**: Default is 56.
   - **Count**: Default is 4. Maximum is 10.
4. Click **Ping**.
5. View ping results at the bottom of the page.
   - Historical ping results are stored for two weeks and are displayed below the current ping results.
   - A maximum of ten results are displayed in the historical ping results.
   - If you leave the **Tools** screen, results are cleared from the page.

Performing a Traceroute Test

Purpose: Use a traceroute test to verify the gateway configuration or to troubleshoot gateway connectivity.

Location: Gateways > (Selected Gateway) > Gateway Information > Tools

Procedure

1. Click on the **Traceroute** tool icon.
2. Enter an IPv4 address or a domain name to which you want to trace the route.
3. Click **Start**.
4. Either wait for the trace to complete or stop the trace route by clicking on **Stop**.

   Only one trace route can run at a time. To start a new trace while one is still running, you must first stop the running trace.
5. View trace results at the bottom of the page.
   - Historical trace route results are stored for two weeks and are displayed below the current trace route results.
   - A maximum of ten results are displayed in the historical trace route results.
   - If you leave the **Tools** screen, results are cleared from the page.

Retrieving ARP Results

Purpose: Retrieve ARP results to verify the gateway configuration or to troubleshoot gateway connectivity.

Location: Gateways > (Selected Gateway) > Gateway Information > Tools

Procedure

1. Click on the **ARP** tool icon.
2. Perform the appropriate action:
   - Click on **Get ARP** to retrieve ARP information.
   - Click on **Clear ARP Cache** to clear the gateway's ARP cache.

Note

This does not clear the current page history.

3. View the ARP cache results at the bottom of the page.
   - The following information displays: IPv4 address, host name (if available), MAC address, interface
   - A maximum of 100 rows is displayed.
   - Click **Get ARP** to retrieve the ARP cache again.
   - If you leave the **Tools** screen, result histories are cleared from the page.

Enabling/Disabling Conservative Mode

Purpose: Conservative mode allows you to configure how the Cloud Edge gateway behaves when the traffic load is high.

Location: Gateways > (Selected Gateway) > Gateway Information > Advanced

Procedure

1. Perform the desired action:
   - Click **On** to enable conservative mode.

     Block additional traffic when the traffic load is high. Normal traffic inspection resumes automatically when traffic load is reduced.
   - Click **Off** to disable conservative mode.

     Do not inspect traffic if traffic load is high. Traffic traverses device without inspection. This is the default option and is the recommended setting.
2. If you clicked **On**, click on **Enable** in the **Enable Conservative Mode** confirmation screen.

Network

View and configure network settings in the cloud to process and identify network traffic on registered gateways. Once a gateway registers with the Cloud Edge Cloud Console, certain network settings move to the cloud and cannot be edited through the Cloud Edge on-premises console. Certain critical network settings that will cause network break down are configured through the on-premises console.

Note

- Cloud Edge supports only IPv4 when configuring Cloud Edge interfaces, VLANs, or functionality related to the gateway's physical or virtual interfaces.

  Additional functionality where only IPv4 is supported includes administrative access, DHCP, Dynamic DNS, DNS, routing, NAT, VPN.

  See *Support for IPv6 on page 1-20*.

- Cloud Edge Cloud Console does not support adding or editing a bridge when deployed in Routing Mode.
- The Software Switch configuration is supported only in Bridge Mode and must be configured using the on-premises console.
- For Cloud Edge gateways with wireless functionality, only IPv4 is supported when configuring the wireless interfaces and related network functionality.

  Wireless functionality is supported only in Routing Mode.

- If some network settings did not deploy successfully, the reason is displayed on Cloud Edge Cloud Console.
- Gateways collect and send network information to the Cloud Edge Cloud Console through a network heartbeat.

Network Settings Moved to the Cloud

1. Interfaces

   Routing Mode

   - Configure interfaces and L3 VLANs for the LAN2-LAN3 interfaces and the MGMT interface

     For gateways with hardware switch chipset, configure the LAN2-LAN8 interfaces and the MGMT interface.

   - Configure wireless network access settings (for gateways that support wireless functionality)

     L3 VLANS are not supported on wireless network interfaces.

   Bridge Mode

   - Configure interface settings and L3 VLANs only on the MGMT interface

2. Administrative access (after gateway registration)

   - Configure administrative access for using the on-premises console, ping, SSH, and SNMP (all interfaces)

3. DHCP (in Routing Mode only)

   - Configure the LAN2-LAN3 and MGMT interfaces to act as DHCP servers

     For gateways with wireless functionality, you can additionally configure DHCP on the main and guest wireless networks if the wireless networks are enabled.

   - For gateways with hardware switch chipset, configure DHCP on LAN2-LAN8 and the MGMT interface

   - You can configure DHCP on L3 VLANS that are subinterfaces of the above physical interfaces.

4. Service - Dynamic DNS

5. Routing (in Routing Mode only)

- View the routing table (also available from the on-premises console)
- Configure static routes

6. NAT
7. Bandwidth control
8. User VPN
    - SSL VPN
    - L2TP VPN
9. Site-to-Site VPN
10. End-User Management
    - General authentication settings (TTL options for authentication cache)
11. Wireless Networks
    - Configure network access control for the main and guest wireless networks
    - Manage wireless network client connections.
    - View wireless network configuration information and troubleshooting logs

Note

You must use the on-premises console to make changes to the wireless configuration.

Network Settings Kept at the Gateway

1. Interfaces
    - Edit interfaces: WAN or LAN1
    - Add/Edit L3 VLANs: WAN or LAN1
    - Enable or disable interfaces: LAN2-LAN3 (LAN2-LAN7 for gateways with hardware switch chipset)

- Wireless network interfaces: You cannot disable these interfaces from the interfaces page.

  To disable wireless interfaces, you must disable the respective wireless network using the on-premises console.

2. DNS - Configure IPv4 DNS servers
3. Addresses - View and edit address objects used in policy routing rules
4. Bridge Mode settings
   - Configure the bridge interface (br0) or switch interface (sw0)
   - Configure other bridge or switch settings
5. Software Switch
   - Configure the bridge interface (br0)
   - Configure other software switch settings
6. Routing
   - Create policy route rules
   - View routing table (also available from Cloud Edge Cloud Console)
7. Service - DHCP

   Configure interfaces to act as DHCP servers: WAN or LAN1
8. Wireless Networks
   - Enable and configure the main and guest wireless networks
   - View wireless network troubleshooting logs

Note

The Cloud Edge 300 does not have a LAN3 interface.

Interfaces

Cloud Edge autodetects the Cloud Edge gateway's L2 and L3 interfaces.

Routing Mode

After registering the gateway on Cloud Edge, you must manage all interfaces with the exception of the WAN and LAN1 interfaces from Cloud Edge Cloud Console.

- All interfaces are configured as L3 interfaces with IPv4 addresses.
- You must configure the LAN2-LAN3 and MGMT interfaces with static IPv4 addresses.

  For Cloud Edge gateways with hardware switch chipset, you must configure LAN2-LAN8 and MGMT interfaces with static IP addresses.

  For Cloud Edge gateways with wireless functionality, you must configure the wireless network interfaces with static IP addresses.

Note

You must configure WAN and LAN1 from the Cloud Edge on-premises console.

Bridge Mode

The Bridge Mode interfaces are read-only from Cloud Edge Cloud Console. You must configure and manage the bridge interface (br0) and physical interface settings from the Cloud Edge on-premises console.

- The virtual bridge interface (br0) is the L3 interface that Cloud Edge uses to connect to the Internet and is assigned an IPv4 address.
- All physical interfaces (other than the MGMT interface) are configured as L2 interfaces.

  You can configure the MTU setting on the physical L2 interfaces.
- You can configure the MGMT port as an L3 interface from Cloud Edge Cloud Console.

Software Switch

Software Switch interfaces are read-only from Cloud Edge Cloud Console. You must configure and manage the bridge interface (br0) used in a software

switch configuration and the physical interfaces from the Cloud Edge on-premises console.

- The virtual bridge interface (br0) is the L3 interface that Cloud Edge uses to connect to the internet and is assigned an IPv4 address.
- You must add at least three physical L2 interfaces to the software switch configuration, WAN and LAN1 and at least one of LAN2 or LAN3.

  You can configure the MTU setting on the physical L2 interfaces.
- You can configure the MGMT port as an L3 interface from Cloud Edge Cloud Console.

Bridge Mode (With Switch Chipset)

Bridge Mode interfaces on gateways with hardware switch chipset are read-only from Cloud Edge Cloud Console. You must configure and manage the switch interface (sw0) used in a hardware switch configuration and the physical interfaces from the Cloud Edge on-premises console. However, switch interface (sw0) settings related to the level of intranet security (traffic that traverses between internal LAN ports) must be managed from Cloud Edge Cloud Console.

- The virtual switch interface (sw0) is the L3 interface that Cloud Edge uses to connect to the Internet and is assigned an IPv4 address.
- All physical interfaces (other than the MGMT interface) are configured as L2 interfaces.

  You can configure certain settings on the physical interfaces, depending on the Intranet Security mode setting selected for the gateway.
- You can configure the MGMT port as an L3 interface from Cloud Edge Cloud Console.

Note

Cloud Edge 300 does not have a LAN3 interface.

For all deployment modes and all Cloud Edge gateway models, you can enable or disable certain interfaces.

Enabling or Disabling Interfaces on page 6-54

Managing Network Interfaces

Purpose: Manage the network interface settings for selected gateways.

Location: Gateways > (Selected Gateway) > NETWORK > Interfaces

Procedure

1. Do the following:
   - View the table to learn about the gateway's network settings and link status.
   - Click an interface name to *Edit an Interface on page 6-51*.
   - Click the ⊞ to add a *VLAN subinterface on page 6-67*.

   The interfaces that you can modify and VLANs you can create from the Cloud Edge Cloud Console vary and are dependent on the gateway model and deployment mode.
2. For Cloud Edge gateways in Bridge Mode or gateways with the with hardware switch chipset in Bridge Mode, you can do the following:
   - View the bridge interface (br0) or switch interface (sw0) settings.
   - Click the switch interface (sw0) to configure Intranet Security mode settings.
3. For existing VLANS, you can do the following:
   - View the **VLAN** table to learn about the VLAN settings and link status.

- Click an VLAN interface name to edit or disable/enable a *VLAN subinterface on page 6-67*.
- Click **Delete** to delete the desired VLAN interface.

Editing Network Interfaces

Purpose: Manage the network interface settings for selected gateways.

Location: Gateways > (Selected Gateway) > NETWORK > Interfaces

Procedure

- Use the appropriate procedure according to your gateway's deployment mode settings.
  - *Routing Mode: Editing Network Interfaces on page 6-51*
  - *Routing Mode: Editing Wireless Network Interfaces on page 6-52*
  - *Bridge Mode: Editing Network Interfaces on page 6-53*

    Use this procedure for Bridge Mode, Bridge Mode (With Switch Chipset), and Software Switch deployments.

Routing Mode: Editing Network Interfaces

Purpose: Manage the network interface settings for selected gateways. After a gateway in Routing Mode is registered you must edit all interfaces, with the exception of the WAN and LAN1 interfaces, from Cloud Edge Cloud Console.

Location: Gateways > (Selected Gateway) > NETWORK > Interfaces

Procedure

1. Click an interface's name.
2. Configure the interface settings.

   To configure wireless network interfaces, see *Routing Mode: Editing Wireless Network Interfaces on page 6-52*.

Option	Description
Type	Select **L3**. If there are any outstanding setting changes on Cloud Edge Cloud Console, you cannot change the interface type until after you click **Deploy All** to make the existing changes effective.
Mode	This is a read-only field where the mode is pre-set to **Static**.
IPv4 address	Specify the IPv4 address (example: `10.10.10.23`).
IPv4 netmask	Specify the IPv4 subnet mask (example: `255.255.254.0`).
IPv4 default gateway	Specify the IPv4 default gateway (example: `10.10.10.1`). This settings is only required for WAN configurations.
MTU	Specify a value from 576 through 1500.
MSS	Select **Overwrite** and specify a value from 536 through 1460. **Note** The MSS value must not be greater than (MTU - 40).

3. Click **Save**.

Routing Mode: Editing Wireless Network Interfaces

Purpose: Manage the wireless network interface settings for selected gateways. After a gateway in Routing Mode is registered you must edit all wireless network interfaces from Cloud Edge Cloud Console.

Location: Gateways > (Selected Gateway) > NETWORK > Interfaces

---

Procedure

1. Click a wireless network interface's name.

   The wireless network interface name is read-only and is preset to the **SSID** assigned to that wireless network.

2. Configure the interface settings.

Option	Description
Type	This is a read-only field where **Type** is pre-set to **L3**.
Mode	This is a read-only field where the mode is pre-set to **Static**.
IPv4 address	Specify the IPv4 address (example: `10.10.10.23`).
IPv4 netmask	Specify the IPv4 subnet mask (example: `255.255.254.0`).
IPv4 default gateway	Specify the IPv4 default gateway (example: `10.10.10.1`). This settings is only required for WAN configurations.
MTU	Specify a value from 576 through 1500.
MSS	Select **Overwrite** and specify a value from 536 through 1460. **Note** The MSS value must not be greater than (MTU - 40). If MTU on the wlan interface is modified, MSS must be set correspondingly (MSS value is less than MTU - 40).

3. Click **Save**.

Bridge Mode: Editing Network Interfaces

Purpose: Manage the network interface settings for selected gateways. After a gateway in Bridge Mode is registered (including the Software Switch variation of Bridge Mode), you can edit only the MGMT interface from Cloud Edge Cloud Console.

Location: Gateways > (Selected Gateway) > NETWORK > Interfaces

Procedure

1. Click an interface's name.
2. Configure the interface using static mode settings.

Option	Description
Type	Select **L3**. If there are any outstanding setting changes on Cloud Edge Cloud Console, you cannot change the interface type until after you click **Deploy All** to make the existing changes effective.
Mode	This is a read-only field where the mode is pre-set to **Static**.
IPv4 address	Specify the IPv4 address (example: `10.10.10.23`).
IPv4 netmask	Specify the IPv4 subnet mask (example: `255.255.254.0`).
MTU	Specify a value from 576 through 1500.
MSS	Select **Overwrite** and specify a value from 536 through 1460. **Note** The MSS value must not be greater than (MTU - 40).

3. Click **Save**.

Enabling or Disabling Interfaces

Certain of the Cloud Edge gateway's interfaces might be enabled or disabled by default, depending on the deployment mode. In certain configurations, you might not be able to disable some interfaces.

Note
You cannot disable the MGMT port in any deployment mode.

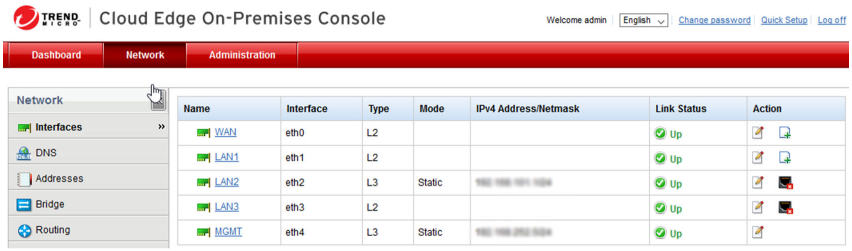


FIGURE 6-1. Example: Cloud Edge 70 in Routing Mode

You enable or disable interfaces from the Cloud Edge on-premises console.

- Routing Mode: LAN2 and LAN3 are enabled by default.

  You can disable or re-enable these interfaces at any time.

- Bridge Mode: LAN2 and LAN3 are disabled by default.

  You can enable or disable these interfaces at any time.

- Software Switch: LAN2 and LAN3 are automatically enabled when you add them as a software switch interface.

  You cannot disable an interface if it is part of a Software Switch configuration.

Note

The Cloud Edge 300 gateway does not have the LAN3 interface.

Cloud Edge Gateways with Hardware Switch Chipset

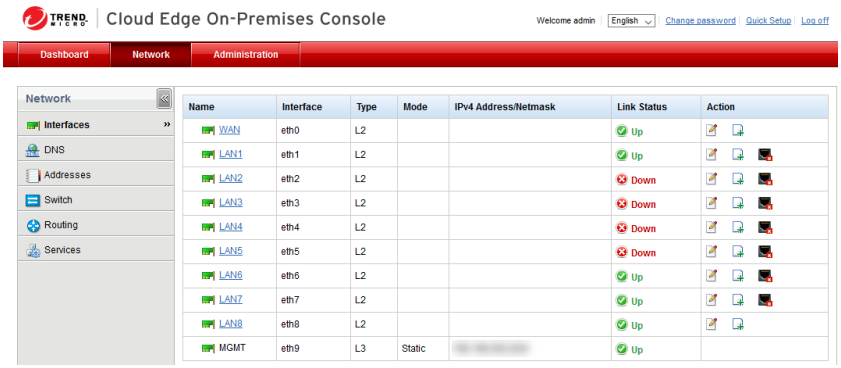


FIGURE 6-2. Example: Cloud Edge 100 G2 in Bridge Mode

All ports are enabled by default. You cannot disable the WAN, LAN8, or MGMT interfaces.

- Routing Mode

  You can disable the LAN1-LAN7 interfaces.

- Bridge Mode

  The WAN and LAN1-LAN8 interfaces are automatically selected as ports for the hardware switch. These ports cannot be removed from the hardware switch configuration; however, you can disable the LAN1-LAN7 interfaces.

Cloud Edge Gateway with Wireless Network Functionality

You cannot enable or disable wireless network interfaces from the **Interfaces** page.

The main wireless network is automatically enabled when you enable wireless access and guest wireless network is automatically enabled when you enable the guest wireless network. The wireless network interfaces are automatically disabled if you disable the corresponding wireless network.

Procedure

1. From the Cloud Edge on-premises console, go to **Network** > **Interfaces**.
2. Do one of the following:
   a. For the interface that you want to enable, click the **Enable** icon ().
   b. For the interface that you want to disable, click the **Disable** icon ().

Configuring Switch Interface (sw0) Settings

Purpose: Configure Intranet Security settings on the switch interface (sw0) for Cloud Edge gateways with hardware switch chipset.

Location: Gateways > (Selected Gateway) > NETWORK > Interfaces > sw0

Procedure

1. Review the list of switch interface (sw0) settings.

   List of Switch Interface (sw0) Settings on page 6-59

2. Select the **Intranet Security mode**.

Option	Description
High Security	Characteristics include the following: • Internet: All security scanning (policy rules, profiles, flooding and port scan, etc.) • Intranet: All security scanning (as above), excluding mail scanning • Security protection: Offers the highest security protection for intranet traffic, but provides slowest performance
Balanced	Characteristics include the following: • Internet: All security scanning (policy rules, profiles, flooding and port scan, etc.) • Intranet: Part of security scanning (policy rules, flooding and port scan)

Option	Description
	• Security protection: Provides medium level security protection with medium level performance for intranet traffic
High Speed	Characteristics include the following: • Internet: All security scanning (policy rules, profiles, flooding and port scan, etc.) • Intranet: No security scanning • Security protection: Provides highest performance without any security protection for intranet traffic.

3. (**High Security** and **Balanced** mode only) Ensure that **Anomaly detection** is set to the desired setting.

Important

This is a read-only field that provides information about whether IPS protection is enabled. Anomaly detection is a feature of IPS. To use anomaly detection, you must enable IPS on the IPS page of the gateway profile that is applied to this gateway. Anomaly detection must be enabled before Cloud Edge can provide flood and port scan protection.

4. (**High Security** and **Balanced** mode only) Select the **Flood rules** that you want enabled, then modify the threshold value for each flood rule if you do not want to keep the default threshold.

   All flood rules are enabled by default to protect against flood attacks.

Option	Description
TCP SYN Flood	Default threshold: 8000
ICMP Flood	Default threshold: 8000
UDP Flood	Default threshold: 8000
IGMP Flood	Default threshold: 8000

5. (**High Security** and **Balanced** mode only) Select the **Port scan rules** that you want enabled, then modify the threshold value for each rule if you do not want to keep the default threshold.

   All port scan rules are enabled by default to protect against port scan attacks.

Option	Description
UDP Port Scan	Default threshold: 1000
TCP Port SYN Scan	Default threshold: 1000
TCP Port FIN Scan	Default threshold: 1000
TCP Port NULL Scan	Default threshold: 1000
TCP Port Xmas Scan	Default threshold: 1000

6. Click **Save**.

List of Switch Interface (sw0) Settings

Before you configure the switch interface (sw0), you should review what configuration settings are available. Some settings are configured using the Cloud Edge on-premises console and some are configured using Cloud Edge Cloud Console.

Cloud Edge Cloud Console is used to configure Intranet Security mode settings, which control the level of security provided for LAN to LAN intranet traffic.

For more information about security protection provided by each Intranet Security mode, see *Security Protections Provided by Each Intranet Security Mode on page 6-61*.

High Security and Balanced Modes

TABLE 6-2. Configured using Cloud Edge Cloud Console

SETTING	DESCRIPTION
Intranet Security mode	Sets the level of network security for the internal network. • High Security mode • Balanced mode • High Speed mode
Anomaly detection	A read-only field that displays whether IPS is enabled on the gateway profile applied to this gateway. IPS must be enabled to use flood rules and port scan rules.
Flood rules	Provides network IPS protection from flooding.
Port scan rules	Provides network IPS protection from port scanning.

TABLE 6-3. Configured using Cloud Edge on-premises console

SETTING	DESCRIPTION
Mode	DHCP or Static
MTU	Range: 576-1500 Default: 1438
Administrative access	Available only if gateway has not been registered.
Advanced Settings: **Enable Spanning Tree Protocol**	Prevents occurrence of loops on networks with redundant paths.
Advanced Settings: **IGMP Snooping**	Monitors IGMP traffic and then forwards IGMP traffic to only interested end points.

High Speed Mode

TABLE 6-4. Configured using Cloud Edge Cloud Console

SETTING	DESCRIPTION
Intranet Security mode	Sets the level of network security for the internal network. • High Security mode • Balanced mode • High Speed mode

TABLE 6-5. Configured using Cloud Edge on-premises console

SETTING	DESCRIPTION
Mode	DHCP or Static
MTU	Range: 576-1500 Default: 1438
Administrative access	Available only if gateway has not been registered.
Advanced Settings: **Enable Spanning Tree Protocol**	Prevents occurrence of loops on networks with redundant paths.

Security Protections Provided by Each Intranet Security Mode

Before you configure the switch interface (sw0), you can review what security protections are provided by each Intranet Security mode to ensure that you are configuring your gateway with the security protections that meet your business needs.

Matrix of Security Protections Provided by for Each Intranet Security Mode

	HIGH SECURITY		BALANCED		HIGH SPEED	
	Internet	Intranet	Internet	Intranet	Internet	Intranet
Anti-Malware	Yes	Yes	Yes	No	Yes	No

	High Security		Balanced		High Speed	
IPS	Yes	Yes	Yes	Limited to IPS listed in Flood Control and Port Scan Switch settings	Yes	No
Other security functions	Yes	Yes	Yes	No	Yes	No

Note

- Other security functions include all of the functions belonging to security profiles and the approved and blocked lists.
- Mail scan is not supported on intranet networks for any Intranet Security mode.

How VLANs Work

A Virtual Local Area Network (VLAN) is a group of endpoints, servers, and other network devices that communicate as if they are on the same LAN segment, regardless of their location. Endpoints and servers can belong to the same VLAN even though they are geographically scattered and connected to numerous network segments.

A VLAN segregates devices logically, not physically. Each VLAN is treated as a broadcast domain. Devices in VLAN 1 can connect with other devices in VLAN 1, but cannot connect with devices in other VLANs. Communication among devices on a VLAN is independent of the physical network.

A VLAN segregates devices by adding `802.1Q` VLAN tags to all packets sent and received by the devices in the VLAN. VLAN tags are 4-byte frame extensions that contain a VLAN identifier as well as other information.

How to Deploy Cloud Edge With VLANs

Review the following information to understand how Cloud Edge supports L3 VLANs.

- Only L3 VLANs are supported.

Note

L2 VLANs are not supported for any deployment mode or model.

- Cloud Edge supports 50 VLAN sub-interfaces with 4096 VLAN tags.
- Locations to configure VLANS:
  - Cloud Edge Cloud Console: All interfaces except **eth0** and **eth1** (if supported for that deployment mode and model)
  - On-premises console: **eth0** and **eth1** (if supported for that deployment mode)
- Considerations when editing or modifying VLANs:
  - VLAN mode can be either static or DHCP.
  - You cannot edit a VLAN if DHCP is enabled on that VLAN.
  - You cannot delete a VLAN if DHCP is enabled or NAT is used on that VLAN.
- You can add VLAN interfaces when creating policy rules and when creating interface group policy objects.
- For information specific to the deployment mode, see:
  - *Bridge Mode VLANs on page 6-63*
  - *Routing Mode VLANs on page 6-66*

Bridge Mode VLANs

Review the following information to understand how Cloud Edge supports VLANs in Bridge Mode.

Bridge Mode Supported Interfaces

- Cloud Edge 5.3 or later devices: Only the MGMT interface is supported for VLAN configuration
- Cloud Edge earlier than 5.3: All interfaces except **eth0** and **eth1** are supported for VLAN configuration
- Bridge interface (**br0** or **sw0**): Does not support VLAN configuration

Bridge Mode Considerations

There are special considerations when configuring VLANs in Bridge Mode.

- Cloud Edge does not natively support VLANs like a standard switch, which leads to the following limitations:
  1. You cannot configure access/trunk mode on a Cloud Edge port, so Cloud Edge cannot tag or untag any pass-through traffic.
  2. Cloud Edge cannot isolate broadcast or multicast traffic from different VLANs.
- Cloud Edge can only support pass-through VLAN traffic by keeping existing VLAN tags. Cloud Edge provides all security functions on pass-through VLAN traffic.

Bridge Mode Scenario

If Cloud Edge is deployed on a trunk link, Trend Micro recommends that you only use two Cloud Edge ports:

- Connect WAN to the upstream trunk port.
- Connect LAN1 to the downstream trunk port.

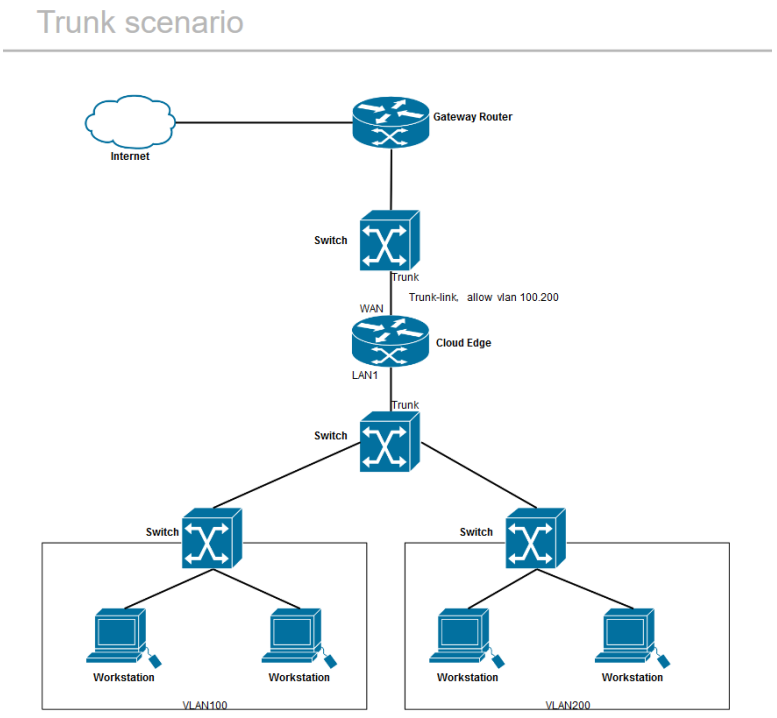
Important

Do not connect more than two ports on a trunk link.

Note

If you are deploying a gateway with hardware switch chipset or other model in software switch mode, connect the WAN port to the upstream trunk port and any LAN port to the downstream trunk port.

The following scenario depicts the recommended Bridge Mode deployment.



In this scenario, to register the Cloud Edge gateway with Cloud Edge Cloud Console, you must set up the gateway in a native VLAN.

- On a trunk link, all traffic is carried with VLAN tags except the traffic that belongs to the native VLAN. The Cloud Edge gateway itself can only send traffic without a VLAN tag.
- Therefore, if br0 is configured with DHCP, you must setup the DHCP server and gateway on a native VLAN. If br0 is configured with a static IP address, you must setup the gateway on a native VLAN.

Routing Mode VLANs

Review the following information to understand how Cloud Edge supports VLANs in Routing Mode.

Routing Mode Supported Interfaces

All interface except **eth0** and **eth1** are supported for VLAN configuration.

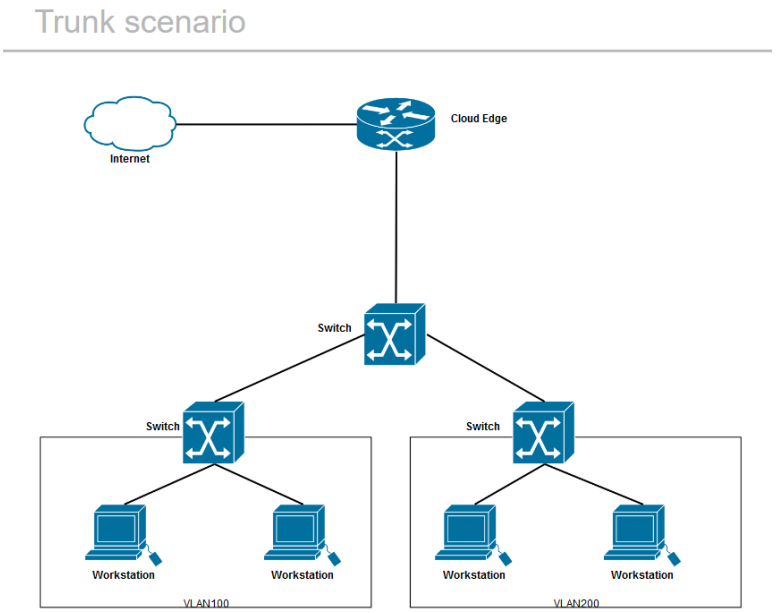
Routing Mode Considerations

There are no special considerations when configuring VLANs in Routing Mode.

Routing Mode Scenario

When a Cloud Edge gateway is in Routing Mode, you can configure VLAN interfaces on LAN interfaces to meet your needs.

The following scenario depicts a typical Routing Mode deployment.



Adding/Editing VLAN Interfaces

Purpose: Add an L3 VLAN interfaces to the Cloud Edge physical interface that receives VLAN-tagged packets. You must configure each L3 VLAN interface with a unique IPv4 address and netmask. You can edit VLAN interfaces if needed.

Location: Gateways > (Selected Gateway) > NETWORK > Interfaces

---

Procedure

1. Review the important information about how VLANs work with Cloud Edge gateways before adding a VLAN interface.

   How to Deploy Cloud Edge With VLANs on page 6-63

2. Perform the appropriate action:

   - To add a VLAN, click the VLAN add configuration icon (⊞)(➕) in the **Action** column.
   - To edit a VLAN, click the VLAN name in the **VLAN** section.

   The **Add/Edit VLAN** page opens.

   Note

   You cannot add VLAN interfaces to wireless interfaces.

3. Specify VLAN settings.

   - **Name**: Name the VLAN interface.
   - **Type**: L3 VLAN displays automatically and is read-only.

     L2 VLANs are not supported.
   - **Mode**: Select either **DHCP** or **Static**.

     For static, specify **IPv4 address** and **IPv4 netmask**.
   - **VLAN ID**: Specify the VLAN ID, which must match the VLAN ID of the packets received by this VLAN interface.

     Each VLAN interface VLAN ID must match the VLAN ID added by the IEEE 802.1Q-compliant router or switch connected to the VLAN interface. The VLAN ID can be any number between 1 and 4094 (0 and 4095 are reserved).

     You cannot change the VLAN ID of an existing VLAN interface.

4. Click **Save**.

Administrative Access

You can use Cloud Edge Cloud Console to configure a Cloud Edge gateway's management interface to allow or block specific types of management services (or traffic) that originates from IPv4 devices behind the gateway. The

Cloud Edge gateway supports administrative access from IPv4 clients using the On-Premises Console, Ping, SSH, and SNMP services.

If the Cloud Edge gateway is not registered with Cloud Edge Cloud Console, you can use the on-premises console to enable administrative access when editing an L3 interface. After the gateway is registered, you must use Cloud Edge Cloud Console to enable or disable administrative access to the gateway.

Once SNMP is enabled, you must configure SNMP settings using the Cloud Edge gateway's on-premises console by going to **Administration** > **Device Management** > **SNMP Settings**. After enabling and configuring SNMP support, users can obtain the supported objects information by using an SNMP manager.

For Cloud Edge gateways with wireless network functionality, you can enable administrative access on the main or guest wireless networks. You should be mindful of security concerns when allowing administrative access on the guest wireless network.

Enabling Administrative Access

Purpose: Enable remote administrative access to the gateway. Enabling SNMP allows users to obtain supported objects information from an SNMP manager.

Location: Gateways > (Selected Gateway) > NETWORK > Administrative Access

---

Procedure

1. Select the services to enable for the interface.
   - **On-Premises Console**
   - **Ping**
   - **SSH**
   - **SNMP**
2. In the field below the table, specify IPv4 addresses allowed to remotely access the gateway.

Note

This setting determines the IPv4 address ranges that can remotely access the gateway. Single IPv4 addresses are supported and the '-' symbol can be used as a range mark. Format the IPv4 address and netmask as `192.168.1.1/24`. If nothing is specified, all IPv4 addresses are allowed.

IPv6 addresses are not supported for administrative access.

3. Click **Save**.

DHCP

You can enable Dynamic Host Configuration Protocol (DHCP) services on one or more LAN interfaces on the Cloud Edge gateway. Each interface that has DHCP services enabled acts as a DHCP server that can assign IPv4 addresses and other network settings such as a default gateway and DNS settings to internal clients.

Cloud Edge automatically responds to DHCP requests directed to interfaces configured with DHCP services.

- When assigning DNS addresses to a client, you can configure DHCP to use the system DNS settings, the interface IPv4 address, or you can manually specify a list of DNS IPv4 addresses.
- You can configure the IPv4 address pool that the DHCP server can use to assign addresses to the DHCP clients.

  Cloud Edge supports multiple pools. You can create a separate DHCP pool for each interface.
- You can also configure DCHP advanced server settings (IPv4 address static mappings and DHCP lease times) for each DHCP server.

Viewing DHCP Services

Purpose: View and manage DHCP settings.

Location: Gateways > (Selected Gateway) > NETWORK > DHCP

Procedure

1. View parameters associated with any DHCP service.

Option	Description
Enable	The icon indicates the state of the service: enabled (green/on) or disabled (red/off).
Name	Name of the DHCP service (examples: LAN1, LAN2). Click an interface name to modify DHCP settings.
IPv4 Address/ Netmask	The IPv4 address and subnet mask assigned to the interface.
IP Pools	Range of applicable IPv4 addresses in the IP address pool for that DHCP service.
Options	The DNS server IPv4 address, the gateway IPv4 address, and the lease time. The DNS IPv4 address shows only when the DHCP server uses a specified DNS.

Editing DHCP Settings

Purpose: Modify the gateway DHCP settings.

Location: Gateways > (Selected Gateway) > NETWORK > DHCP > Add/Edit

Procedure

1. Review the following information as needed:
   - *Deployment Mode Information for DHCP on page 6-73*

     Information about which interfaces you can configure as DHCP servers for each deployment mode.
   - *Default DHCP IP Address Pools on page 6-74*

     What IP addresses are assigned by default to each IP address pool.
2. Configure DHCP settings.

Option	Description
Enable DHCP	Select to enable the service.
IP address / Netmask	The IPv4 address and subnet mask assigned to the interface.
Preferred DNS	Select the preferred DNS method. • Select **Use system DNS settings** to use the gateway system DNS configured at **Network** > **DNS**. • Select **Use the interface IP address** to use the interface IPv4 address as the DNS. • Select **Use specified DNS servers** to manually configure IPv4 addresses as the DNS settings.
Gateway	The DHCP server gateway automatically populates based on interface IPv4 address and netmask settings. Optionally change the IPv4 gateway address.
IP address range from and to	Specify the range of IPv4 addresses to create the IP address pool to which the DHCP configuration applies.

3. Configure **Advanced Settings**.

   - For **Lease time**, adjust the time and date when the leased IPv4 address and netmask are no longer valid.

     Specify days, hours, or minutes. For example, if you specify only hours, then the lease is restricted to that number of hours.

   - You can use static mapping to manually bind a static IPv4 address to a specific MAC address.

     For **Static mapping**, specify MAC address / IPv4 address maps. You can enter multiple maps as a comma-delimited list. Example:

     `00-FF-8A-B9-5A-49 / 192.168.1.1, 00:0C: 29:A9:69:25 / 192.168.2.1.`

4. Click **Save**.

Deployment Mode Information for DHCP

You should understand on which interfaces you can configure DHCP services for each deployment mode.

- Bridge Mode: The MGMT interface is the only interface that can be configured as a DHCP server.

  Software Switch: By default all interfaces except the MGMT interface are L2 interfaces that are part of the software switch. The WAN, LAN1, and LAN2 interfaces must be included in the switch configuration.

  You can, if desired, remove LAN3 from the switch configuration. After you remove the LAN3 interface from the software switch configuration, you can change it to an L3 interface, assign it an IPv4 address, and then enable DHCP services on the interface.

- Routing Mode: All L3 interfaces that are enabled can be configured as DHCP servers.

Deployment Mode Information for Gateways with Hardware Switch Chipset

- Bridge Mode: The MGMT interface in the only interface that can be configured as a DHCP server.

  All interfaces except the MGMT interface are L2 interfaces and are part of the switch configuration. They cannot be removed from the switch configuration and cannot be configured as DHCP servers.

- Routing Mode: All L3 interfaces that are enabled can be configured as DHCP servers.

Deployment Mode Information for Gateways with Wireless Network Functionality

- Bridge Mode: Only the MGMT interface can be configured as a DHCP server.
- Routing Mode: All L3 interfaces can be configured as DHCP servers including the main and guest wireless network interfaces.

DHCP services are enabled by default on a wireless network interface. By default, when you enable a wireless network, DHCP services will be enabled on the interface.

However, if DHCP services on a wireless interface is disabled before enabling the wireless network and the wireless network is later enabled, the DHCP services will not be enabled when you enable the wireless network. In this case, you must manually enable the DHCP service on that wireless interface.

Default DHCP IP Address Pools

Cloud Edge assigns certain L3 interfaces a default DHCP IP address pool.

Default DHCP IP Address Pools

Interface	Interface Name	IP Address Pool
eth0	WAN	N/A
eth1	LAN1	192.168.100.1/24
eth2	LAN2	192.168.101.1/24
eth3	LAN3	192.168.102.1/24
eth4	MGMT	192.168.103.1/24

Default DHCP IP Address Pools for Gateways with Hardware Switch Chipset

Interface	Interface Name	IP Address Pool
eth0	WAN	N/A
eth1	LAN1	192.168.100.1/24
eth2	LAN2	192.168.101.1/24
eth3	LAN3	192.168.102.1/24
eth4	LAN4	192.168.103.1/24
eth5	LAN5	192.168.104.1/24

Interface	Interface Name	IP Address Pool
eth6	LAN6	192.168.105.1/24
eth7	LAN7	192.168.106.1/24
eth8	LAN8	192.168.107.1/24
eth9	MGMT	N/A

Default DHCP IP Address Pools for Gateways with Wireless Network Functionality

Wireless Interface	Interface Name	IP Address Pool
wlan0	<WIRELESS_SSID>	192.168.201.1/24
wlan1	<GUEST_WIRELESS_SSID>	172.16.20.1/24

Dynamic DNS

A Dynamic Domain Name System (DDNS) automatically updates Internet DNS name servers in real-time to keep the active DNS configuration of host names, addresses, and other information up to date. DDNS is typically used when businesses have frequent changes to the public host-name-to-IP-address mappings, usually when companies use PPPoE or DHCP to obtain Internet access.

Dynamic IP addresses present a problem if the customer wants to provide a service to other users on the Internet, such as a web service. As the IP address may change frequently, corresponding domain names must be quickly re-mapped in the DNS, to maintain accessibility using a well-known URL. Many providers offer commercial or free DDNS service for this scenario. The automatic reconfiguration is generally implemented in the user's router or computer, which runs software to update the DDNS service. The communication between the user's equipment and the provider is not standardized, although a few standard web-based methods of updating have emerged over time (RFC 2136 or other protocols).

Using DDNS automates the propagation of new host-name-to-IP-address mapping across the Internet. DDNS service providers act as a broker to manage this process. The Cloud Edge gateway is designed as the first Internet-facing device an external client connects to when trying to reach the business, it needs to make sure that all Internet users route their traffic to it for each host name / domain that they are trying to reach on the business side. With the DDNS client, Cloud Edge can communicate host-name-to-IP-address changes to the DDNS service provider.

Supported DDNS Service Providers

The three supported DDNS service providers are:

Provider	User Scope
Dyn DNS	Global
Free DNS	
DNSPod	China

Note

IPv6 is not supported.

Configuring Dynamic DNS Settings

Purpose: Configure basic settings according to the service vendor. The information needed varies between different services. Basically, each service requires the domain name, account, and password information.

Location: Gateways > (Selected Gateway) > NETWORK > Dynamic DNS

Procedure

1. **Enable Dynamic DNS** by selecting **On**.
2. Select a **Vendor**.

   Available vendors are DynDNS, FreeDNS, and DNSPod.

If a version earlier than Cloud Edge 5.5 is installed on the gateway, the **DNSPod** option will not be available in the **Vendor** drop-down box.

3. Perform the appropriate action:
   - For DynDNS or FreeDNS, enter the **User name** and **Password**.
   - For DNSPod, enter the **User id** and **User token**.
4. Enter the domain information:
   - For DynDNS or FreeDNS, enter the FQDN in **Domain**.
   - For DNSPod, enter the host name in **Host record** and the domain name in **Domain**.
5. Select the WAN interface:

Auto:	(Default) Cloud Edge auto-discovers an interface with a non-private IP address according to RFC 1597.
(Interface Name):	Select the WAN interface from the list of available interfaces (for example, WAN or LAN1).

6. If **DynDNS** was selected in **Vendor**, optionally enable HTTPS.

   DynDNS provides HTTPS connections as an option. Other vendors (such as FreeDNS) do not expose the HTTPS interface, while DNSPod requires mandatory HTTPS connections.
7. Click **Save**.

Viewing DDNS Status

Purpose: View the current DDNS running status.

Location: Gateways > (Selected Gateway) > NETWORK > Dynamic DNS > Status

---

Procedure

1. View the DDNS status messages.

See *DDNS Status Messages on page 6-78*.

DDNS Status Messages

The **Dynamic DNS** > **Status** tab shows the current DDNS running status, including current interface (auto-discovered or specified), WAN IP address, and status message.

Possible status messages include:

- SUCCESS
- ERROR: Authentication failed
- ERROR: Account hasn't been activated
- ERROR: Invalid or unregistered domain info
- ERROR: Internet access unavailable or can't connect to service vendor
- ERROR: Used some paying user only features, such as HTTPS connection service, related settings has been reset
- ERROR: Service unavailable Message from Service Vendor
- ERROR: No Available WAN IP detected
- ERROR: No suitable IP on specified interface
- ERROR: Service Interface may have changed, please contact Trend Micro for updating
- ERROR: Too many authentication failures, the account was banned temporarily
- ERROR: Invalid or unregistered sub domain info
- ERROR: Update host in a round robin way is not allowed.
- ERROR: Unknown error, please check your internet access.
- Not Enabled

Routing Table

In the factory default configuration, the Cloud Edge routing table contains a single static IPv4 default route. Add routing information to the routing table by defining additional IPv4 static routes. The table may include several different routes to the same destination—the IPv4 addresses of the next-hop router specified in those routes or the Cloud Edge interfaces associated with those routes may vary.

Cloud Edge evaluates the information in the routing table and selects the best route to a destination, typically the shortest distance between the Cloud Edge gateway and the closest next-hop router. In some cases, a longer route is selected if the best route is unavailable. Cloud Edge installs the best available routes in the unit's forwarding table, which is a subset of the unit's routing table. Packets are forwarded according to the information in the forwarding table.

Note

Cloud Edge does not support IPv6 routing.

Viewing the Routing Table

Purpose: View the routing table to learn how IPv4 network traffic from different sources routes to a destination—the IPv4 addresses of the next-hop router specified in those routes or the Cloud Edge interfaces associated with those routes may vary.

Location: Gateways > (Selected Gateway) > NETWORK > Routing Table

Procedure

1. View table indicators.

   See *Routing Table Indicators on page 6-79*.

Routing Table Indicators

The following table explains routing table indicators.

Code	Definition
K	Kernel route
C	Connected
S	Static

Static Routes

Static routes control how traffic moves between endpoints connected to the network. Defining an IPv4 static route provides Cloud Edge with the information to forward a packet to a particular destination. Configure IPv4 static routes by defining the destination IPv4 address and netmask of packets that the Cloud Edge gateway is intended to intercept, and by specifying a gateway IPv4 address for those packets. The gateway address specifies the next-hop router to which traffic will be routed.

You can specify through which interface packets leave and to which device to route packets. The Static Route list at **Gateways** > **(gateway name)** > **NETWORK** > **Static Routes** displays information that the Cloud Edge gateway compares to packet headers in order to route packets.

Adding a Static Route

When new IPv4 static routes are added, Cloud Edge checks whether a matching route and destination already exist in the Cloud Edge routing table. If no match is found, Cloud Edge adds the route to the routing table.

Note

Since Routing Mode does not support IPv6, you can configure only IPv4 static routes.

Procedure

1. Go to **Gateways** > **(gateway name)** > **NETWORK** > **Static Routes**.
2. Click **Add** to add a default route.

   The **Add/Edit Static Route** window appears.

3. Select **Enable static route**.
4. In **Destination network**, specify the network address.

   Any of the following options are valid:

   - **IP address**
   - **Default gateway** (Example: `10.10.10.10/16`)

     Note

     If multiple default gateways are configured, outgoing traffic is routed from these gateways using round-robin selection.

   - **Bitmask**

     Note

     The bitmask is the decimal equivalent of the netmask.

   - **Class InterDomain Routing (CIDR) notation** (Example: `255.255.255.0/24`)
5. In **Nexthop**, specify the next-hop IPv4 address.
6. Click **Save**.

Enabling/Disabling Static Routes

Procedure

1. Go to **Gateways** > **(gateway name)** > **NETWORK** > **Static Routes**.
2. In the list of static routes, do one of the following:
   - Select the **Enable** icon () to enable the static route.
   - Deselect the **Enable** icon () to disable the static route.

Modifying a Static Route

Procedure

1. Go to **Gateways** > **(gateway name)** > **NETWORK** > **Static Routes**.
2. Do one of the following:
   - In the **Route ID** column, click the route name.
   - In the **Action** column, click the edit icon ().

   The **Add/Edit Static Route** screen appears.
3. Use the check box to enable or disable the static route.
4. View the network IP address/bitmask. This field is read-only.
5. Specify the next hop parameters.
6. Click **Apply**.

Deleting a Static Route

Procedure

1. Go to **Gateways** > **(gateway name)** > **NETWORK** > **Static Routes**.
2. In the **Action** column, click the delete icon ().
3. Click **Delete** to verify the deletion.

Network Address Translation (NAT)

Use Network Address Translation (NAT) policies to specify whether source or destination IP addresses and ports are converted between public and private addresses and ports on Layer 3 interfaces. For example, private source addresses can be translated to public addresses on traffic sent from an internal (trusted) zone to a public (untrusted) zone.

The following NAT policy rule translates a range of private source addresses (`10.0.0.1` to `10.0.0.100`) to a single public IP address (`200.10.2.100`) and a unique source port number (dynamic source translation). The rule applies only to traffic received on a Layer 3 interface in the internal (trusted) zone that is destined for an interface in the public (untrusted) zone. Because the private addresses are hidden, network sessions initiate from the public network. If the public address is not a Cloud Edge interface address (or on the same subnet), the local router requires a static route to direct return traffic to Cloud Edge.

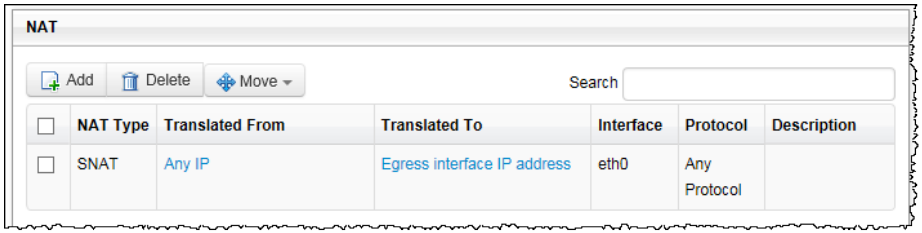


FIGURE 6-3. Simple NAT Rule

NAT Rules

NAT address translation rules are based on the source and destination IPv4 addresses and ports. Similar to security policies, NAT policy rules are compared against the incoming traffic in sequence, and the first rule matching the traffic is applied.

You can apply NAT rules to all physical interfaces except the MGMT interface.

For Cloud Edge gateways with wireless network functionality, you can configure NAT rules on a wireless network interface provided that the wireless network (main or guest) is enabled.

As needed, add static routes to the local router so that traffic to all public IPv4 addresses is routed to Cloud Edge. You can also add static routes to the receiving interface on Cloud Edge to route traffic back to the private IPv4 address.

Consideration when both client and server access a gateway from the same LAN interface

When a client and server access the Cloud Edge gateway from the same LAN interface, the client cannot access this server by domain name. You can support this scenario by adding both a source NAT rule and a destination NAT rule to this LAN interface. See *Adding NAT Rules to Support Hairpin NAT on page 6-88*.

Adding a Destination NAT Rule

Destination NAT (DNAT) changes the destination address in the IP header of a packet. The primary purpose of this is to redirect incoming packets with a destination of a public address/port to a private IP address/port inside the network.

Procedure

1. Go to **Gateways** > **(Selected Gateway)** > **NETWORK** > **NAT** > **Add**.
2. Select **Destination** for **NAT type**.
3. Configure the NAT settings:

Option	Description
Ingress interface	Select **ANY** or any L3 interface from the drop-down list to act as the interface for network traffic that originates from outside of the network's routers and proceeds toward a destination inside of the network. For Cloud Edge gateways with wireless network functionality, you can select a wireless network interface as the ingress interface provided that wireless network (main or guest) is enabled.
Destination IP translation	Select from the following options: • **Ingress interface IP address** and then specify **Translated IP address/range**. The ingress interface is used for the external IP address and the specified translation IP address/range is used for translating (mapping) the ingress interface IP address to an internal IP address. • **Virtual IP** and then specify **External IP address/range** and **Translated IP address/range**.

Option	Description
	You must explicitly specify an external IP address/range to use for NAT mapping. The translated IP address range is automatically generated according to the beginning IP address. The mapping is one-to-one of external IP addresses to translated IP addresses.
Description	Specify an identifying characteristic about the use or configuration for the NAT rule.
Port forwarding	**Port forwarding**: Select **On** for static one-to-one NAT mapping with port forwarding. When **On**, an external IP address is always translated to the same mapped IP address, and an external port number is always translated to the same mapped port number. If set to **On**, specify the following: • **Protocol**: Select **TCP** or **UDP**. • **External service port**: Specify a port range. **Map to port**: Specify a port. When you specify the **External service port** range, the **Map to port** is generated automatically according to the beginning port. The mapping is one-to-one.
Set matching condition	You can specify more detailed information or matching conditions, including: • **Source IP address range** • **Source port range**

4. Click **Save**.
5. Verify that the new rule is added to the list of NAT rules.

Modifying NAT Rules

Procedure

1. Go to **Gateways** > **(Selected Gateway)** > **NETWORK** > **NAT**.
2. In the **Translated From** column, click the NAT rule to change.
3. Edit the parameters as needed.
4. Click **Save**.

Changing NAT Rule Priorities

Procedure

1. Go to **Gateways** > **(Selected Gateway)** > **NETWORK** > **NAT**.
2. Select the check box of the NAT rule priority you want to change.
3. To rearrange the order, select **Move** and use the operators (Up, Down, Top, Bottom) above the NAT rules list.

Adding a Source NAT Rule

Source NAT (SNAT) changes the source address in the IP header of a packet. The primary purpose is to change the private (RFC 1918) address/port into a public address/port for packets leaving the network. Cloud Edge automatically creates a default source NAT rule. You can create additional source NAT rules or modify the default source NAT rule. To modify the default source NAT rule, see *Modifying NAT Rules on page 6-86*.

Procedure

1. Go to **Gateways** > **(Selected Gateway)** > **NETWORK** > **NAT** > **Add**.
2. Select **Source** for **NAT type**.
3. Configure the NAT settings:

Option	Description
Egress interface	Select **ANY** or any L3 interface (for example, WAN) from the drop-down box list to act as an interface for egress traffic, which is traffic that originates from inside the network. For Cloud Edge gateways with wireless network functionality, you can select a wireless network interface as the egress interface provided that wireless network (main or guest) is enabled.
Source IP translation / **Translate to**	Select one of the following methods for source IP translation: • **Egress interface IP address** If this method is selected, the **Translate to** option is not available. The egress interface's IP address is used for translation. • **Single IP address** and then specify an IP address for **Translate to** The specified IP address is used for translation. • **IP address range** and then specify an IP address range for **Translate to** The specified IP address range is used for translation. • **Subnet** and then specify a subnet for **Translate to** The subnet is used for translation. **Note** If you select **Single IP address**, **IP address range**, or **Subnet**, you must explicitly specify an L3 interface for the **Egress interface** option.
Description	Specify an identifying characteristic about use or configuration for the NAT rule.
Set matching condition	You can expand the **Set matching condition** section to specify more detailed information or matching conditions, including: • **Protocol**—Any, TCP, UDP, or ICMP. Any means all protocols. • **Source IP address range**—Specified by the network. • **Source port range**—Specified by administrator. • **Destination IP address range**—Specified by administrator. • **Destination port range**—Specified by administrator.

Option	Description
	Note If you specify **ICMP** for **Protocol**, the **Source port range** and **Destination port range** options are not available.

4. Click **Save**.
5. Verify that the new rule is added to the list of NAT rules.

Deleting NAT Rules

Procedure

1. Go to **Gateways** > **(Selected Gateway)** > **NETWORK** > **NAT**.
2. Select the row of the NAT rule to delete.
3. Click **Delete**.

   The **Delete** confirmation message appears.
4. To confirm, click **Delete**.
5. Verify that the NAT rule is no longer in the list of NAT rules.

Adding NAT Rules to Support Hairpin NAT

When a client and server access the Cloud Edge gateway from the same LAN interface, the client cannot access this server by domain name. To support this scenario, add both a source NAT rule and a destination NAT rule to this LAN interface. Use the following procedure to perform this configuration.

Procedure

1. Go to **Gateways** > **(Selected Gateway)** > **NETWORK** > **NAT** > **Add**.
2. Select **Source** for **NAT type**.
3. Configure the client and server linked LAN interface for **Egress interface**.

4. Select **Egress interface IP address** for **Source IP translation**.
5. Click **Save**.
6. Go to **Gateways** > **(Selected Gateway)** > **NETWORK** > **NAT** > **Add**.
7. Select **Destination** for **NAT type**.
8. Configure the client and server linked LAN interface for **Ingress interface**.
9. Select **Virtual IP** for **Destination IP translation**.
10. Configure **External IP address/range** with the server Internet IP address registered to DNS server.
11. Configure **Translated IP address/range** with the server's local IP address.
12. Click **Save**.
13. Verify that the new rules are added to the list of NAT rules.

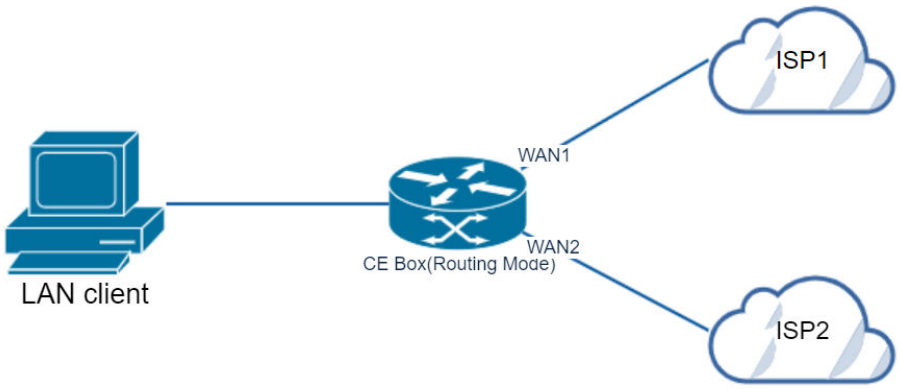
SD-WAN

Software-Defined Wide Area Networks (SD-WAN) is a software approach managing Wide-Area Networks, which offers ease of deployment, central manageability and reduced costs, and it can improve connectivity to the Internet and the cloud.

A key application of SD-WAN is to allow companies to build higher-performance WANs using lower-cost and commercially available Internet access, enabling businesses to partially or wholly replace more expensive private WAN connection technologies such as MPLS.

In order to fully utilize SD-WAN function, users need to make changes to their network topology and perform configuration in CE On-Premises UI.

Cloud Edge WAN supports three modes: PPPoE, DHCP, and Static. If you want to enable SD-WAN, you need to have two WAN links (WAN1 and WAN2/LAN1) ready. See the diagram below:



Note

- If your WAN interface uses a static IP, ensure the gateways for WAN1 and WAN2 are correctly configured in the On-Premises Console. If you leave your gateway for CE box unconfigured (empty), when SD-WAN settings are deployed, the deployment will fail.

Cloud Edge has three types of routing strategies:

- Static Routing
- SD-WAN Routing
- Policy Routing

After deploying SD-WAN, the priority of the routing strategy should be:

Static Routing > SD-WAN Routing > Policy Routing

Enabling SD-WAN and Bandwidth Settings

Purpose: Enable SD-WAN function and view SD-WAN overview configuration and interface usage.

Location: Gateways > (Selected Gateway) > SD-WAN > Home

Procedure

1. Click the **On** button beside **Enable SD-WAN**.
2. Under SD-WAN Uplinks, the WAN1 and WAN2 fields are read-only, and they can only be edited on Cloud Edge On-Premises Console. For how to manage network interface settings for selected gateways, refer to *Editing Network Interfaces on page 6-51*.
3. Under Bandwidth Settings, select **WAN1** (default) from the dropdown. Configure the upstream bandwidth and downstream bandwidth and specify the limits. Also configure the Mbps and Kbps limits using the dropdown.

   Note

   Step 3 is optional.

4. Click **Save**.

Overview Widgets

After SD-WAN is enabled, you can see the volume and bandwidth data on the SD-WAN Home page. It will also show how many SD-WAN rules and Health Check SLAs you have configured.

There are two types of overview widgets shown on the bottom of the SD-WAN Home page. They are Configuration Overview and Bandwidth and Volume Usage.

- Configuration Overview: Displays the number of SD-WAN rules added and the number of Health Check SLAs created.
- Bandwidth and Volume Usage: The Bandwidth tab shows the upstream and downstream for the WAN interfaces (WAN1 and WAN2). The Volume tab shows the sent and received volume for the WAN interfaces (WAN1 and WAN2).

Note

To quickly get to the SD-WAN rules and Health Check SLAs, under Configuration Overview, click the numbers (above SD-WAN Rules or Health Check SLAs) that link to the Rules page or SLAs page.

SD-WAN Rules

An SD-WAN rule is used to route the desired traffic and dynamically forward the traffic to the best link with the help of SLA. There are three modes for SD-WAN rules:

- Best Quality: Selects the best link in the network performance parameters you desire.
- Maximized Bandwidth: Selects the link to fully utilize the Internet bandwidth.
- Preferred Link: Selects a higher priority link to forward traffic to.

Cloud Edge uses the DPI engine to detect traffic and cache the identity to implement application-aware routing.

Use SD-WAN rules to do dynamic path selection for WAN traffic between SD-WAN member interfaces.

SD-WAN rules have the following features and characteristics:

- The default SD-WAN rule can do load balance by source IP, source-destination IP, sessions or volume. No SLA can be configured in the default rule.
- For the default SD-WAN rule, the weights of Session and Volume are in percentage. The sum of weights must be 100%.
- You can define a maximum of 200 SD-WAN rules (including one default rule).

Do the following at **Gateways** > **(Selected Gateway)** > **SD-WAN** > **Rules**:

- View the list of existing rules

- Add, edit, duplicate, and delete rules
- Move rule priority
- Enable and disable rules
- Search

Note

Deploy SD-WAN settings by clicking the **Deploy All** button (all configurations are deployed at the same time, no separate deployment for SD-WAN settings.)

Note

You cannot disable, delete, move, or duplicate the default SD-WAN rule.

There are 3 kinds of events that will trigger SD-WAN rules to reroute the traffic:

- Interface down: The physical condition of this interface is down. For example, the cable is unplugged, the interface has hardware problems, or the directed interface connection is disrupted.
- SLA down: The traffic from the Cloud Edge gateway to monitor server fails to receive response exceeding the value of Failure Threshold that the user has configured.
- Failure to meet SLA: The SLA performance detection data exceeds the threshold that the user has configured.

For all the Best Quality strategies, as the strategy itself already specifies the performance metrics, the SLA parameter of the selected Health Check SLA will not take effect.

For the Maximized Bandwidth and Preferred Link strategies, if one of the two WAN links fails to meet an SLA parameter, it will reroute the traffic to an alternative link.

The other 2 events will take effect on rerouting the traffic on all kinds of strategies.

Also, for all 3 kinds of events mentioned above, the priority goes in the order listed below:

1. Interface down (highest)
2. SLA down (medium)
3. Failure to meet SLA (lowest)

Managing SD-WAN Rules

Purpose: Manage SD-WAN rules to control traffic that passes through registered gateways.

Location: Gateways > (Selected Gateway) > SD-WAN > Rules

Procedure

1. Do the following:

- View information about existing SD-WAN rules.
- Click the expansion arrow located to the left of the rule name to view more details about the SD-WAN configuration for that rule.
- Click **Add** to create a new rule.

Note

The default SD-WAN rule is added automatically when SD-WAN is enabled for the first time.

- Use **Search** at the top right to locate a rule.
- Click a rule's name to view or modify settings.
- Select a rule and then click **Edit** to view or modify settings.
- Select a rule and then click **Move** to change the rule priority.
- Select a rule and then click **More** to change the status or duplicate the rule.

- Select a rule and then click **Delete** to remove the rule.

Adding/Editing SD-WAN Rules

Purpose: Add or edit SD-WAN rules by specifying the users or user groups, IP addresses or FQDNs.

Location: Gateways > **(Selected Gateway)** > **SD-WAN** > **Rules** > **Add/Edit**

Procedure

1. On the **Add/Edit SD-WAN Rule** > **Rule Name** page:
   a. Specify the **Rule Name** (between 1 and 32 characters, consisting of letters, numbers, or underscores).
   b. Specify **Description** (optional).
   c. Click **Next**.

   Note
   You can click a SD-WAN rule name to edit it.

2. On the **Add/Edit SD-WAN Rule** > **Source** page, configure **Source**.
   a. Select **Any** if you want to apply this SD-WAN rule to any user groups or IP.
   b. Select **Selected Users/User Groups** if you want to apply this SD-WAN rule to specific users or user groups. Then in the **Select from** box, select the users or user groups and move it to the **Selected** box.
   c. Select **Selected IP Addresses/FQDNs** if you want to apply this SD-WAN rule to specific IP addresses and FQDNs. Then in the **Select from** box, select the IP address or FQDN and move it to the **Selected** box. Click **Add New IP Addresses/FQDNs Object** to add new IP address or FQDN object (see *Adding/Editing IP Address/FQDN Objects on page 6-168*). Use the Search box to search for any selected users/ user groups/IP addresses/FQDNs.

d. Click **Next**.

3. On the **Add/Edit SD-WAN Rule** > **Destination** page, configure **Destination**.

   a. Under **Addresses**, select **Any** if you want to apply this SD-WAN rule to any IP address or FQDN. Select **Selected IP Addresses/FQDNs** if you want to apply this SD-WAN rule to specific IP addresses and FQDNs.

   b. Under **Services and Applications**, select **Any** if you want to apply this SD-WAN rule to any services or applications. Select **Selected Services** if you want to apply this SD-WAN rule to specific services. Click **Add New Service Object** to add new service objects. Select **Selected Applications** if you want to apply this SD-WAN rule to specific applications. Click **Add New Application Group** to add a new application group.

   c. Click **Next**.

4. On the **Add/Edit SD-WAN Rule** > **Strategy** page, configure **Strategy**.

   a. Select **Best Quality – Latency** if you want to use the link whose latency is low.

   b. Select **Advanced** if you want to prioritize traffic based on the following 3 options:

   - Maximized Bandwidth: Use **Maximized Bandwidth** so that traffic is distributed among all available links.
   - Best Quality: Use **Best Quality** to select the quality criteria from the dropdown (Jitter, Packet Loss, or Bandwidth). Or click **Custom Profile** in the dropdown to make percentage allocation for Latency, Jitter, Packet Loss, and Bandwidth.
   - Preferred Link: Use **Preferred Link** when traffic is sent to the physical link you select from the Select Link dropdown unless when the link does not meet SLA. Select **WAN1** or **WAN2** from the **Select Link** dropdown.

   c. Click **Next**.

5. On the **Add/Edit SD-WAN Rule** > **Health Check SLA** page, select a user-defined Heath Check SLA or create a new Health Check SLA. (see *SLAs on page 6-100*) You can optionally click **Add New Health Check SLA** to add a new Health Check SLA.

   a. On the **Add/Edit Health Check SLA** > **General** page, specify the **SLA Name**, **Description**, **Monitor Server**, and **Type** of protocol. Click **Add Server** to add a second server. (Note: A second server can be added and it can also be removed if not needed.) Then click **Next**.

   b. On the **Add/Edit Health Check SLA** > **SLA Parameters** page, choose SLA parameters from the **recommended SLAs** or enter custom parameter(s) for **Latency**, **Jitter**, and **Packet Loss**. [Note: Cloud Edge Cloud Console (CECC) provides 4 pre-defined SLAs (VoIP-Video, Audio-Streaming, General Web, and Office 365)] (see the Recommended SLA Type and Description table). Then click **Next**.

   c. On the **Add/Edit Health Check SLA** > **Link Check Status** page, configure the thresholds and interval for link check status. Then click **Next**.

   d. On the **Add/Edit Health Check SLA** > **Action When Inactive** page, disable static routes when SLA parameters cannot be met by selecting **Update Static Route**. (Note: If enabled when a link is inactive, the routes on that link are removed, and traffic is routed through the other link. When the link is active again, the routes are re-enabled.) Then click **Save**. (Note: After you click Save, it takes you back to the **Add/Edit SD-WAN Rule** > **Health Check SLAs** page.) Then click **Next**.

6. On the **Add/Edit SD-WAN Rule** > **Review** page, review the SD-WAN rule details and then click **Save**. After clicking Save, it takes you back to the Rules page.

Editing the Default SD-WAN Rule

Purpose: To change load balance mode or adjust interface weight.

Location: Gateways > (Selected Gateway) > SD-WAN > Rules > Edit Default SD-WAN Rule

When SD-WAN is enabled and saved, a default SD-WAN rule is created. The default SD-WAN rule can do load balance by source IP and destination IP, sessions or volume. No SLA can be configured in default rule. For default SD-WAN rule, weights of Session and Volume are in percentage. The sum of weights must be 100%.

The default SD-WAN rule is created when SD-WAN is enabled for the first time. It appears on the **Gateways** > **(Selected Gateway)** > **SD-WAN** > **Rules** page.

Procedure

1. Under **Load Balance Mode**, select a mode used to do load balance traffic between WAN1 and WAN2 links.
   a. Select **Source IP** if you want to do traffic load balance based on source IP.
   b. Select **Source IP and Destination IP** if you want to do traffic load balance based on combination of source IP and destination IP.
   c. Select **Session** if you want to do load balance according to the session number's ratio. Configure the weight using percentage (the sum of the weights must be 100%).
   d. Select **Volume** if you want to do load balance according to the bandwidth ratio. Configure the weight using percentage for the volume (the sum of the weights must be 100%).
2. Click **Save**.

Duplicating SD-WAN Rules

Purpose: Duplicate an SD-WAN rule. The new rule has the highest priority.

Location: Gateways > (Selected Gateway) > SD-WAN > Rules

Note

You cannot duplicate the default SD-WAN rule.

Procedure

1. Select the checkbox next to the SD-WAN rule to duplicate and click the **More** pull-down menu.
2. Click **Duplicate**.
3. Verify that a new SD-WAN rule (with a duplicated number) appears in the list at **SD-WAN** > **Rules**.

Moving SD-WAN Rules

Purpose: Move and change the priority of a user-defined SD-WAN rule.

Location: Gateways > (Selected Gateway) > SD-WAN > Rules

Note

You cannot move a default SD-WAN rule.

Procedure

1. Select the checkbox next to the SD-WAN rule to move and change the priority.
2. Click the **Move** pull-down menu and select **Up**, **Down**, **Top**, or **Bottom**.

Enabling/Disabling SD-WAN Rules

Purpose: Enable a user-defined SD-WAN rule or disable it after it is enabled.

Location: Gateways > (Selected Gateway) > SD-WAN > Rules

Note

You cannot enable or disable the default SD-WAN rule.

Procedure

1. Select the checkbox next to the SD-WAN rule to enable or disable.
2. Click the **More** pull-down menu and select **Enable**, or **Disable**.

Deleting SD-WAN Rules

Purpose: Delete a user-defined SD-WAN rule.

Location: Gateways > (Selected Gateway) > SD-WAN > Rules

Procedure

1. Select the checkbox next to the SD-WAN rule to delete.
2. Click **Delete**.
3. Verify the deleted SD-WAN rule is not in the list at **SD-WAN** > **Rules**.

SLAs

A Service-Level Agreement (SLA) is a contract between a service provider and its customers.

The monitoring of SLA links measures the health of links that are connected to SD-WAN member interfaces by sending probing packets through each WAN interface to a server and by measuring the link quality based on latency, jitter, and packet loss. If a link is broken, the SLA will detect this event and notify the Cloud Edge gateway to reroute traffic to an alternative link. When the link is working again, the Cloud Edge gateway will recover the link and route the traffic on the available links again. This prevents the traffic from being sent to a broken link and thus causing a traffic break.

Cloud Edge recommends four types of SLAs:

- VoIP-Video
- Audio-Streaming
- General Web

- Office 365

Note

On the bottom of the Manage SLAs page, there are four recommended SLAs. The example descriptions will be displayed when you mouse over them.

The maximum number of SLAs supported by Cloud Edge is 50.

Managing SLAs

Purpose: Manage SLAs to measure the health of links connected to SD-WAN member interfaces.

Location: Gateways > (Selected Gateway) > SD-WAN > SLAs

Procedure

1. Do the following:
   - Select an SLA and view information about it by clicking the **Latency**, **Jitter**, or **Packet Loss** buttons.
   - Use **Search** at the top right of the lower pane to search for an SLA.
   - Click **Add** to create a new SLA.
   - Select an SLA and then click **Edit** to modify the SLA settings or click an SLA name to edit the SLA.
   - Select an SLA and then click **Delete** to remove the SLA.

   On the SLA configuration page, Cloud Edge Cloud Console provides a step-by-step UI for the user to configure SLAs. Pay attention to the following when you configure SLAs.
   - Configure the SLA name and Monitor Server. The server can be either FQDN or IP address.
   - You can configure a maximum of two monitor servers.

Note

If you configure two monitor servers, the first server will have a higher priority. On Cloud Edge Cloud Console, by default, the displayed SLA data is data of the first server. If the first server is down, it will check if the second server is reachable. If yes, it will use the SLA data of the second server. If both servers are unreachable, it means the SLA is down.

- The detection types to be configured include PING and HTTP.

Note

Some servers ban PING or HTTP, so when you configure a monitor server, confirm that the monitor server allows PING or HTTP.

Adding/Editing Health Check SLAs

Purpose: Add or edit Health Check SLAs which can measure the health of links connected to SD-WAN member interfaces.

Location: Gateways > (Selected Gateway) > SD-WAN > SLAs

Procedure

1. On the **Add/Edit Health Check SLA** > **General** page, specify the **SLA Name**, **Description**, **Monitor Server**, and **Type** of protocol. Click **Add Server** to add a second server. (Note: A second server can be added and it can also be removed if not needed.) Then click **Next**.
2. On the **Add/Edit Health Check SLA** > **SLA Parameters** page, choose SLA parameters from the recommended SLAs or enter custom parameter(s). Also specify the parameters for **Latency**, **Jitter**, and **Packet Loss**. **Note**: Cloud Edge Cloud Console (CECC) provides 4 pre-defined SLAs (VoIP-Video, Audio-Streaming, General Web, and Office 365) (see the Recommended SLA Type and Description table), Then click **Next**.
3. On the **Add/Edit Health Check SLA** > **Link Check Status** page, configure the thresholds and interval for link check status. Then click **Next**.

4. On the **Add/Edit Health Check SLA** > **Action When Inactive** page, disable static routes when SLA parameters cannot be met by selecting **Update Static Route**. (Note: If enabled when a link is inactive, the static routes on that link are removed, and traffic is routed through other links. When the link is active again, the static routes are re-enabled.) Then click **Save**. After you click Save, it takes you back to the Manage SLAs page.

Deleting SLAs

Purpose: Delete an SLA.

Location: Gateways > (Selected Gateway) > SD-WAN > SLAs

Procedure

1. Select the checkbox next to the SLA to delete.
2. Click **Delete**.
3. Verify the deleted SLA is not in the list at **SD-WAN** > **SLAs** (Note: If an SLA is used in an SD-WAN rule, it cannot be deleted.)

Wireless

View information about wireless general settings and configure wireless network access control settings for registered gateways.

Viewing Wireless Network Information

You can view information about wireless networks from Cloud Edge Cloud Console.

Viewing Wireless Network General Settings

Purpose: View general settings for the wireless network.

Location: Gateways > (Selected Gateway) > WIRELESS > Wireless Settings > General Settings

Procedure

1. View information for the following settings:

   - **Wireless access point**

     Displays whether wireless access is enabled. Enabling this settings enables the main wireless network. It does not enable the guest wireless network. However, this setting must be enabled before you can enable the guest wireless network. Default is enabled.

   - **Country / Region**
   - **Frequency**

     Cloud Edge supports 2.4 Ghz and 5.0 Ghz frequencies.

   - **Enable SSID broadcast**

     If enabled, the Cloud Edge gateway broadcasts the **SSID** so that nearby clients can see the main wireless network in the available wireless networks screen.

   - **SSID**

     Displays the **SSID** for the main wireless network.

   - **Channel**
   - **Mode**

     This setting applies to both the main and guest wireless network.

   - **Security**

     Displays the security setting for the main wireless network.

2. View information for the following advanced settings:

   - **DTIM interval** (default)
   - **Beacon interval**
   - **Short preamble**
   - **RTS threshold**

- **Enable short GI**
- **Transmit power**

Note

DTIM interval, **Beacon interval**, and **Transmit power** are the only fields displayed if the network frequency is set to 5 GHz.

Viewing Wireless Guest Network Settings

Purpose: View general settings for the wireless network.

Location: Gateways > (Selected Gateway) > WIRELESS > Wireless Settings > Guest Network

Procedure

1. View information for the following settings:
   - **Enable guest network**

     Displays whether the guest network is enabled or disabled. The default is disabled.
   - **Enable access to local network**

     Displays whether users on the guest wireless network can access resources on the local internal network, provided they have the appropriate permissions. Default is disabled.
   - **Enable SSID broadcast**

     If enabled, the Cloud Edge gateway broadcasts the **SSID** so that nearby clients can see the guest wireless network in the available wireless networks screen.
   - **SSID**

     Displays the **SSID** for the guest network.
   - **Security**

Displays the security setting for the guest network.

Viewing Wireless Troubleshooting Information

Purpose: View troubleshooting information for the wireless network.

Location: Gateways > (Selected Gateway) > WIRELESS > Wireless Settings > Troubleshooting

Procedure

1. View the wireless logs to assist with troubleshooting.
2. Click on **Refresh** to update the displayed log entries.

Wireless Network Access Control

You can configure wireless network access control and manage client connections from Cloud Edge Cloud Console.

How Wireless Network Access Control Rules Work

You can control network access to the main and guest wireless networks using MAC address filtering lists.

There are two MAC address filtering lists: the blocked list and the approved list. You can use either the blocked list or the approved list. You cannot use both at the same time.

How the MAC address filtering options work

Whether the selected MAC address filtering list is applied to the main and guest wireless networks depends on your settings for the **Enable global MAC address filtering** and **Enforce MAC filtering for guest wireless network** options. The following describes how these settings affect wireless network access control:

Enable global MAC address filtering setting is...	Enforce MAC filtering for guest wireless network setting is...	Selected MAC address filtering list applied to...
On	**On**	Both the main and guest wireless networks.
On	**Off**	Both the main and guest wireless networks.
Off	**On**	The guest wireless network but is not applied to the main network.
Off	**Off**	Not applied to either the main or guest wireless networks.

How Use blocked list and Use approved list work

- **Use blocked list** selected:
  - Cloud Edge accepts all wireless connections unless the client MAC address is in the blocked list.
  - If switching to **Use blocked list**, clients with MAC addresses in the blocked list will be disconnected if they are currently connected.
  - After adding a MAC address to the blocked list, the client will be disconnected if currently connected.
  - Consider using the blocked list if you want to generally allow access to the wireless networks, but want to block a small number of clients.
  - Maximum number entries in the blocked list: 256
- **Use approved list** selected:
  - Cloud Edge denies all wireless connections unless the client MAC address is in the approved list.

- If switching to **Use approved list**, clients with MAC addresses that are not in the approved list will be disconnected if they are currently connected.
- After adding a MAC address to the approved list, the client with that MAC address will be able to connect to the wireless networks.
- Consider using the approved list if you do not want to allow broad access to the wireless networks, but want to allow access to a small number of approved clients.
- Maximum number entries in the approved list: 256

Configuring Access Control for the Wireless Networks

Purpose: Configure access control for the Cloud Edge gateway's wireless networks. Access control is used to allow or restrict (deny) specific clients from accessing the main and guest wireless networks.

Location: Gateways > (Selected Gateway) > WIRELESS > Access Control

---

Procedure

1. Under **Enable global MAC address filtering**, click **On**.

   If set to **On**, MAC address filtering is enforced on both the main and guest wireless networks.

2. (Optional) Under **Enforce MAC filtering for guest wireless network**, click **On**.

   Select **On** for this option if you want to enforce MAC address filtering for the guest network even if global MAC address filtering is turned **Off**.

3. Under **MAC Address Filtering List**, select the appropriate option:

   - To use a blocked list for access control, select **Use blocked list**.
   - To use an approved list for access control, select **Use approved list**.

   You can choose to use either a blocked list or an approved list to provide access control to the wireless networks. You cannot use both.

4. Click **Save**.

What to do next

Allow or restrict specific clients from wireless network access by adding clients to the blocked list or approved list (depending on which list is selected).

- *Adding Wireless Network Access Control Rules on page 6-110*
- *Adding Connected Clients to Access Control Rules on page 6-110*

Viewing Wireless Connected Clients

Purpose: View information about wireless connected clients in the **Connected Clients** section.

Location: Gateways > (Selected Gateway) > WIRELESS > Access Control

Procedure

1. In the **Connected Clients** section, you can view the following information about connected clients:

   - **Client ID**

     A unique identifier is assigned to each connected client.

   - **MAC Address**

     The MAC address of the connected client.

   - **IP Address**

     The IP address associated with the connected MAC address.

   - **Hostname**

     The host name associated with the connected MAC address.

   - **SSID**

     You can use the **SSID** to determine whether the client is connected to the main or guest network.

What to do next

You might want to add certain connected clients to the **MAC Address Filtering List** blocked list or approved list to control network access to the wireless networks. See *Adding Connected Clients to Access Control Rules on page 6-110*

Adding Connected Clients to Access Control Rules

Purpose: Add clients in the **Connected Clients** section to access control rules in the approved list or blocked list in the **MAC Address Filtering List** section to allow or restrict (deny) specific clients from accessing the wireless network.

Location: Gateways > (Selected Gateway) > WIRELESS > Access Control

---

Procedure

1. Under the **Connected Clients** section, perform the appropriate action:
   - Using blocked list: Select the clients that you want to add, and then click **Add to Blocked List**.
   - Using approved list: Select the clients that you want to add, and then click **Add to Approved List**.
2. Click **Save**.

The connected clients are added to the appropriate list in the **MAC Address Filtering List** section.

Adding Wireless Network Access Control Rules

Purpose: Add access control rules to the approved list or blocked list in the **MAC Address Filtering List** section. Access control rules allow or restrict (deny) specific clients, identified by their MAC address, from accessing the main and guest wireless networks.

Location: Gateways > (Selected Gateway) > WIRELESS > Access Control

Procedure

1. Under the **MAC Address Filtering List** section, perform the appropriate action, depending on which list you are using for access control:
   - Using blocked list: Click **Add** under **Use blocked list**.
   - Using approved list: Click **Add** under **Use approved list**.

   The **Add/Edit MAC Address Filtering Rule** dialog box appears.
2. Specify the MAC address that you want to use for filtering in **MAC address**.
3. (Optional) Specify a description.
4. Click **Save**.

Deleting Wireless Network Access Control Rules

Purpose: Delete MAC address filtering rules from the blocked list or the approved list to remove those MAC addresses from wireless network access control.

Location: Gateways > (Selected Gateway) > WIRELESS > Access Control

Procedure

1. Under the **MAC Address Filtering List** section, perform the appropriate action:
   - Select the MAC address access control rules in the blocked list that you want to delete and then click **Delete**.
   - Select the MAC address access control rules in the approved list that you want to delete and then click **Delete**.

Bandwidth Control

Peer-to-peer downloading, video streaming and instant message applications consume network bandwidth and can impact productivity. Bandwidth control reduces network congestion by controlling communications,

reducing unwanted traffic and allowing critical traffic or services the appropriate bandwidth allocation. Bandwidth control gives all users fair access to resources and ensures better access to resources that are more central to the organization. Similar to policy rules, bandwidth control can limit traffic based on source or destination IP address, application or service, and time of day.

Bandwidth control rules can be as general or specific as needed. The bandwidth control rules are compared against the incoming traffic in sequence, and because the first rule that matches the traffic is applied, the more specific rules must precede the more general ones. For example, a rule for a single application must precede a rule for all applications if all other traffic-related settings are the same. If the traffic does not match any of the rules, the traffic uses the remaining bandwidth.

Note

Bandwidth control policies cannot exceed the interface bandwidth settings.

Managing Bandwidth Control

Purpose: Bandwidth control reduces network congestion by controlling communications, reducing unwanted traffic and allowing critical traffic or services the appropriate bandwidth allocation.

Location: Gateways > (gateway name) > Bandwidth Control

Procedure

1. Do the following:
   - Click **Add** to create a new rule.
   - Use **Search** at the top right to locate a rule.
   - Click a rule's name to view or modify settings.
   - Select a rule and then click **Edit** to view or modify settings.
   - Select a rule and then click **Move** to change the rule order.

- Select a rule and then click **More** to change the status or duplicate the rule.
- Select a rule and then click **Delete** to remove the rule.

2. Configure available settings.
3. Click **Save**.

Adding/Editing Bandwidth Control Rules

Purpose: Add or edit bandwidth control rules by specifying source users, user groups or addresses, destination, traffic type, schedules, egress interface and other bandwidth settings.

Location: Gateways > (gateway name) > Bandwidth Control > Add / Edit

---

Procedure

1. Specify a rule name between 1 and 32 characters, consisting of letters, numbers, or underlines.
2. Specify the **Description**.
3. Enable or disable the rule.
4. Configure **Source Users / User Groups / IP Addresses / MAC Addresses**.
   - Select **Any** for the rule to affect all users and all IP addresses.
   - Select **Selected users / user groups** for the rule to affect only specific users or groups.
   - Select **Selected IP addresses** for the rule to affect only specific IP addresses.
   - Select **Selected MAC addresses** for the rule to affect only specific MAC addresses.
5. Configure **Destination Addresses**.
   - Select **Any** for the rule to include all IP addresses (default).

- Select **Selected IP addresses** for the rule to affect only specific IP addresses.

6. Configure **Traffic Type**.
   - Select **Any** or **Selected applications** for the rule to include all application groups (default) or only specific applications.
   - Select **Any** or **Selected services** for the rule to include all services (default) or only specific services.
7. Configure the **Schedule**.

Option	Description
Always	Includes all schedules. (Default)
Schedule name	Displays names of available schedule objects.
Add New Schedule Object	Access the **Add/Edit** schedule object creation dialog box.

8. Configure **Egress Interface** by selecting an interface from the drop-down menu.
9. Configure **Bandwidth** by specifying the upstream and downstream settings.
10. Click **Save**.

Duplicating Bandwidth Control Rules

Purpose: Duplicate an existing rule.

Location: Gateways > (gateway name) > Bandwidth Control

Procedure

1. Select a rule and click the **More** pull-down menu.
2. Click **Duplicate**.

3. Verify that a new rule appears in the list.

Enabling/Disabling Bandwidth Control Rules

Purpose: Bandwidth control rules can be provisioned disabled. This procedure applies to bandwidth control rules already created but not enabled. Changes take effect after clicking **Deploy All**.

Location: Gateways > (gateway name) > Bandwidth Control

Procedure

1. Select the check boxes next to the rules to enable or disable.
2. Click the **More** pull-down menu and select **Enable** or **Disable**.
3. Click **Deploy All** to make the changes take effect.

Deleting Bandwidth Control Rules

Purpose: Delete bandwidth control rules.

Location: Gateways > (gateway name) > Bandwidth Control

Procedure

1. Select the check boxes next to the rules to delete.
2. Click **Delete**.
3. Click **OK** to confirm.
4. Verify the deleted rule is not in the list.

User VPN

Whenever users access the organization from remote locations, it is essential that the usual requirements of secure connectivity be met but also the special demands of remote clients. User Virtual Private Networking (VPN) extends VPN functionality to remote users, enabling users to securely

communicate sensitive information to networks and servers over the VPN tunnel, using dial-up (including broadband), LAN, and mobile connections.

Virtual Private Networks

Virtual Private Network (VPN) technology is generally used to ensure that employees working off-site can remotely access their corporate network with appropriate security measures in place. In general terms, authentication is the process of attempting to verify the (digital) identity for both accessing network resources and logging on the VPN network. VPN leverages existing infrastructure (the Internet) to securely build and enhance existing connectivity. Based on standard secure Internet protocols, VPN implementation enables secure links between special types of network nodes, secure gateways. Site-to-site VPN ensures secure links between gateways. User VPN ensures secure links between gateways and remote access clients.

A typical Cloud Edge deployment allows users to remotely connect to the corporate network resources using VPN. Other remote sites are guarded by Cloud Edge and strict security policies regulate communication between all network resources and the remote endpoint.

Cloud Edge supports IPV4-to-IPV4 VPN access.

Encryption Algorithms

The following table explains encryption algorithms. The Digital Encryption Standard (DES) is a 64-bit block algorithm that uses a 56-bit key. The Advanced Encryption Standard (AES) is a private key algorithm supporting key lengths from 128 to 256 bits and variable-length blocks of data.

Algorithm	Description
AES 128 CBC	A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 128-bit key.
AES 192 CBC	A 192-bit block Cipher Block Chaining (CBC) algorithm that uses a 192-bit key.

Algorithm	Description
AES 256 CBC	A 256-bit block Cipher Block Chaining (CBC) algorithm that uses a 256-bit key.
DES EDE3 CBC	Triple-DES, in which plain text is encrypted three times by three keys.
BF-CBC	A 64-bit block keyed, symmetric Cipher Block Chaining (CBC) algorithm by Blowfish.

Authentication Algorithms

Algorithm	Description
MD5	Message Digest (version 5) hash algorithm (on one-way hash function) developed by RSA Data Security, which is intended for digital signature applications, where a large file must be compressed in a secure manner before being encrypted with a private key/public key algorithm.
SHA1	Secure Hash Algorithm 1, which produces a 160-bit message digest. The large message digest provides security against brute-force collision and inversion attacks.
SHA-256 and **SHA-512**	Secure Hash Algorithm 2, which allows you to choose either a 256-bit or 512-bit message digest. SHA-512 message digests provide the highest security against brute-force collision and inversion attacks.

Internet Key Exchange (IKE) Protocols

Internet Key Exchange (IKE) protocol creates a tunnel to transfer IP Security (IPSec) encoded data.

SSL VPN

A Secure Sockets Layer Virtual Private Network (SSL VPN) is a form of VPN that can be used with a standard web browser. SSL VPN requires client

software installation, and is ideal for applications including web-based email, business and government directories, file sharing, remote backup, remote system management, and consumer-level electronic commerce.

When users have complete administrative rights over their endpoints and use a variety of applications, tunnel mode allows remote clients to access the local internal network as if they were connected to the network directly.

Note

Cloud Edge supports IPv4-to-IPv4 SSL VPN access.

Certain Cloud Edge gateway models do not support VPN.

Managing SSL VPN

Purpose: Configure Secure Sockets Layer Virtual Private Network (SSL VPN) to use VPN with a standard web browser.

Location: Gateways > (gateway name) > USER VPN > SSL VPN > General

Procedure

1. Optionally enable SSL VPN.
2. Configure basic settings.
   - **Protocol**
   - **Port**
   - **Add New Address Object**
   - **Local networks**
   - **Client network pool**
3. Configure advanced settings.
   - **Encryption algorithm**

     See *Encryption Algorithms on page 6-116*.

- **Authentication algorithm**

  See *Authentication Algorithms on page 6-117*.

- **Key size**
- **Key lifetime**
- **Local DNS**
- **Local domains**
- **Enable compressed traffic**
- **Enable debug mode**
- **Enable simultaneous logon**
- **Enable network masquerade**

Viewing SSL VPN Clients

Purpose View all clients currently connecting through VPN. The table displays the user name, when the session started, the client public IP address, and the virtual IP address. The total number of connected clients is displayed above the table.

Location: Gateways > (gateway name) > USER VPN > SSL VPN > Clients

Procedure

1. View all clients connecting through SSL VPN in the table.

Troubleshooting SSL VPN

Purpose View general troubleshooting guidelines when setting up SSL VPN.

Location: Gateways > (gateway name) > USER VPN > SSL VPN > Troubleshooting

Procedure

1. Do the following to troubleshoot SSL VPN:
   - Learn about error messages at *Understanding SSL VPN Error Messages on page 6-120*.
   - Verify that the client can ping the Cloud Edge gateway successfully.
   - Verify that the client can access the SSL VPN-configured TCP or UDP port.
   - Verify that the Windows client configuration file `openvpn.ovpn` is configured the same as the `https://<gateway_server_IP_address>/Config/openvpn.ovpn` file.
   - Verify that the mobile client configuration file **mobile.ovpn** is configured the same `https://<gateway_server_IP_address>/Config/mobile.ovpn`.

Understanding SSL VPN Error Messages

Error Message	Explanation	Recommended Action
`TCP: connect to X.X.X.X:8445 failed, will try again in 5 seconds: Connection refused`	SSL VPN client cannot reach the Cloud Edge gateway.	1. Ping the Cloud Edge gateway, assuming ping is allowed (that is, not blocked) between the SSL VPN client and the Cloud Edge gateway. Confirm that you have network connectivity between the SSL VPN client and the Cloud Edge gateway. 2. To allow SSL VPN traffic, configure the network firewall to open the SSL VPN-configured TCP or UDP port to the Cloud Edge gateway.

Error Message	Explanation	Recommended Action
`SIGTERM[soft,auth-failure] received, process exiting`	User name and/or password is invalid.	Specify the correct user name and/or password or ask an administrator to reset the password.

L2TP VPN

A Cloud Edge L2TP VPN allows remote users to establish secure connections to the internal company network over a public network such as the Internet.

Cloud Edge uses the L2TP tunneling protocol to set up a point-to-point connection between the client and the Cloud Edge gateway. Security is ensured by encrypting the L2TP packets using IPsec before transporting the data to the end point over the L2TP tunnel. L2TP creates the VPN tunnel, and this tunnel is used to transfer IPsec encoded data. Think of L2TP as the process that builds a tunnel, and IPsec packets as trucks that carry the encrypted data along the tunnel.

Cloud Edge supports L2TP/IPsec VPNs for Windows 7, 8.1, and 10 clients and iOS and Android mobile clients.

There is no need for end-users to install a VPN client. Cloud Edge L2TP/IPsec VPNs use a Windows standard L2TP/IPsec configuration.

By default, the Cloud Edge L2TP/IPsec VPN sends all data from the client through the VPN. To send only traffic destined for internal networks through the VPN tunnel, you can configure the VPN for split-tunnel mode in the client's L2TP configuration.

Cloud Edge maintains a persistent L2TP/IPsec connection with the end point until the VPN is manually disconnected or unless the endpoint is not available.

Note

Cloud Edge supports IPv4-to-IPv4 L2TP VPN access.

Certain Cloud Edge gateway models do not support VPN.

Related information

- *Virtual Private Networks*

Managing L2TP VPN

Purpose: Configure Layer 2 Tunneling Protocol Virtual Private Network (L2TP VPN) with IPsec to use as a VPN from remote Windows clients.

Note

To configure L2TP VPNs, the Cloud Edge gateway must be in Routing Mode.

Location: Gateways > (gateway name) > USER VPN > L2TP VPN > General

Procedure

1. Optionally enable L2TP VPN.
2. For **Client network pool**, enter the IPv4 address pool in CIDR format.

   Important

   The assigned IP addresses must be part of an independent network segment (the network segment is different from network segments used on any other interface).

3. Enter a key known to both endpoints in **Preshared key**.

   The key is used to authenticate the L2TP endpoints while establishing the connection.

   Before establishing the connection, the remote user must provide authentication credentials using a Cloud Edge hosted user.

   To configure hosted users, see *Hosted Users and Groups on page 6-173*.

4. Configure advanced settings.

   - **Primary DNS server** and **Secondary DNS server**

If both the **Primary DNS server** and **Secondary DNS server** are left blank, the gateway's default DNS servers are used as L2TP DNS servers.

- **Primary WINS server** and **Secondary WINS server**
- **MTU**

  Supported values are 500 through 1400. This is a required field. The **MTU** field cannot be left blank.

- **Enable L2TP debug mode**
- **Enable dead peer detection**

  Dead peer detection identifies inactive or unavailable VPN peers and can help restore resources that are lost when a peer is unavailable. Selecting **Enable dead peer detection** reestablishes VPN tunnels on idle connections and cleans up dead VPN peers if required.

  Use this option to keep the tunnel connection open when no traffic is being generated inside the tunnel.

- **Enable network masquerade**
- **IKE Authentication algorithm**
  - `MD5`
  - `SHA1`
  - `SHA-256`
  - `SHA-512`

  `SHA1` is the default.

  See *Authentication Algorithms on page 6-117*.

- **IPsec authentication algorithm**
  - `MD5`
  - `SHA1`

- SHA-256
- SHA-512

SHA1 is the default.

- IKE Debugging

  Enable or disable IKE debugging.

5. Click **Save**.

What to do next

If you do not want all traffic to route through the VPN tunnel, you can configure split tunneling on the Windows client.

- You must first configure L2TP on the client and connect the L2TP VPN.
- Disconnect the L2TP connection and right-click on the L2TP new connection and select **Properties**.
- You can then select **Internet Protocol Version 4 (TCP/IPv4)** and click on **Properties** and then on **Advanced**.
- You can deselect **Use default gateway on remote network** to enable split tunneling. Only traffic destined for the gateway's internal network will route through the L2TP gateway.

Viewing L2TP VPN Clients

Purpose View all clients currently connecting through L2TP VPNs. The table displays the user name, when the session started, the client public IP address, and the virtual IP address. The total number of connected clients is displayed above the table.

Location: Gateways > (gateway name) > USER VPN > L2TP VPN > Clients

---

Procedure

1. View all clients connecting through L2TP VPN in the table.

Troubleshooting L2TP VPN

Purpose View general troubleshooting guidelines when setting up L2TP VPN.

Location: Gateways > (gateway name) > USER VPN > L2TP VPN > Troubleshooting

Procedure

1. View the live L2TP and IPsec log readouts.

Note

The live IPsec log is shared for L2TP and Site-to-Site VPNs.

Site-to-Site VPN

A site-to-site Virtual Private Network (*VPN on page 6-116*) allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the Internet. Site-to-site VPN extends the company's network, making computer resources from one location available to employees at other locations. An example of a company that needs a site-to-site VPN is a customer with dozens of branch offices around the world.

Cloud Edge creates encrypted tunnels by using the Internet Key Exchange (IKE) and IP Security (IPsec) protocols. IKE creates the VPN tunnel, and this tunnel is used to transfer IPsec encoded data. Think of IKE as the process that builds a tunnel, and IPsec packets as trucks that carry the encrypted data along the tunnel.

Cloud Edge gateways implement the Encapsulated Security Payload (ESP) protocol. The encrypted packets look like ordinary packets that can be routed through any IP network.

IKE is performed automatically based on pre-shared keys or X.509 digital certificates. As an option, you can specify manual keys. Interface mode, supported in NAT/Route mode only, creates a virtual interface for the local end of a VPN tunnel.

Note

Cloud Edge supports IPv4-to-IPv4 Site-to-Site VPN access.

Certain Cloud Edge gateway models do not support VPN.

IPsec Connections

An IPsec (or VPN) tunnel is a virtual interface on a security gateway associated with an existing VPN connection, and is used by IP routing as a point-to-point interface directly connected to a VPN peer gateway.

Outbound packets use the following routing process:

- An IP packet with destination address X is matched against the routing table
- The routing table indicates that IP address X should be routed through a point-to-point link which is the VPN tunnel interface that is associated with peer gateway Y
- The VPN kernel intercepts the packet as it specifies the virtual tunnel interface
- The packet is encrypted using the proper IPsec authentication type parameters with peer gateway Y, and the new packet receives the peer gateway Y's IP address as the destination IP
- Based on the new destination IP, the packet is rerouted to the physical interface according to the appropriate routing table entry for Y's address

Inbound packets use the following routing process:

- An IPsec packet specifies the machine coming from gateway Y
- The VPN kernel intercepts the packet on the physical interface
- The VPN kernel identifies the originating VPN peer gateway
- The VPN kernel decapsulates the packet, and extracts the original IP packet

- The VPN kernel detects that a VPN tunnel interface exists for the peer VPN gateway, and reroutes the packet from the physical interface to the associated VPN tunnel interface
- The packet specifies the IP stack through the VPN tunnel interface

Supported Configuration Information

- The Yamaha VPN router is supported as part of a Cloud Edge site-to-site VPN (non-aggressive mode).

Note

The Yamaha FWX 120 and RTX 1200 models are tested and supported.

- The Cloud Edge gateway can be an edge device (directly connected to the Internet) or an internal device (behind a NAT device configured for port forwarding or NAT rules).
- Cloud Edge supports Site–to–Site VPNs in a dual WAN scenario for Cloud Edge gateways running Cloud Edge 6.0 or later.

Note

For gateways running Cloud Edge 5.x or earlier, you can configure only a single WAN for VPN support, even if dual-WAN access is enabled.

- Certain Cloud Edge gateway models do not support VPN.

Site-to-Site VPN Topologies

You should understand the three site-to-site VPN topologies before planning and creating your VPN configuration.

Peer-to-Peer VPN Topology

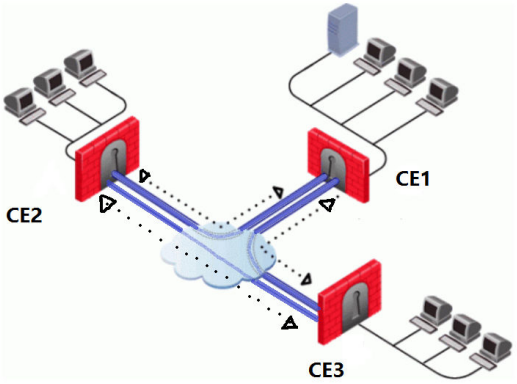
A single encrypted VPN gateway between two sites.

Full-Mesh VPN Topology

Every remote site is connected to every other remote site as well as the central site. All remote sites can communicate directly with the central site

and with every other remote site without need to route through the central site.

Full-mesh VPNs are extremely reliable, because all the remote sites can still communicate even if the main site goes down. A full-mesh configuration also offers reduced latency for sensitive applications, because each remote site can communicate with the other remote sites directly.



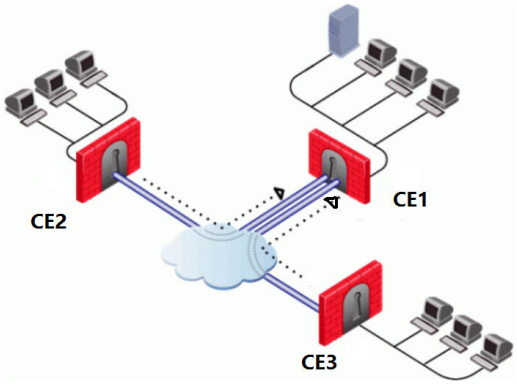
Each device can set up a VPN connection with four other devices, including third-party devices. Any two directly-connected peers can communicate. Any indirectly connected peers cannot communicate.

See *Example: Full-Mesh Site-to-Site VPN on page 6-129*

Star VPN Topology

Multiple remote sites all connect to a central site. This topology resembles a spoke and hub configuration. All remote sites can communicate directly with the central site; however, for communication from one remote site to

another remote site, the IPsec traffic must travel to the central site and then the hub device routes traffic to the destination remote site.



Star topologies support one hub device and four spoke devices, including third-party devices (five total devices). A spoke device can communicate with the hub device directly. A spoke device communicates with other spoke devices indirectly as all IPsec traffic is first sent to the hub device.

See *Example: Star Site-to-Site VPN on page 6-130*

Example: Full-Mesh Site-to-Site VPN

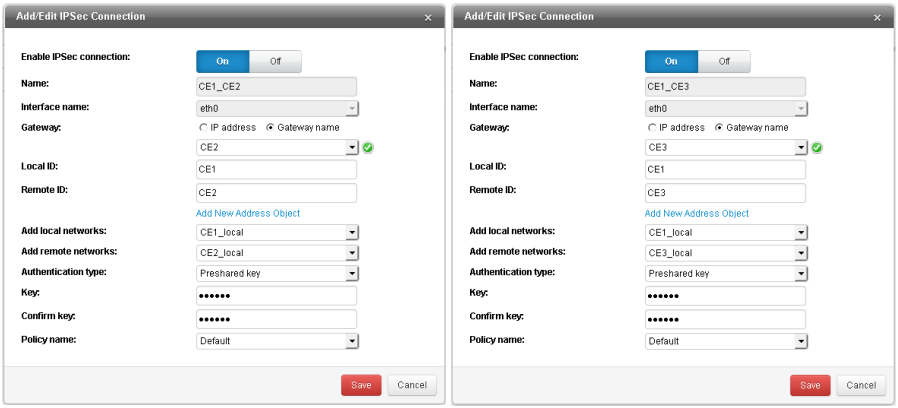
In the following example, three Cloud Edge gateways are used to create a full-mesh site-to-site VPN configuration.

Configuration Summary

Device names: CE1, CE2, and CE3

- In CE1, set up two connections, one to each of the other devices: CE1 to CE2, CE1 to CE3
- In CE2, set up two connections, one to each of the other devices: CE2 to CE1, CE2 to CE3
- In CE3, set up two connections, one to each of the other devices: CE3 to CE1, CE3 to CE2

Configuration on CE1



Configuration on CE2 and CE3

Connections for the CE2 and CE3 gateways are configured similarly to CE1.

Example: Star Site-to-Site VPN

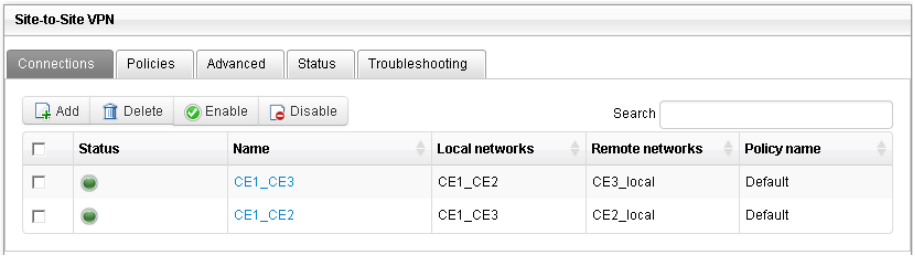
In the following example, three Cloud Edge gateways are used to create a star site-to-site VPN configuration.

Configuration Summary

Device names: CE1 (hub), CE2 (spoke), and CE3 (spoke)

- In hub device CE1, set up two connections to the spoke devices: CE1 to CE2, CE1 to CE3
- In spoke device CE2, set up a connection to hub device CE1: CE2 to CE1.
- In spoke device CE3, set up a connection to hub device CE1: CE3 to CE1.

Configuration on CE1 (hub)



CE1 connection to CE2:

- Local ID: CE1
- Remote ID: CE2

> **Note**
>
> CE2 is the Local ID in the CE2 gateway's configuration.

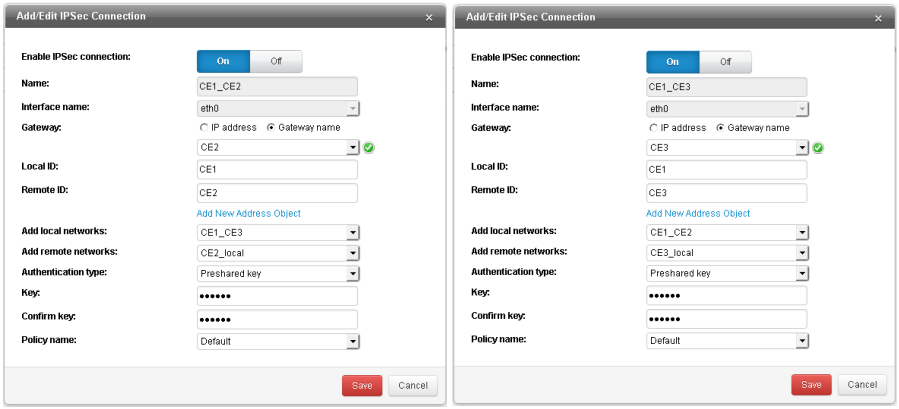
- Local network: Address object contains IPv4 ranges for both CE1 and CE3's local networks
- Remote network: Address object contains IPv4 range for CE2's local network

CE1 connection to CE3:

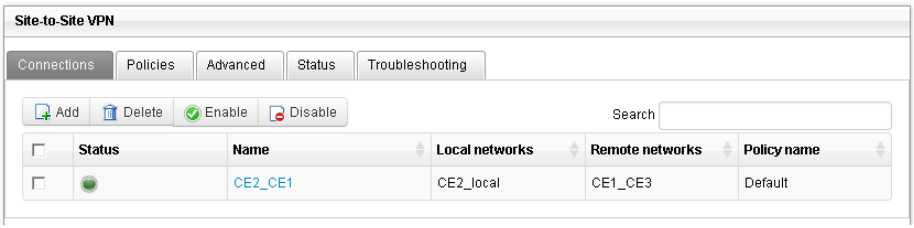
- Local ID: CE1
- Remote ID: CE3

> **Note**
>
> CE3 is the Local ID in the CE3 gateway's configuration.

- Local network: Address object contains IPv4 ranges for both CE1 and CE2's local networks
- Remote network: Address object contains IPv4 range for CE3's local network



Configuration on CE2 (spoke)

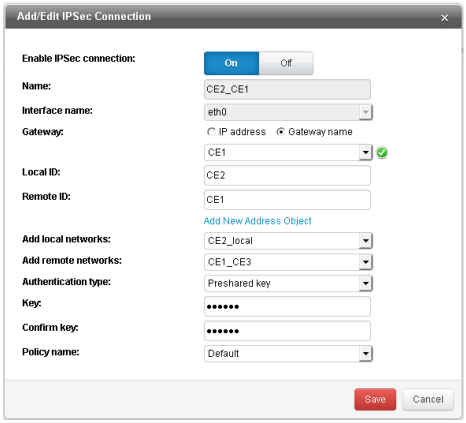


CE2 connection to CE1:

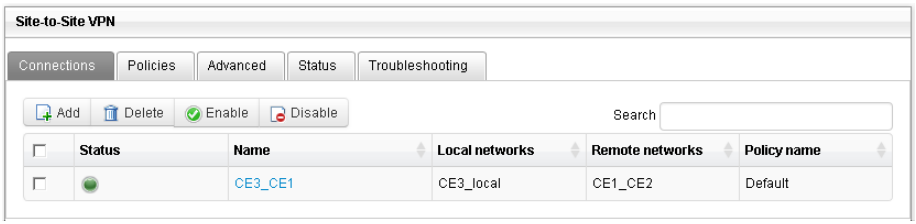
- Local ID: CE2

> **Note**
> CE2 is the Remote ID in the CE1 gateway's configuration.

- Local network: Address object contains IPv4 range for CE2's local network
- Remote network: Address object contains IPv4 ranges for both CE1 and CE3's local networks



Configuration on CE3 (spoke)

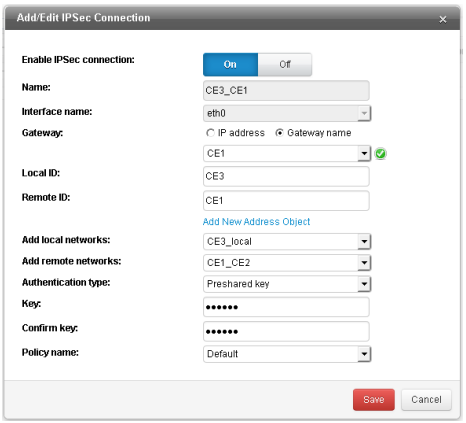


CE3 connection to CE1:

- Local ID: CE3

> **Note**
> CE3 is the Remote ID in the CE1 gateway's configuration.

- Local network: Address object contains IPv4 range for CE3's local network
- Remote network: Address object contains IPv4 ranges for both CE1 and CE2's local networks



Configuring Full-Mesh Site-to-Site VPNs

There are several steps to configuring a full-mesh site-to-site VPN.

Every gateway must be configured with a tunnel to every other gateway.

Procedure

1. Create local and remote address objects that you will need during the VPN configuration.

   Adding/Editing IP Address/FQDN Objects on page 6-168

For information about what address objects are needed, you can review the example: *Example: Full-Mesh Site-to-Site VPN on page 6-129*

2. Choose which IPsec policy to use when configuring the IPsec VPN connections.

   IPsec policies are selected when configuring an IPsec VPN connection. You can use the Default IPsec policy, use another existing policy, or you can add a new IPsec policy.

   Adding an IPsec Policy on page 6-141

3. On the central hub gateway, configure a tunnel to every remote gateway.

   Adding an IPsec VPN Connection on page 6-138

4. On every remote gateway, configure a tunnel to every remote gateway and back to the central hub.

   Adding an IPsec VPN Connection on page 6-138

5. Optional: Configure advanced options for site-to-site VPN settings including dead peer detections and enabling IKE debugging.

   Configuring Advanced Site-to-Site VPN Settings on page 6-144

Configuring Star Site-to-Site VPNs

There are several steps to configuring a star site-to-site VPN.

First, the central hub gateway must be configured with a tunnel connection to every remote gateway. Then, every remote gateway must be configured with a connection back to the central hub.

Procedure

1. Create local and remote address objects that you will need during the VPN configuration.

   Adding/Editing IP Address/FQDN Objects on page 6-168

   For information about what address objects are needed, you can review the example: *Example: Star Site-to-Site VPN on page 6-130*

2. Choose which IPsec policy to use when configuring the IPsec VPN connections.

   IPsec policies are selected when configuring an IPsec VPN connection. You can use the Default IPsec policy, use another existing policy, or you can add a new IPsec policy.

   Adding an IPsec Policy on page 6-141

3. On the central hub gateway, set up a connection to each spoke device.

   Adding an IPsec VPN Connection on page 6-138

4. On each spoke gateway, set up a connection to the hub device.

   Adding an IPsec VPN Connection on page 6-138

5. Optional: Configure advanced options for site-to-site VPN settings including dead peer detections and enabling or disabling IKE debugging.

   Configuring Advanced Site-to-Site VPN Settings on page 6-144

Configuring Peer-to-Peer Site-to-Site VPNs

There are several steps to configuring a peer-to-peer site-to-site VPN.

In the peer-to-peer configuration, a local gateway is connected to a single remote gateway.

Procedure

1. Create local and remote address objects that you will need during the VPN configuration.

   Adding/Editing IP Address/FQDN Objects on page 6-168

2. Choose which IPsec policy to use when configuring the IPsec VPN connections.

   IPsec policies are selected when configuring an IPsec VPN connection.

   You can use the `Default` IPsec policy, use another existing policy, or you can add a new IPsec policy.

Adding an IPsec Policy on page 6-141

3. On one of the peer devices, set up a connection to the other peer device.

   Adding an IPsec VPN Connection on page 6-138

4. On the other peer device, set up a connection back to the first device.

   Adding an IPsec VPN Connection on page 6-138

5. Optional: Configure advanced options for site-to-site VPN settings including dead peer detections and enabling or disabling IKE debugging.

   Configuring Advanced Site-to-Site VPN Settings on page 6-144

Managing Site-to-Site VPNs

You can manage Site-to-Site VPN configurations including the following:

- *Managing IPsec Connections on page 6-137*
- *Managing IPsec Policies on page 6-141*
- *Configuring Advanced Site-to-Site VPN Settings on page 6-144*

Managing IPsec VPN Connections

Purpose: Manage site-to-site IPsec VPN connections used to establish IPsec tunnels between Cloud Edge gateways or third-party devices.

Location: Gateways > (gateway name) > Site-to-Site VPN > Connections

---

Procedure

1. Review information about configuring site-to-site VPNs:
   - *Supported Configuration Information on page 6-127*
   - *Site-to-Site VPN Topologies on page 6-127*
   - *Configuring Full-Mesh Site-to-Site VPNs on page 6-134*
   - *Configuring Star Site-to-Site VPNs on page 6-135*

- *Configuring Peer-to-Peer Site-to-Site VPNs on page 6-136*
- *Best Practice Configuration for IPsec Traffic Traversing Multiple Gateways on page 6-145*

2. Do the following:
   - Click **Add** to create a new IPsec connection.
   - Click a connection's name to view or modify settings.

     Note

     You cannot modify the local network or remote network settings on an existing Site-to-Site VPN connection. If you want to change the local networks or remote networks, you must delete the existing Site-to-Site VPN connection and create a new connection with the desired settings.

   - Select a connection and then click **Delete** to delete the connection.
   - Select a connection and then click **Enable** to enable the connection.
   - Select a connection and then click **Disable** to disable the connection.

Related information

- *Adding an IPsec VPN Connection*

Adding an IPsec VPN Connection

Purpose: Add a site-to-site IPsec VPN connection to establish IPsec tunnels between Cloud Edge gateways or third-party devices.

Location: Gateways > (gateway name) > Site-to-Site VPN > Connections

For more information about supported site-to-site VPN topologies and configuration steps for implementing those topologies see:

- *Site-to-Site VPN Topologies on page 6-127*

- *Supported Configuration Information on page 6-127*
- *Configuring Full-Mesh Site-to-Site VPNs on page 6-134*
- *Configuring Star Site-to-Site VPNs on page 6-135*
- *Configuring Peer-to-Peer Site-to-Site VPNs on page 6-136*
- *Best Practice Configuration for IPsec Traffic Traversing Multiple Gateways on page 6-145*

Note

When you finish configuring a Site-to-Site VPN connection, you cannot modify the local network or remote network settings. If you want to change the local networks or remote networks after you save the configuration, you must delete the existing Site-to-Site VPN connection and create a new connection with the desired settings.

Procedure

1. Click **Add**.

   The **Add/Edit IPSec connection** window opens.

2. Specify the IPsec connection parameters.

Enable IPSec connection	Select **ON** to enable the tunnel.
Name	Type a name to identify the IPsec VPN tunnel.
Interface name	Select the interface name from the drop-down list.

Gateway	Select the desired method for specifying the gateway: **IP address**: Specify the gateway IP address. **Gateway name**: Select an available gateway from the drop-down list. **Note** You can select either **IP address** or **Gateway name** if the VPN device is Cloud Edge. If the VPN device is a third-party device, you must choose **IP address**.
Local ID	Enter a text string for **Local ID**. Cloud Edge uses the **Local ID** to help identify which gateways are local in the topology.
Remote ID	Enter a text string for **Remote ID**. Cloud Edge uses the **Remote ID** to help identify which gateways are remote in the topology.
Add local networks	Select the local network or add a new address object.
Add remote networks	Select the remote network or add a new address object.
Authentication type	Select **Preshared key** or **RSA key** from the drop-down list.
For **Preshared key**	Specify the key and confirm it. If **Preshared Key** is selected, specify the pre-shared key in **Key** and confirm it in **Confirm key**. Cloud Edge uses the key to authenticate itself to the remote peer or dial-up client. Make sure to define the same value at the remote peer or client. The key must contain at least six printable characters and should be known only by network administrators. For optimum protection against currently known attacks, the key should consist of a minimum of 16 randomly chosen alphanumeric characters.

Policy name	Select the policy name from the drop-down list, either **Default** or a specific policy, that applies to the IPsec tunnel. **Note** Configure non-default IPsec policies at **Gateway** > **Site-to-site VPN** > **Policies**. See *Adding an IPsec Policy on page 6-141*.

3. Click **Save**.

Managing IPsec Policies

Purpose: Manage IPsec policies used when establishing site-to-site VPN tunnels between Cloud Edge gateways or third-party devices.

Location: Gateways > (gateway name) > Site-to-Site VPN > Policies

Procedure

1. Do the following:
   - Click **Add** to create a new IPsec policy.
   - Click a policy's name to view or modify settings.
   - Select a policy and then click **Delete** to delete the policy.

Adding an IPsec Policy

Purpose: Add IPsec policies to configure the IKE encryption and authentication algorithms used for site-to-site VPN connections.

Location: Gateways > (gateway name) > Site-to-Site VPN > Policies

Procedure

1. Click **Add**.

   The **Add/Edit IPSec Policy** window opens.

2. Specify a name for the new IPsec policy.
3. Select the `IKE encryption algorithm` from the drop-down list box.

Note

The Digital Encryption Standard (DES) is a 64-bit block algorithm that uses a 56-bit key. The Advanced Encryption Standard (AES) is a private key algorithm supporting key lengths from 128 to 256 bits and variable-length blocks of data.

Option	Description
3DES	Triple-DES, in which plain text is encrypted three times by three keys.
AES 128	A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 128-bit key.
AES 192	A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 192-bit key.
AES 256	A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 256-bit key.

4. Select the **IKE authentication algorithm** value from the drop-down list box.
    - **MD5**—Message Digest (version 5) hash algorithm (on one-way hash function) developed by RSA Data Security, which is intended for digital signature applications, where a large file must be compressed in a secure manner before being encrypted with a private key/public key algorithm.
    - **SHA1**—Secure Hash Algorithm 1, which produces a 160-bit message digest. The large message digest provides security against brute-force collision and inversion attacks.
    - **SHA-256**—Secure Hash Algorithm 2 with a 256-bit digest. SHA2 digests provide higher security against brute-force collision and inversion attacks.
    - **SHA-512**—Secure Hash Algorithm 2 with a 512-bit message digest. The largest message digests provide the highest security against brute-force collision and inversion attacks.

5. Select the `IKE SA lifetime` value (in hours, maximum 24) from the drop-down list box (1-24). It specifies the length of time that the negotiated key will stay effective.
6. Select the `IKE DH group` value from the drop-down list box that are supported by secure gateways.
   - **Group2: MODP**—1024 bits (default)
   - **Group5: MODP**—1536 bits
   - **Group14:MODP**—2048 bits

   The above groups refer to the Diffie-Hellman key computation (also known as exponential key agreement) that is based on the Diffie-Hellman (DH) mathematical groups supported by a security gateway for IKE and IPsec Security Association (SA).
7. Select the `IPsec encryption` value from the drop-down list box.
   - `No encryption`—Do not use an encryption algorithm.
   - `3DES`
   - `AES 128`
   - `AES 192`
   - `AES 256`
8. Select the `IPsec authentication algorithm` value from the drop-down list box.
   - `MD5`
   - `SHA1`
   - `SHA-256`
   - `SHA-512`
9. Select the `IPsec lifetime` value (in hours, maximum 24) from the drop-down list box (1-24).
10. Select the `IPsec PFS group` value from the drop-down list.

- None
- Group2: MODP
- Group5: MODP
- Group14:MODP

11. Click **Save**.

Configuring Advanced Site-to-Site VPN Settings

Purpose: Configure advanced options for site-to-site VPN settings including whether to use dead peer detection and enabling/disabling IKE debugging. Advanced settings apply to all site-to-site VPN connections on the gateway.

Location: Gateways > (gateway name) > Site-to-Site VPN > Advanced

Procedure

1. Configure advanced site-to-site VPN settings.

Option	Description
Dead peer detection	Dead peer detection (DPD) identifies inactive or unavailable IKE peers. Using IPsec traffic patterns, DPD can use a minimal number of IKE messages to confirm whether the connection is live. DPD is used to restore resources that are lost when a peer is unavailable. Selecting **Enable dead peer detection** reestablishes VPN tunnels on idle connections and cleans up dead VPN peers if required.
IKE Debugging	Enable or disable IKE debugging.

2. Click **Save**.

IPsec Status

Purpose: View the live IPsec connection status.

Location: Gateways > (gateway name) > Site-to-Site VPN > Status

Procedure

1. View the IPsec status.

IPsec Troubleshooting

Use the IPsec troubleshooting logs to view activity over IPsec VPN tunnels.

You should be aware of a performance issue for a certain IPsec connection configuration and the best practice recommendation for eliminating the performance issue. For more information, see *Best Practice Configuration for IPsec Traffic Traversing Multiple Gateways on page 6-145*.

Best Practice Configuration for IPsec Traffic Traversing Multiple Gateways

You should be aware of a performance issue for a certain IPsec connection configuration and the best practice recommendation for eliminating the performance issue.

Performance issues can occur when a customer environment contains more than one Cloud Edge gateway with multiple IPsec VPN connections. When the traffic passes through multiple IPsec connections Cloud Edge scans the traffic as it traverses each connection. Multiple scans do not provide better detection, but multiple scans of the same traffic do result in a performance drop.

To avoid any unnecessary scans, the best practice is to scan traffic only once by the Cloud Edge gateway that is closest to the incoming traffic and configure other gateways in the route from source to destination to bypass the scan.

To achieve this, you can use the gateway policy rules to bypass scanning on all but the closest gateway to the IPsec traffic.

Best Practice Configuration Rules

Gateway's Role in Configuration	Rule Guidelines
Full-mesh IPsec gateways	Create a policy rule where the **Action** is to **Bypass** traffic and add the following to the specified fields: • **Destination** Add a network object that contains the gateway's own private network. • **Source users/User Groups/IP Addresses/FQDN/MAC Addresses** Add a network object that contains all other private networks in the mesh VPN.
Spokes of a star IPsec gateway	Create a policy rule where the **Action** is to **Bypass** traffic and add the following to the specified fields: • **Destination** Add a network object that contains the gateway's own private network. • **Source users/User Groups/IP Addresses/FQDN/MAC Addresses** Add a network object that contains all other private networks in the star VPN.
Hub of a star IPsec gateway	Create a policy rule where the **Action** is to **Bypass** traffic and add the following to the specified fields: • **Destination** Add a network object that contains all private networks (including its own private network). • **Source users/User Groups/IP Addresses/FQDN/MAC Addresses** Add a network object that contains all spoke private networks in the star VPN (does not contain its own private network).

Example: Star Site-to-Site IPsec VPN with one hub and two spokes

GATEWAY	ROLE	PRIVATE NETWORK	BYPASS RULE
Spoke IPsec gateway (GS1)	Star spoke	NS1	• Action: Bypass • Source: NH1, NS2 (all other private networks) • Destination: NS1 (its own private network)
Hub IPsec gateway (GH1)	Star hub	NH1	• Action: Bypass • Source: NS1, NS2 (all other private networks) • Destination: NS1, NS2, and NH1 (all private networks)
Spoke IPsec gateway (GS2)	Star spoke	NS2	• Action: Bypass • Source: NH1, NS1 (all other private networks) • Destination: NS2 (its own private network)

Viewing Troubleshooting Logs

Purpose: Use the IPsec troubleshooting logs to view activity over IPsec VPN tunnels.

Location: Gateways > (gateway name) > Site-to-Site VPN > Troubleshooting

Procedure

1. Review the troubleshooting logs.

Updates

Using the **Updates** screen, you can easily perform Cloud Edge gateway updates that Trend Micro releases from time to time. The **Update** screen provides the following two sections:

- **Available Updates**: If there are any updates available for your gateway, it will be available in this section. To know more about any available updates, click the **readme** link to view the readme file.
- **Installed Updates**: The updates that are already installed are displayed in this section.

Updating the Cloud Edge Gateway

Purpose: Install Cloud Edge gateway updates.

Location: Gateways > (gateway name) > Updates

Procedure

1. Click **Update Now** under the **Action** column for the available update that you want to install.

   To know more about the current update, click the **Readme** link.

   Note

   If the update has any dependency on any other file, Cloud Edge will install that file automatically.

   Important

   For HA groups, an update (manual or scheduled) occurs in a specific order — the standby gateway is updated first, followed by a failover from the primary to the secondary. After failover completes, the primary is updated. Then another failover returns the primary to active status. There is no network outage during this process.

   If a gateway is part of an HA group and one of the gateways is offline or the HA group is in a split brain status, manual updates are disallowed to the HA group gateways.

Managing Network Access Control

You can manage network access control to provide endpoint protection using Cloud Edge Cloud Console.

- Cloud Edge integrates with Worry Free Business Security Services (WFBSS) to provide a compliance check for WFBSS endpoints. Cloud Edge can provide network access control for WFBSS endpoints who have an out-of-date WFBSS Security Agent pattern or who do not have the WFBSS Security Agent installed.

  See *WFBSS Endpoint Protection on page 6-149*.

- Cloud Edge provides security services by providing compliance checks for endpoints to see if C&C callbacks above the configured threshold have been detected. Cloud Edge can provide network access control for endpoints who have exceeded the threshold.

  See *Suspicious Endpoints on page 6-157*.

WFBSS Endpoint Protection

Worry Free Business Security Services (WFBSS) provides security services for endpoints. To provide security services, WFBSS customers must install an WFBSS Security Agent on the endpoints. These agents help manage network access control. When an agent has an out-of-date pattern or if an endpoint does not have the agent installed, compliance is not assured.

Cloud Edge WFBSS Endpoint Protection integrates with WFBSS to provide a means for enforcing compliance. Cloud Edge provides a compliance check for endpoints by determining if endpoints have an out-of-date WFBSS Security Agent pattern or if they do not have the WFBSS Security Agent installed. Additionally, Cloud Edge can provide network access control for out-of-compliance endpoints.

Note

WFBSS Endpoint Protection does not support endpoint checking and compliance for IPv6 endpoints.

Enable Compliance Checks

You must enable this feature. The default is disabled.

After you enable the feature, you can specify what action (block or detect) to take for the following two conditions:

- Endpoint has WFBSS Security Agent installed but pattern is out-of-date.
- Endpoint does not have the WFBSS Security Agent installed.

Cloud Edge synchronizes information with Worry Free Business Security Services every hour to get updated information about the latest pattern status for endpoints.

Protection List

Endpoints are not automatically checked for compliance. You must configure protection lists to specify which endpoints to put under compliance protection.

- Endpoints in the protection list are checked to determine if they have installed agents and if so, whether patterns for the installed agents are up-to-date.
- If the endpoints are not in compliance, the configured action is taken.
- You can add MAC addresses or IPv4 addresses (single or range).
- Maximum entries is 256.

Actions

If the compliance check finds that an endpoint in the protection list is non-compliant, Cloud Edge can take one of two courses of action:

- **Block**

  All access to the Internet is blocked.

  Exceptions: Endpoints are not blocked if the traffic/URLs are in the global approved list. Traffic to DNS and DHCP are not blocked.

If an endpoint is blocked by the WFBSS Endpoint Protection function, the client browser is redirected to the WFBSS Endpoint Protection Violation notification page.

Note

If you set the action for endpoints without agents to **Block**, endpoints without agents cannot access the Internet.

If a user attempts to install agent on these endpoints, the following URLs should be added to **Approved List**; otherwise, installation might fail.

- `*.symcb.com/*`
- `*.digicert.com/*`
- `*.affirmtrust.com/*`
- `crl.microsoft.com/*`

In addition, if a user accesses the Trend Micro CLP site on an endpoint without an agent, the following URLs should be added to **Approved List**; otherwise, the following access requests might be affected: `www.google-analytics.com/*` `www.googletagmanager.com/*`

- **Detect**

  Access to the Internet is allowed, but access is logged in the WFBSS Endpoint Protection troubleshooting page along with the reason that the endpoint is out-of-compliance.

Exception List

You can configure an exception list that specifies which endpoints are not under compliance protection. The compliance action is not enforced for endpoints in the exception list.

- You can add MAC addresses or IPv4 addresses (single or range).
- Maximum entries is 256.

Client List

You can use the **Client List** section to view all endpoints detected by the Cloud Edge gateway over the last 24 hours.

- The list is initially empty.
- After you enable WFBSS Endpoint Protection and click on **Apply** to deploy the update to the Cloud Edge gateway, the gateway begins to tabulate information about endpoints that have had traffic pass through the Cloud Edge gateway over the past 24 hours. Cloud Edge displays the resultant list in the **Client List** section.

  For convenience, the endpoints initially detected after WFBSS Endpoint Protection deployment are automatically added to the protection list.
- After initial endpoint detections, you can easily add a listed endpoint to the protection or exceptions lists by clicking on either the **Protection List** or **Exception List** option provided for each listed endpoint.

Managing WFBSS Endpoint Protection

Purpose: Manage WFBSS Endpoint Protection, an integrated solution with Worry Free Business Security Services (WFBSS) that checks the status of WFBSS protection on endpoints and manages network access control for out-of-compliance endpoints.

Location: Gateways > (gateway name) > NETWORK ACCESS CONTROL > WFBSS Endpoint Protection > General

---

Procedure

1. Do the following:
   - Enable WFBSS Endpoint Protection.
   - Select the action to take for endpoints without WFBSS Security Agents. Default is **Detect**.
   - Select the action to take for endpoints with an out-of-date WFBSS Security Agent pattern. Default is **Detect**.

- Add or delete endpoints from the protection list.
- Add or delete endpoints from the exception list.
- View information in the list of endpoints under the Cloud Edge gateway.
- Use the list of endpoints under the Cloud Edge gateway to add specific endpoints to either the protection or exception list.
- Refresh the list of endpoints.

Configuring WFBSS Endpoint Protection

Purpose: Configure to bolster your gateway security against emerging threats.

Location: Gateways > (gateway name) > NETWORK ACCESS CONTROL > WFBSS Endpoint Protection > General

---

Procedure

1. Optionally enable **WFBSS Endpoint Protection**.
2. Choose the action for the following:
   a. **Clients without agent**: **Detect** or **Block**
   b. **Clients with agents using out-of-date patterns**: **Detect** or **Block**
      - **Block**: All access to the Internet is blocked.

        If any client is blocked by the WFBSS Endpoint Protection function, the client browser is redirected to the WFBSS Endpoint Protection violation notification page.
      - **Detect**: Access to the network resource is logged but not blocked. This is the default.
3. Configure the **Protection List**.

   See *Adding Endpoints to the Protection List on page 6-154*.

4. Configure the **Exception List**.

   See *Adding Endpoints to the Exception List on page 6-155*.

5. Click **Apply**.

Adding Endpoints to the Protection List

Purpose: Add endpoints to the protection list for WFBSS Endpoint Protection.

Location: Gateways > (gateway name) > NETWORK ACCESS CONTROL > WFBSS Endpoint Protection > General

---

Procedure

1. Add endpoints to the **Protection List**.

   a. In the **Protection List** section, click **Add**.

      The **Add Protection** screen opens.

   b. Add endpoints to the protection list by specifying the following:

Option	Description
Name	Specify a name that helps you identify information about this entry. **Example**: JSmith **Example**: Office
Address Type	Choose either **IPv4** or **MAC**.
IP/MAC Address	Enter the appropriate information according to the chosen type: • **IPv4**: Enter information as a comma-delimited list. Value can be a single IP address, an IP address range, or a CIDR. **Example**: 192.168.0.1,10.0.0.1-10.0.0.4,10.0.0.8/24 • **MAC**: Enter a single MAC address

Option	Description
	Example: 00:FF:8A:B9:5A:49 **Example**: 00-FF-8A-B9-5A-49

2. Click **Save**.
3. Continue adding endpoints to the protection list as needed.

   You can add up to a maximum of 256 entries to the protection list.

Adding Endpoints to the Exception List

Purpose: Add endpoints to the exception list for WFBSS Endpoint Protection.

Location: Gateways > (gateway name) > NETWORK ACCESS CONTROL > WFBSS Endpoint Protection > General

---

Procedure

1. Add endpoints to the **Exception List**.
   a. In the **Exception List** section, click **Add**.

      The **Add Exception** screen opens.

   b. Add endpoints to the exception list by specifying the following:

Option	Description
Name	Specify a name that helps you identify information about this entry. **Example**: JSmith **Example**: Office
Address Type	Choose either **IPv4** or **MAC**.
IP/MAC Address	Enter the appropriate information according to the chosen type: • **IPv4**: Enter information as a comma-delimited list.

Option	Description
	Value can be a single IP address, an IP address range, or a CIDR. **Example**: 192.168.0.1,10.0.0.1-10.0.0.4,10.0.0.8/24 • **MAC**: Enter a single MAC address **Example**: 00:FF:8A:B9:5A:49 **Example**: 00-FF-8A-B9-5A-49

2. Click **Save**.
3. Continue adding endpoints to the exception list as needed.

   You can add up to a maximum of 256 entries to the exception list.

Viewing the WFBSS Endpoint Protection Client List

Purpose View all endpoints currently under the Cloud Edge gateway that are checked for WFBSS Security Agent compliance.

Location: Gateways > (gateway name) > NETWORK ACCESS CONTROL > WFBSS Endpoint Protection > General

---

Procedure

1. View information for all endpoints in the table:
   - Host name
   - IP address
   - MAC address
   - Whether agent is installed
   - If installed, whether the agent has an out-of-date pattern
   - Operating system (example: Windows 10)
2. (Optional) Refresh the list by clicking on **Refresh**.

3. (Optional) Add an endpoint to the protection list by clicking on **Protection List** for the selected endpoint.
4. (Optional) Add an endpoint to the exception list by clicking on **Exception List** for the selected endpoint.

Troubleshooting WFBSS Endpoint Protection

Purpose View general troubleshooting information when using WFBSS Endpoint Protection.

Location: Gateways > (gateway name) > NETWORK ACCESS CONTROL > WFBSS Endpoint Protection > Troubleshooting

Procedure

1. Do the following to troubleshoot WFBSS Endpoint Protection:
   - View individual log entries to determine why a client has been blocked.
   - Click **Refresh** to update the logs.

Suspicious Endpoints

Suspicious Endpoints provides security services for endpoints. Configuring Suspicious Endpoints provides network access control for endpoints on which C&C callbacks above a configured threshold are detected.

Note

- Suspicious Endpoints does not provide endpoint checking and compliance for IPv6 endpoints.
- If a NAT device or a proxy is between the Cloud Edge gateway and the endpoint, Cloud Edge is not able to detect the client's real IP address, and instead, Cloud Edge counts the C&C callback event to the NAT/proxy device. Therefore, any future traffic from the NAT/proxy device that triggers a violation will be blocked or monitored, depending on the configured settings. This behavior might not be as expected.

What You Can Specify After Enabling Suspicious Endpoints

You must enable this feature. The default is disabled.

After you enable the feature, you can specify what action (block or monitor) to take if Cloud Edge detects C&C callback detections on the endpoint that are above the configured threshold.

The threshold is reached when a specified number of events is detected over a specified time period. You can configure the number of events and the time period:

- Events (50 default)

  Range: 1-1000

- Time Period (default 1 hour)

  Valid time periods: 30 minutes, 1 hour, 6 hours, 12 hours, 1 day

Cloud Edge synchronizes information with the endpoints periodically to get updated information.

Actions You Can Specify

If the compliance check finds that an endpoint violated the threshold settings, Cloud Edge can take one of two courses of action:

- **Block**

All access to the Internet is blocked.

Exceptions: Endpoints are not blocked if the traffic/URLs are in the global approved list. Traffic to DNS and DHCP are not blocked.

If an endpoint is blocked, the client browser is sent the Suspicious Endpoints Violation notification page.

Note

If you set the action to **Block**, suspicious endpoints cannot access the Internet.

- **Monitor**

  Access to the Internet is allowed, but the suspicious endpoint is added to the violation list.

How You Can Use the Violation List

You can use the **Violation List** section to view information about all endpoints with suspicious activity detections that are above the threshold.

- Cloud Edge begins to populate the violation list with endpoints that exceed the threshold after enabling Suspicious Endpoints.
- If the action is set to **Block**, you can exempt specific endpoints in the violation list from being blocked by clicking on **Dismiss** in the appropriate row.

How You Can Use the List on the Troubleshooting Page

If the action is set to **Block**, you can view the list on the troubleshooting page to see which endpoints are blocked because of violations.

If the Cloud Edge gateway is offline, you view the list, but cannot perform operations, such as **Dismiss**.

Managing Suspicious Endpoints

Purpose: Manage Suspicious Endpoints, a security service that provides compliance and network access control for risky endpoints.

Location: Gateways > (gateway name) > NETWORK ACCESS CONTROL > Suspicious Endpoints > General

Procedure

1. Do the following:
   - Enable **Suspicious Endpoints**.
   - Select the action to take for out-of-compliance endpoints. Default is **Monitor**.
   - Set the threshold for the number of C&C callback events that can occur within the specified time period before the action is triggered. The default is 50 events over 1 hour.
   - Use the violation list to view information about endpoints that are in violation of the endpoint policy.
   - If you do not want endpoints to be blocked, remove the selected endpoints from the violation list.

Configuring Suspicious Endpoints

Purpose: Configure Suspicious Endpoints to bolster your gateway security against emerging threats.

Location: Gateways > (gateway name) > NETWORK ACCESS CONTROL > Suspicious Endpoints > General

Procedure

1. Optionally enable **Suspicious Endpoints**.
2. Choose the action to take for endpoints in violation of the policy:
   - **Block**: All access to the Internet is blocked.

     If any endpoint is blocked by the Suspicious Endpoints function, the client browser is sent the Suspicious Endpoints Violation notification page and the incident is logged in the troubleshooting screen.

- **Monitor** (default): Access to the Internet is allowed, but the suspicious endpoint is added to the violation list.

3. Configure the threshold for C&C callbacks:
   a. Enter the number of threshold events (default: 50).

      The range is 1 to 1000.

   b. Enter the time period within which the number of threshold events are counted (default: 1 hour).

      Supported values are **30 minutes**, **1 hour**, **6 hours**, **12 hours**, and **1 day**.

4. Click **Apply**.

Viewing the Suspicious Endpoints Violation List

Purpose View all endpoints with suspicious activity.

Location: Gateways > (gateway name) > NETWORK ACCESS CONTROL > Suspicious Endpoints > General

---

Procedure

1. View information for all endpoints with violations:
   - Host name
   - IP address
   - Triggering time
2. (Optional) Remove selected endpoints from the violation list by clicking on **Dismiss**.

Troubleshooting Suspicious Endpoints

Purpose View general troubleshooting information when using Suspicious Endpoints.

Location: Gateways > (gateway name) > NETWORK ACCESS CONTROL > Suspicious Endpoints > Troubleshooting

Procedure

1. Do the following to troubleshoot Suspicious Endpoints:
   - View individual log entries to determine which endpoints have been blocked for suspicious activity.
   - Click **Refresh** to update the logs.

Device Recognition

In Cloud Edge Cloud Console you can discover, view, and manage endpoint devices. In addition, Cloud Edge can scan endpoint devices for vulnerabilities.

Cloud Edge automatically detects new endpoint devices in your network. It may take several minutes before Cloud Edge detects a new endpoint device in your network. To discover endpoint devices, Cloud Edge actively sends packets to probe for new endpoint devices and passively detects endpoint devices that send network traffic through Cloud Edge.

Each Cloud Edge gateway can support a maximum of 2000 endpoint devices.

Use the following screens under **Gateways** > **(gateway)** > **Device Recognition** to perform these functions:

- Endpoint Devices: This screen shows a filterable list of endpoint devices, the severity of each endpoint device, and the amount of vulnerabilities on each endpoint device. For more details, see *Endpoint Devices on page 6-163*.
- General Settings: This screen provides the option to manually initiate or schedule vulnerability scans as well as set the recognition mode. For more details, see *General Scan Settings on page 6-166*.
- Endpoint Device Details: This screen shows detailed device information and vulnerabilities on the device. For more details, see *Endpoint Device Details on page 6-164*.

While most functions are performed under **Device Recognition**, the following elements are also related to endpoint device management:

- Device Categories Requiring Attention: Located in the **Device Map & Security** tab of the **Dashboard**, this widget shows the network topology as well as the amount of endpoint devices with vulnerabilities, Internet security, and policy enforcement.
- Policy Rules: Located in **Polices**, this screen provides the option to deploy a policy to an endpoint device based on the endpoint device category.

Endpoint Devices

The **Endpoint Devices** screen contains a table with the following information about endpoint devices discovered in your network by Cloud Edge:

- **Name**: The name of the device.
- **Device Category**: The device category that is automatically assigned by Cloud Edge.
- **IP Address**: The IPv4 and IPv6 address of the device.
- **MAC Address**: The MAC address of the device.
- **Severity**: The severity level based on the vulnerabilities and weak passwords discovered on the device.

  Cloud Edge shows the following severity levels:

  - Green: The device may have open ports. The device has no detected weak passwords and no detected vulnerabilities.
  - Yellow: The device has weak passwords and may have open ports. The device has no detected vulnerabilities.
  - Red: The device has vulnerabilities. The device may have weak passwords and open ports.
- **Vulnerabilities**: The amount of vulnerabilities and weak passwords on the device.

Viewing Endpoint Devices

Purpose: View endpoint devices discovered on your network by Cloud Edge.

Location: Gateways > (gateway) > Device Recognition > Endpoint Devices

Procedure

1. (Optional) Click on a device name to view more device information and vulnerabilities.
2. (Optional) Above the table, select a range of time to view the history of discovered devices during that time period.
3. (Optional) Above the table, click the refresh button to refresh the Cloud Edge Cloud Console screen.

   Note

   The information from the Cloud Edge gateway is not refreshed.

4. (Optional) On the left side of the table, select specific device categories to filter the devices shown in the table.
5. Click on a column header to sort the table by that column.

   Note

   By default, the table is sorted by **Severity** and then by **Name**.

6. (Optional) At the bottom of the table, use the pagination controls to navigate the multiple pages of the table.

Endpoint Device Details

The endpoint device details screen contains the following details about endpoint devices discovered in your network by Cloud Edge:

- Device Information
  - Name: The name of the device.

- Device Category: The device category that is automatically assigned by Cloud Edge.
- IP Address: The IPv4 and IPv6 address of the device.
- MAC Address: The MAC address of the device.
- Hostname: The hostname of the device.
- Brand: The brand of the device.
- Model: The model of the device.

- Vulnerability Information

Note

By default, the vulnerability and weak password scan is disabled. To enable the scan, see *General Scan Settings on page 6-166*.

- CVE IDs: A list of vulnerabilities detected on the device.

Note

Click on a vulnerability to get more information about the vulnerability, such as the possible risks, how to prevent the vulnerability, and where to get more information.

- Weak Passwords: A list of applications with weak passwords detected on the device.

  Cloud Edge scans only the following application passwords: SSH, FTP, and Telnet.

Note

Click on an application name to get more information about the weak password, such as the possible risks, and how to prevent the weak password.

- Open Ports: A list of open TCP/UDP ports and the applications typically associated with the ports.

  Cloud Edge scans only the following ports:

  - TCP: 21, 22, 23, 53, 80, 135, 139, 443, 445, 515, 554, 631, 2869, 5000, 5357, 5432, 7777, 8008, 8080, 8192, 9100, 9700, 12345, 49152, 49153, 49154, 49155, 62078
  - UDP: 53, 67, 68, 69, 111, 123, 137, 138, 161, 427, 500, 1022, 1023, 1026, 1029, 1812, 1900, 3702, 4500, 5353

Viewing an Endpoint Device

Purpose: View details and vulnerabilities related to an endpoint device on your network by Cloud Edge.

Location: Gateways > (gateway) > Device Recognition > Endpoint Devices > (device)

Procedure

1. (Optional) Under **CVE IDs** or **Open Ports** click **Show All** to view additional items.
2. (Optional) Click on a CVE ID or weak password to view more details.
3. (Optional) Click **Back to All Devices** to return to the list of all devices.

General Scan Settings

Cloud Edge can scan endpoint devices for vulnerabilities based on the CVE list, as well as weak passwords. In addition, Cloud Edge can use advanced recognition mode to identify open ports and identify the endpoint device category.

After running a vulnerability scan, the scan results are shown on the following screens:

- Endpoint Devices: This screen shows a filterable list of endpoint devices, the severity of each endpoint device, and the amount of vulnerabilities

on each endpoint device. For more details, see *Endpoint Devices on page 6-163*.

- Endpoint Device Details: This screen shows detailed device information and vulnerabilities on the endpoint device. For more details, see *Endpoint Device Details on page 6-164*.
- Device Categories Requiring Attention: Located in the **Device Map & Security** tab of the **Dashboard**, this widget shows the network topology as well as the amount of endpoint devices with vulnerabilities, Internet security, and policy enforcement.

Configuring General Scan Settings

Purpose: Run or schedule a vulnerability scan, as well as configure the recognition mode for discovered endpoint devices.

Location: Gateways > (gateway) > Device Recognition > General Settings

CAUTION!

By default, the scheduled vulnerability and weak password scan is disabled. Be aware that security software and devices may detect the scan as a security event.

Procedure

1. (Optional) For **Recognition Mode**, toggle the following options.
   - **Advanced**
   - **Standard**

Note

Advanced recognition mode uses an active scan to help identify the category and open ports of an endpoint device. Selecting standard recognition mode may reduce the accuracy of the device category identification.

2. (Optional) Click **Scan Now** to run an on-demand vulnerability scan.
3. (Optional) For **Enable**, select **On** to enable a scheduled vulnerability scan, or **Off** to disable the scan.
   a. If you selected **On**, then select the scan frequency.

Managing IP Address/FQDN Objects

Purpose: Manage address objects by adding, modifying, duplicating, or deleting IPv4, IPv6, and FQDN address objects.

Location: Policies > IDENTITY OBJECTS > IP Addresses/FQDNs

Procedure

1. Do the following:
   - Click **Add** to create a new object.
   - Click the object's name to view or modify settings.
   - Select an object and then click **Duplicate** to copy the object.
   - Select an object and then click **Delete** to delete the object.
2. Configure available settings.
3. Click **Save**.

Adding/Editing IP Address/FQDN Objects

Purpose: Add or edit address objects to configure IPv4 addresses, IPv6 addresses, or FQDN objects.

Location: Policies > IDENTITY OBJECTS > IP Addresses/FQDNs > Add / Edit

Procedure

1. Specify a name for the IP address/FQDN object.

2. Select the object type.

   Available types: **IPv4**, **IPv6**, or **FQDN**

   Bridge Mode or **Software Switch**

   Cloud Edge supports IPv6 if the Cloud Edge gateway is running in Bridge Mode or as a Software Switch deployment.

   - You can configure both IPv4 and IPv6 address objects.
   - FQDNs can resolve to either IPv4 or IPv6 addresses.

   Routing Mode

   Cloud Edge does not support IPv6 if the Cloud Edge gateway is running in Routing Mode.

   - You can configure only IPv4 address objects.
   - FQDNs must resolve to IPv4 addresses.

3. Specify the address object as IP addresses (single or comma-delimited), or FQDNs (single or comma-delimited).

   You can specify IP address objects as a single address, a range, or as a Class InterDomain Routing (CIDR) network.

   Examples:

   - `192.168.0.1`
   - `10.0.0.1-10.0.0.4`
   - `10.0.0.8/23`
   - `fd00:1:1111:200::1fff`
   - `fd00:1:1111:200::1000-fd00:1:1111:200::1fff`
   - `fd00:1:1111:200::1000/116`
   - `host.example.com`
   - `example.com`
   - `*.com`

- `*example.com`
- `*.example.com`

Note

As indicated by the previous examples, FQDN objects support usage of the wildcard character (*) for fuzzy match. Be aware to only use the wildcard at the beginning of an FQDN, rather than in the middle or at the end of an FQDN.

4. Click **Save**.

IP Address/FQDN Object Parameters

The following table describes the configurable IPv4 address, IPv6 address, and FQDN (Fully Qualified Domain Name) object parameters.

TABLE 6-6. Address Object Parameters

PARAMETER	DESCRIPTION
Object name	Specify a name that describes the object. This name appears in the address list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Type	Specify one of the following address types: • IPv4 • IPv6 • FQDN For objects used in Bridge Mode and Software Switch deployments, you can configure both IPv4 and IPv6 addresses. Additionally, FQDNs can resolve to either IPv4 or IPv6 addresses. For objects used in Routing Mode deployments, you can configure IPv4 addresses and FQDNs must resolve to IPv4 addresses.

Parameter	Description
Addresses	**IPv4 Address:** Specify the IP address or network using the following notation: • `ip_address` • `ip_address_range` • `ip_address/bitmask` Example: 192.168.1.1 or 192.168.1.1-192.168.1.10 or 192.168.80.0/24 **IPv6 address** Specify the IPv6 address or network using the following notation: • `ipv6_address` • `ipv6_address_range` • `ipv6_address/bitmask (IPv6 CIDR)` Example: 2001:db8:123:1::1 or 2001:db8:123:1::1-2001:db8:123:1::10 or 2001:db8:123:1::/64 **FQDN** Specify an FQDN using the following notation: • `[domain].[tld]` • `[hostname].[domain].[tld]` **Note** FQDN objects support usage of the wildcard character (*) for fuzzy match. Be aware to only use the wildcard at the beginning of an FQDN, rather than in the middle or at the end of an FQDN. Example: • Exact FQDN: `example.com`, or `host.example.com` • Wildcard FQDN: `*.com`, `*example.com`, or `*.example.com`

Parameter	Description
	Note Use the FQDN object type only when configuring policy rules to match source/destination connections.

User Authentication

Authentication Settings

Define authentication source and authentication cache settings for end user authentication.

- User authentication via Hosted User accounts, LDAP accounts, or RADIUS accounts.
- Cloud Edge supports two Authentication Cache Time to Live (TTL) options:
  - Fixed TTL (first hit)—Cache the last time that the user authenticated. Default: 2 hours
  - Last active TTL (last hit)—Cache the last time that the user interacted with Cloud Edge. Default: 2 hours

Configuring Authentication Settings

Purpose: Use authentication settings for authentication source and authentication cache TTL.

Location: Administration > USER AUTHENTICATION > Authentication Settings

---

Procedure

1. Under **Authentication Source**, select one of the following options:
   - **Hosted User**

Users log on with the credentials configured in Cloud Edge. For details, see *Hosted Users and Groups on page 6-173*.

- **LDAP**

  Users log on using LDAP authentication. For details, see *LDAP Settings on page 6-178*.

- **RADIUS**

  Users log on using RADIUS authentication. For details, see *RADIUS Settings on page 6-181*.

2. Under **Authentication Cache**, select one of the following and then select the number of hours for TTL:
   - Fixed TTL (hours)
   - Last Active TTL (hours)
3. Click **Save**.

Note

- Gateways of Cloud Edge 6.0 and later support LDAP for authentication.
- Gateways of Cloud Edge 6.0SP3 and later support RADIUS for authentication.

Hosted Users and Groups

Allow users to log on through VPN or Captive Portal by creating hosted user accounts on Cloud Edge Cloud Console. Optionally organize hosted users into groups to deploy policies that affect all hosted users assigned to the hosted group. VPN and Captive Portal are managed by Cloud Edge Cloud Console.

Cloud Edge Cloud Console synchronizes hosted users and groups to all gateways in the same company. Optionally set policies and perform reports on this synchronized information.

If using hosted users and groups for authentication, disabling a hosted user account blocks that user from logging on to VPN and Captive Portal.

Note

For Cloud Edge gateway models that do not support VPN, you can use hosted users and groups to log on through Captive Portal.

Authentication for users is not supported for IPv6 traffic. This includes any functionality that depends on user authentication such as administrative access, policies that use users for security control, Captive Portal, and so on.

Managing Hosted Users

Purpose: Manage hosted users to allow end users access to resources managed by the gateway.

Location: Administration > USER AUTHENTICATION > Hosted Users & Groups > Hosted Users

Procedure

1. Do the following:
   - Click **Add** to create a new hosted user account.
   - Use **Search** at the top right to locate a user account.
   - Click a hosted user account name to view or modify settings.
   - Select a hosted user and then click **Enable** to allow the account to log on VPN and captive portal.
   - Select a hosted user and then click **Disable** to block the account from logging on VPN and captive portal.
   - Select a hosted user and then click **Delete** to remove the user.

Adding/Editing a Hosted User

Purpose: Add hosted users to allow the user to log on through VPN or Captive Portal.

Location: Administration > USER AUTHENTICATION > Hosted Users & Groups > Hosted Users > Add/Edit User

---

Procedure

1. Enable the hosted user.
2. Specify the user details.
3. Assign the hosted user to existing hosted groups or optionally assign the hosted user to new hosted groups.

   See *Adding/Editing a Hosted Group on page 6-176*.
4. Select the check box to allow the user to change the Captive Portal or VPN Portal password.

   WARNING!

   Do not select this check box if multiple users share the same account. Otherwise, some users may lose access if the password changes.
5. Click **Save**.

Managing Hosted Groups

Purpose: Manage hosted groups to organize hosted users and more efficient control similar hosted user accounts.

Location: Administration > USER AUTHENTICATION > Hosted Users & Groups > Hosted Groups

---

Procedure

1. Do the following:

- Click **Add** to create a new hosted group.
- Use **Search** at the top right to locate a hosted group.
- Click a hosted group account name to view or modify settings.
- Select a hosted group and then click **Enable** to allow all associated hosted users to log on VPN and captive portal.
- Select a hosted group and then click **Disable** to block all associated hosted users from logging on VPN and captive portal.
- Select a hosted group and then click **Delete** to remove the group.

Adding/Editing a Hosted Group

Purpose: Add hosted groups to organize hosted users and deploy policies that affect all hosted users assigned to the hosted group.

Location: Administration > USER AUTHENTICATION > Hosted Users & Groups > Hosted Group > Add/Edit Group

Procedure

1. Specify hosted group details.
2. Click **Save**.

Importing/Exporting Hosted Users and Groups

Purpose: Import or export users and groups to simplify hosted user / host group creation and updates or to create a backup of the configuration.

Location: Administration > USER AUTHENTICATION > Hosted Users & Groups > Import / Export

Procedure

1. Do the following:
   - Import hosted users and group by selecting a CSV file and then clicking **Import**.

Optionally select the check box to overwrite existing users and groups when a conflict exists on import. Keep the check box deselected (default) to maintain the existing hosted user and group information when a duplicate exists.

Note

For details about configuring the import file, see *Preparing the Import File on page 6-177*.

- Export hosted users and groups to a CSV file by clicking **Export**.

Note

Hosted groups with no assigned hosted users will not appear in the exported CSV file. Only hosted groups with assigned hosted users export to the CSV file.

Preparing the Import File

Cloud Edge Cloud Console uses UTF-8 encoding for the CSV file to support more languages. Some spreadsheet programs (Microsoft Excel) may require additional configurations to correctly render CSV files encoded in UTF-8.

Note

Trend Micro recommends using Google Spreadsheet to prepare the hosted users and groups CSV file.

Procedure

1. Create the CSV file in the following format.

```
user name, full name, email address, group, description, enable, password
juser, joe user, joeuser@example.com, group1, user's group, yes, asdg#2345
```

2. Open the CSV file in Microsoft Excel or another spreadsheet program.

3. Go to **File** > **Save As**.
4. In the **Save as type** drop-down menu, select **CSV (Comma delimited) (*.csv)**.
5. Click **Save**.
6. If using Microsoft Excel, click **Yes** to confirm.
7. Open the CSV file in Notepad or another text editor.
8. Go to **File** > **Save As**.
9. Set the **Encoding** drop-down menu to **UTF-8**.
10. Click **Save**.

LDAP Settings

Cloud Edge 6.0 and later gateways support Lightweight Directory Access Protocol (LDAP) for authentication. Using an LDAP server, it is convenient to create user- or group-specific policies with Cloud Edge. Users can authentication through Captive Portal or VPN Portal using LDAP. Event logs, reports, and notifications will use your LDAP hierarchies for user identification.

Important

The Cloud Edge G3 devices do not support LDAP or Radius.

Cloud Edge supports the following for LDAP:

- Microsoft Windows 2012R2, Windows 2016, and Windows 2019
- OpenLDAP

LDAP Authentication

Use LDAP settings to designate which LDAP servers are integrated with Cloud Edge. Cloud Edge uses the designated LDAP servers to do the following:

- Authenticate users to be identified in the captive portal

- Authenticate users to be identified in the VPN portal
- Use LDAP users or groups as a source in policy rule settings
- Use LDAP users or groups in the **Report By** field when adding or editing reports

To simplify a user's configuration for LDAP, Cloud Edge offers basic and advanced methods for setting up LDAP authentication.

Configuring LDAP Settings

Purpose: Configure LDAP settings for user authentication.

Location: Administration > USER AUTHENTICATION > LDAP Settings

Procedure

1. Select one of the following options:

Basic	Specify the **Domain name**, **User name**, and **Password**. For details, see *Basic LDAP Authentication on page 6-180*.
Advanced	Specify the authentication server, base DN, user name and password used to bind to the LDAP server, add LDAP servers, and select the authentication method. For details, see *Advanced LDAP Authentication on page 6-180*.

Important

The Cloud Edge G3 devices do not support LDAP or Radius.

2. Click **Test LDAP Server Connection**.

Note

After clicking the **Test LDAP Server Connection** button, the system will use the automatically-selected gateway to test the connection. If you are to select a specific gateway, choose from the dropdown list beside **Choose a gateway to sync or test**.

3. Click **Save**.

Basic LDAP Authentication

Cloud Edge provides a simple LDAP configuration for the most widely used LDAP service: Microsoft Active Directory (AD). If you use AD, then input the basic information into Cloud Edge Cloud Console to configure the user identification method: domain name, user name, and password.

With this information, Cloud Edge uses the AD auto-discover tool to obtain the necessary information, including:

- LDAP server addresses
- Base domain name
- Authentication information (Kerberos realm/domain/KDC)

That information populates the **Advanced LDAP Authentication** fields. If an Administrator decides that the auto-discovered result is incorrect or does not work, the Administrator can switch to Advanced Mode and modify the settings.

For LDAP server addresses, the auto-discovery tool determines all of the Domain Controllers for the domain, and Cloud Edge selects and uses the two fastest servers.

Advanced LDAP Authentication

Cloud Edge provides an advanced authentication mode configuration for users familiar with LDAP.

In the advanced mode configuration, users can add, delete, move, and refresh LDAP servers.

Cloud Edge supports the following LDAP server types:

- MS Active Directory
- OpenLDAP

For server relationships, Cloud Edge only supports “fail-over” for the previously mentioned servers. If authentication against the primary server fails, Cloud Edge will attempt to authenticate against a secondary server.

Note

Cloud Edge only supports multiple LDAP servers in same domain for fail-over. Cloud Edge does not support multiple domains for different LDAP servers.

For LDAP authentication method, Cloud Edge supports the following LDAP authentication methods for both MS Active Directory and OpenLDAP:

- Simple
- Kerberos

For both Basic and Advanced Modes, click the **Test LDAP Server Connection** button to verify the ability to authenticate against the configured LDAP servers, and to report the results.

RADIUS Settings

Cloud Edge 6.0SP3 and later gateways support RADIUS for authentication. Users can perform authentication through Captive Portal or VPN Portal using RADIUS. You can also add users and groups in the settings and then create user-specific or group-specific policies with Cloud Edge. Cloud Edge supports the following for RADIUS:

- Network Policy Server on Microsoft Windows 2012R2, Windows 2016, and Windows 2019.
- FreeRADIUS 3.0.13 or later.

RADIUS Authentication

Use RADIUS settings to designate which RADIUS servers are integrated with Cloud Edge. Cloud Edge uses the designated RADIUS servers to do the following:

- Authenticate users to be identified in the captive portal

- Authenticate users to be identified in the VPN portal
- Use RADIUS users or groups as a source in policy rule settings
- Use RADIUS users in the **Report By** field when adding or editing reports

You can configure RADIUS servers and RADIUS users or groups to do RADIUS authentication.

Configuring RADIUS Settings

Purpose: Configure RADIUS settings for user authentication.

Location: Administration > USER AUTHENTICATION > RADIUS Settings > General Settings

---

Procedure

1. Configure the RADIUS settings by specifying the **Primary RADIUS server**, **Port**, and **Secret**.
2. Click **Test Connection** to verify the connection to the RADIUS server.
3. Click **Test User Credentials** to test RADIUS server authentication ability. Specify the username and password in RADIUS server and click **Test**.

   Note

   After clicking the **Test Connection** button, the system will use the automatically-selected gateway to test the connection. If you are to select a specific gateway, choose from the dropdown list beside **Choose a gateway to test**.

4. Configure **Secondary RAIUDS server** (optional).
5. Specify the **RADIUS mapping attribute** (**Vendor-Specific/Filter-Id**).

   Note

   If you select the Vendor-Specific option, you must configure TrendMicro code (6101) as vendor code in the RADIUS server.

6. Click **Save**.

Managing RADIUS Users/Groups

Purpose: Manage RADIUS users/groups to configure users/groups to policies and reports.

Location: Administration > USER AUTHENTICATION > RADIUS Settings > RADIUS Users/Groups

Procedure

1. Do the following:
   - Click **Add** to create a new RADIUS user/group.
   - Use **Search** at the top right to locate a RADIUS user/group name.
   - Click a RADIUS user/group name to view or modify description.
   - Select a RADIUS user/group name and then click **Delete** to remove the user/group.

RADIUS Users and Groups

Users can be authenticated by RADIUS servers, but if you want to configure RADIUS users or groups to policies and reports, you must add the same users or groups on Cloud Edge Cloud Console.

If users don't want to configure Radius users or groups to policies or reports, they only need to configure Radius server settings.

Cloud Edge does not synchronize RADIUS users and groups to the gateway, but it just deploys the related policies.

Synchronizing User Accounts and Groups

The following procedure explains how to immediately synchronize user accounts and groups. You can set policies and generate reports based on this synchronized user and group information. Cloud Edge Cloud Console

automatically synchronizes users and groups from all registered gateways every 8 hours.

The synchronized information includes hosted user and group information configured on Cloud Edge Cloud Console.

Procedure

1. Go to **Administration** > **USER AUTHENTICATION** > **UserID Sync**.
2. Click **Sync All Gateways**.

   Cloud Edge Cloud Console synchronizes user and group information across all registered gateways.

Adding Cloud Console Administrator Accounts

Cloud Edge Cloud Console user accounts can access all registered gateways that belong to the same company. The “Admin” account with Administrator rights is created by default.

Cloud Edge Cloud Console has two user account types:

- **Administrator**
- **Read-only User**

Procedure

1. Go to **Administration** > **USER & ACCOUNTS** > **Accounts Management**.
2. Click **Add** or click the full name of the account to change.

   The **Add/Edit Account** screen appears.
3. Configure available settings.

Option	Description
Full name	Type the full name of the user. This displays at the top-right of Cloud Edge Cloud Console when the user is logged in.

Option	Description
User name	Type the email address of the user. The user types this email address to log on. **Note** After creating a user account, the user name cannot change.
Password	Type the user's password. The password must be at least 8 characters and must contain at least one uppercase letter, one lowercase letter, and one number, and can optionally contain special characters. **Tip** The following tips can help you create effective passwords: • Include special characters in the password • Avoid words found in any dictionary, of any language • Intentionally misspell words • Use phrases or combine words
Confirm Password	Retype the user's password.
Read Only	Select this check box to restrict the user's privileges. The user is an **Administrator** if this check box is unselected. A **Read-only User** can only: • View objects on the **Gateways**, **Policies**, **Analysis & Reports**, and **Administration** tabs • View and modify tabs and widgets in the **Dashboard** • Use the **Change User Profile** screen • Click the **Run Now** button in the **Reports** screen

4. Click **Save**.

Importing the Cloud Edge CA Certificate on Mail Clients

When configuring security profiles, you can enable secure protocols (SMTPS, POP3S, and IMAPS) for email security. When using secure email, Cloud Edge acts as a private Certificate Authority (CA) and dynamically generates digital certificates that are sent to mail clients to complete a secure passage for connections. However, the default CA is not signed by a well-known (trusted) CA on the Internet. In this case, mail clients always generate a pop-up warning message that states "The server you are connected to is using a security certificate that cannot be verified."

To eliminate the warning message and for clients to successfully send and receive email over SSL or startTLS, you can install the Cloud Edge CA certificate on the mail clients.

This section includes procedures for the following:

- *Exporting the CA Certificate on page 6-186*
- *Importing a Cloud Edge CA Certificate for Microsoft Outlook on page 6-187*
- *Importing a Cloud Edge CA Certificate for Mozilla Thunderbird on page 6-188*
- *Importing a Cloud Edge CA Certificate for Mac OS on page 6-189*
- *Importing a Cloud Edge CA Certificate to an Android Device on page 6-190*
- *Importing a Cloud Edge CA Certificate to an iOS Device on page 6-191*

Note

A procedure is not supplied for Foxmail. Secure email scan for Foxmail is not supported on this version of Cloud Edge.

Exporting the CA Certificate

You must first export the Cloud Edge CA certificate before installing it on your mail clients.

Procedure

1. Go to **Administration** > **Certificate Management**.
2. To export the certificate, click **Export**.
3. Save the certificate file (`CloudEdge.crt`) to your computer.

Importing a Cloud Edge CA Certificate for Microsoft Outlook

To provide seamless decryption of secure email for Microsoft Outlook, you must import the Cloud Edge CA certificate to the Microsoft Windows Trusted Root Certification Authorities certificate store.

Procedure

1. Copy the certificate file that you previously exported from Cloud Edge (`CloudEdge.crt`) to the target mail client machine.
2. On the target, double-click the certificate file to open it.
3. Click **Install Certificate**.

   The **Certificate Import Wizard** screen appears.
4. Select **Place all certificates in the following store** and click **Browse**.

   The **Select Certificate Store** screen appears.
5. Select the **Trusted Root Certification Authorities** store and click **OK**.
6. Click **Next** and select **Yes** on the **Security Warning** page.

   The certificate import was successful if the following prompt is displayed: “The import was successful.”
7. Restart Microsoft Outlook.

   Sending and receiving email will no longer generate certificate warnings.

Importing a Cloud Edge CA Certificate for Mozilla Thunderbird

To provide seamless decryption of secure email for Mozilla Thunderbird, you must import the Cloud Edge CA certificate to the Thunderbird Trusted Certification Authorities certificate store.

Note

This procedure is for Thunderbird 45.7.1. The steps might vary for different versions of Thunderbird. Consult the Thunderbird documentation for your version if necessary.

Procedure

1. Copy the certificate file that you previously exported from Cloud Edge (`CloudEdge.crt`) to the target mail client machine.
2. On the target, open the Thunderbird email application and click the Application menu button (☰).
3. Select **Options** from the pull-down menu.

   The **Options** screen appears.
4. Select **Advanced** and go to the **Certificates** tab.
5. Click **View Certificates**.

   The **Certificates Manager** screen appears.
6. Click the **Authorities** tab.
7. Click **Import**.

   The **Downloading Certificate** screen appears where you will be asked for which purposes you want to trust the Cloud Edge certificate.
8. Select **Trust this CA to identify websites** and **Trust this CA to identify email users**.
9. Click **OK**.

10. Restart the Thunderbird application and open the **Certificates Manager** screen to verify that the Cloud Edge certificate was successfully imported to the trusted CA store.

Importing a Cloud Edge CA Certificate for Mac OS

To provide seamless decryption of secure email for Mac OS, you must import the Cloud Edge CA certificate to the Mac OS Trusted Certification Authorities certificate store.

Note

This procedure is for Mac OS El Capitan 10.11.6. The steps might vary for different versions of Mac OS. Consult the Mac OS documentation for your version if necessary.

During the procedure, the system might ask for admin credentials for authentication purposes.

Procedure

1. Copy the certificate file that you previously exported from Cloud Edge (`CloudEdge.crt`) to the target Mac OS machine.
2. Right click the `CloudEdge.crt` file.
3. Go to **Open With** > **Keychain Access**.

   The **Keychains** screen appears.
4. In the left pane, select the **System** keychain.

   The Cloud Edge certificate is listed in the right pane, but is not trusted by the system.
5. In the right pane, right click on the **Cloud Edge** certificate item and select **Get Info**.

   The **Cloud Edge** certificate information screen appears.
6. Expand the **Trust** information section.

7. In the **When using this certificate** drop-down menu, select **Always Trust**.

   The value for all specific applications listed in this screen automatically changes to **Always Trust**.

8. Close the screen.

   The right pane of the **System** keychain shows that the Cloud Edge certificate is now trusted.

9. Restart the mail client.

   Sending and receiving email will no longer generate certificate warnings.

Importing a Cloud Edge CA Certificate to an Android Device

To provide seamless decryption of secure email on Android devices, you must import the Cloud Edge CA certificate to the Trusted Credentials store.

Note

Steps to install certificates might vary by Android device and version. Consult you Android documentation for more details if necessary.

If you do not want to install the Cloud Edge CA certificate, you can go into the advanced settings of the email account and ensure that **Accept All Certificates** is checked.

Procedure

1. Download the certificate file that you previously exported from Cloud Edge (`CloudEdge.crt`) to the target android device.

   Methods for accessing and downloading the certificate can include via a browser or via an email attachment.

2. On the target android device, go to **Settings** > **Security**.

3. Navigate to and tap **Install from phone storage**.

The **Open from** screen appears.

4. Select **Internal storage** and select the **Downloads** folder.
5. Select and install the Cloud Edge certificate.
   - Use the default credential name.
   - Make sure that **VPN and apps** is selected.
6. Verify that the Cloud Edge certificate import was successful by going to **Settings** > **Security** > **Trusted Credentials** and select the **User Certificates** tab.
7. Restart the mobile mail client in the Android device.

Importing a Cloud Edge CA Certificate to an iOS Device

To provide seamless decryption of secure email on iOS devices, you must import the Cloud Edge CA certificate to the trusted credentials store.

Note

Steps to install certificates might vary by iOS version. Consult you iOS documentation for more details if necessary.

Procedure

1. Use an email account to send and download the certificate file that you previously exported from Cloud Edge (`CloudEdge.crt`).
2. Click the attached certificate file in email.

   The **Install Profile** screen opens and you will be prompted to install the certificate.
3. Tap on **Install**.

   Since this is an untrusted certificate, a warning is displayed.
4. Confirm that you want to install the profile by tapping on **Install**.

The **Profile Installed** verification screen opens, which displays a green **Verified** check mark.

5. Tap on **Done** to close the **Profile Installed** screen.
6. Verify that the Cloud Edge certificate is installed by going to **Settings** > **General** > **Profiles**.

   You must now enable full trust for the Cloud Edge CA certificate.
7. Enable full trust for the Cloud Edge CA certificate by going to **Settings** > **General** > **About** > **Certificate Trust Settings** and sliding **Cloud Edge** to **ON**.
8. Restart the mobile mail client in the iOS device.

Updates

To ensure up-to-date protection against the latest risks, there are several pattern files components you can update. These files contain the binary “signatures” or patterns of known security risks. Cloud Edge uses them to detect known risks as they pass through the Internet gateway. New virus pattern files are typically released at the rate of several per week, while the protocol and IPS pattern files are updated less frequently.

The effectiveness of Cloud Edge depends upon using the latest pattern files. Signature-based virus scanning works by comparing the binary patterns of scanned files against binary patterns of known risks in the pattern files. Trend Micro frequently releases new versions of the virus pattern and spyware pattern in response to newly identified risks. Similarly, new versions of the Phish pattern are released as new phishing URLs are identified.

Cloud Edge uses ActiveUpdate, the Trend Micro utility that enables on-demand or background updates to the virus pattern file and scan engine, spyware or grayware pattern files. ActiveUpdate is a service common to many Trend Micro products. ActiveUpdate connects to the Trend Micro Internet update server to enable downloads of the latest pattern files and engines. ActiveUpdate does not interrupt network services, or require endpoints to restart. Updates are available on a regularly scheduled interval or on demand.

Related information

- *Updateable Components*

Updateable Components

To ensure up-to-date protection against the latest risks, there are several engine and pattern files components you can update.

Pattern files contain the binary “signatures” or patterns of known security risks. Cloud Edge uses them to detect known risks as they pass through the Internet gateway. Some pattern files, for example virus and Smart Scan pattern files, are typically released multiple times per week, while some pattern files, for example, the protocol and IPS pattern files, are updated less frequently.

Anti-Spam Pattern and Engine

The spam pattern helps Cloud Edge identify the latest spam in messages and attachments. The anti-spam engine detects spam in messages and attachments.

C&C Information Pattern

Command & Control (C&C) Information Pattern provides Cloud Edge with enhanced detection and alert capabilities to mitigate the damage caused by advanced persistent threats and targeted attacks.

IntelliTrap Pattern and Exceptions

IntelliTrap detection uses a scan option in the Trend Micro’s virus scanning engine with IntelliTrap pattern (for potentially malicious files) and IntelliTrap Exception pattern (as an allowed list). Cloud Edge uses the IntelliTrap option and patterns available for detecting malicious compressed files, such as bots in compressed files. Virus writers often attempt to circumvent virus filtering by using different file compression schemes. IntelliTrap provides a heuristic evaluation of compressed files to help reduce the risk that a bot or any other malicious compressed file might cause to a network.

IPS Pattern

Cloud Edge uses the IPS pattern file to block IPS vulnerabilities. If a comparison between patterns suggests that a network connection has a vulnerability, Cloud Edge proceeds with the configured action.

Spyware Pattern

As new hidden programs (grayware) that secretly collect confidential information are written, released into the public, and discovered, Trend Micro collects their tell-tale signatures and incorporates the information into the spyware/grayware pattern file.

Virus Scan Engines and Pattern

The virus scan engine analyzes each file's binary patterns and compares them against the binary information in the pattern files. If there is a match, the file is determined to be malicious.

Smart Scan Agent Pattern

The Smart Scan agent pattern is the local part of the Smart Scan advanced malware scanning solution. If Smart Scan is enabled Cloud Edge sends content to the Smart Scan server for scanning. The Smart Scan agent pattern is the handler portion of the Smart Scan solution. The Smart Scan pattern (located on the Smart Scan server) is updated frequently while the local Smart Scan agent pattern is updated once per day.

Scheduling Updates

Schedule updates to ensure that Cloud Edge provides security from the latest threats. Trend Micro frequently releases new versions of the virus pattern and spyware pattern in response to newly identified risks.

Procedure

1. Go to **Administration** > **Scheduled Updates**.
2. Click **On** to enable scheduled updates.

- **Component Updates**
- **Firmware & Factory Reset Version Updates**

Note

The scheduling for automatic factory reset version update periods shares the same scheduling pattern as the automatic firmware update periods.

3. Select the frequency to run the update.

Note

When selecting the frequency, the time specified to run the scheduled update is the local time on the Cloud Edge gateway.

4. Click **Save**.
5. Wait several minutes for the updates to take effect.
6. Click **Deploy All** to make changes effective.

Manual Updates

Schedule updates to ensure that Cloud Edge provides security from the latest threats. Trend Micro frequently releases new versions of the virus pattern and spyware pattern in response to newly identified risks.

Procedure

1. Go to **Gateways**.
2. Right-click the gateway and select **Update**.

   The **Manual Update** screen appears.
3. Select the components to update.
4. Click **Update**.

Chapter 7

Cloud Edge On-Premises

This chapter explains how to deploy the Cloud Edge gateway in customer networks and provides information about basic management operations.

Deployment

Safety Guidelines

Follow these guidelines to ensure general safety:

- Keep the chassis area clear and dust-free during and after installation.
- Do not wear loose clothing or jewelry that could get caught in the chassis. Fasten your tie or scarf and roll up your sleeves.
- Wear safety glasses if you are working under any conditions that might be hazardous to your eyes.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Disconnect all power by turning off the power and unplugging the power cord before installing or removing a chassis or working near power supplies.
- Do not work alone if potentially hazardous conditions exist.
- Never assume that power is disconnected from a circuit; always check the circuit.

Package Contents

You must verify contents when you open the Cloud Edge gateway package. You can use the Quick Start Card included in the package to verify the contents.

Deployment Modes

Deployment Mode Overview

The Cloud Edge gateway has three deployment configurations: Routing Mode, Bridge Mode, and Software Switch (a variation of Bridge Mode). These configurations control how the Cloud Edge gateway routes network packets and interfaces perform forwarding decisions.

TABLE 7-1. Deployment Modes

DEPLOYMENT MODE	PURPOSE
Bridge Mode	If the deployment mode is set to Bridge Mode, you can deploy either a Bridge Mode or a Software Switch configuration. **Bridge Mode configuration** The Cloud Edge unit is invisible to the network and acts as a layer 2 bridge between network devices (switch, router, firewall, or endpoints), transparently scanning network traffic in both directions. All of its interfaces are on the same subnet. You only have to configure the bridge interface (br0) with an IP address that can provide connectivity to the Internet. The bridge interface (br0) is used to connect to Cloud Edge Cloud Console, to provide Cloud Message Scan services, and to provide access to other cloud services such as Trend Micro ActiveUpdate. You would typically use a Bridge Mode deployment on a private network behind an existing firewall or behind a router. Bridge Mode is the simplest way to deploy Cloud Edge into an existing network topology and does not require client, router, or switch modifications. **Software Switch configuration** Software Switch is a variation of Bridge Mode (mode switch is set to Bridge). Cloud Edge acts as a software switch between an upstream network device (switch, router, or firewall) and endpoints. The Cloud Edge gateway scans all traffic that passes through it for malware. Similar to Bridge Mode, all of its interfaces are on the same subnet and you can configure only the bridge interface (br0) with an IP address. The bridge interface (br0) provides connectivity to the Internet. However, with a Software Switch deployment, all ports besides the uplink port are connected directly to endpoints such as clients, servers, and Wi-Fi access routers. You would typically use a Software Switch deployment when Cloud Edge operates on a private network behind an existing firewall or router and you want to connect endpoints directly to the Cloud Edge gateway. **Bridge Mode (With Switch Chipset)**

Deployment Mode	Purpose
	Cloud Edge gateways with hardware switch chipset offer additional benefits. In Bridge Mode, the gateway functions as a hardware switch with seven LAN ports that can be connected directly to endpoints such as clients, servers, and Wi-Fi access routers. Cloud Edge gateways with hardware switch chipset provide full security functionality on Internet traffic. Additionally, you can configure the level of security provided on intranet traffic: high security, balanced security, or high speed security. You would typically deploy a Cloud Edge gateway as a hardware switch when Cloud Edge operates on a private network behind an existing firewall or router and you want to connect multiple endpoints directly to the Cloud Edge gateway.
Routing Mode	The Cloud Edge unit is visible to the network and acts as a layer 3 routing device – a gateway between a private network and the Internet. It hides the IP addresses of the private network by using NAT with traffic stream scanning capabilities. Deploying in Routing Mode requires configuring at least two network interfaces: one for internal use and one for external use. All of its interfaces are on different subnets, enabling you to have a single IP address available to the public Internet. Each interface connected to a network must be configured with an IP address valid for that network. Cloud Edge can perform network address translation before it sends and receives packets to the destination network and works as a router. Cloud Edge in Routing Mode also provides Point–to–Point Protocol over Ethernet (PPPoE) functionality to support dialing to the ISP through asymmetric digital subscriber line (ADSL). You would typically use a Routing Mode deployment when the Cloud Edge unit is deployed as a gateway between private and public networks. **Wireless Networks in Routing Mode** For Cloud Edge gateway models that support wireless access, you can configure a main wireless access point and a guest wireless access point. Full security scanning is provided for the wireless networks.

Deployment Mode	Purpose
	For Cloud Edge gateway models running Cloud Edge 6.0 SP1 or later in Routing Mode, you can configure an high-availability group (HA group) to avoid a single point of failure and to increase network availability.

Note

Certain gateway features that rely on layer 3 networking such as VPN or NAT are not available in Bridge Mode or Software Switch.

All deployment configurations protect your network by supporting all security features deployed by policies.

Routing Mode Network Topology

In Routing Mode, Cloud Edge is visible on the network and acts as a layer 3 routing device with traffic stream scanning capabilities.

The following figure depicts a typical network topology for Cloud Edge in Routing Mode:

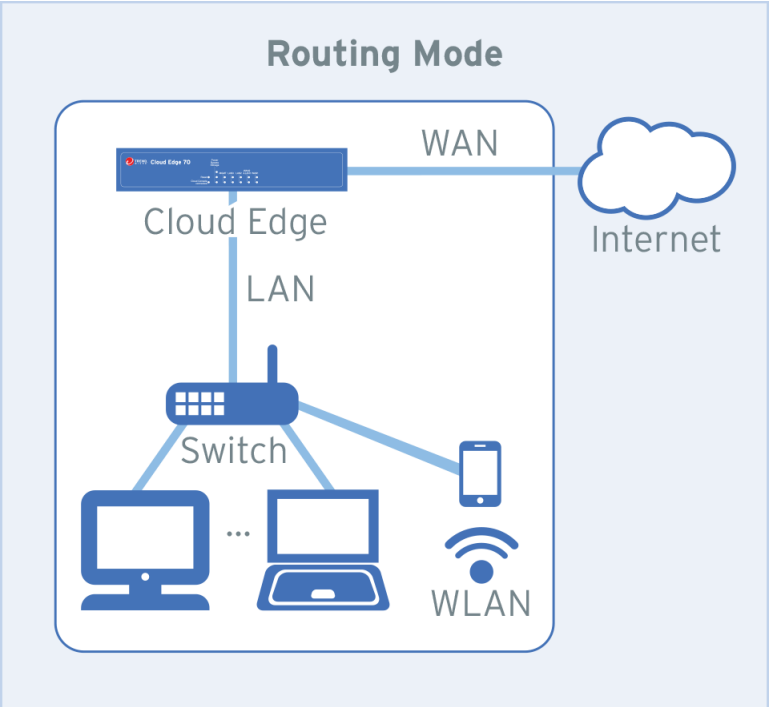


FIGURE 7-1. Cloud Edge in Routing Mode

In Routing Mode, the Cloud Edge gateway operates as a layer 3 device that is a gateway between private and public networks and works as a router. Each connected interface is assigned an IP address. All the interfaces are on different subnets, enabling you to have a single IP address available to the public Internet. Cloud Edge can perform network address translation (NAT) before it sends and receives packets to the destination network.

You must connect the WAN interface to the Internet to enable the Cloud Edge gateway to register with Cloud Edge Cloud Console. The WAN connection is also used for Cloud Message Scan (CMS), to manage Cloud Edge for

scheduled pattern updates, and to leverage the real-time security information power of the Trend Micro™ Smart Protection Network™ in the cloud.

Cloud Edge also provides Point–to–Point Protocol over Ethernet (PPPoE) functionality to support dialing to the ISP through asymmetric digital subscriber line (ADSL).

Cloud Edge Gateways with Hardware Switch Chipset

Cloud Edge gateways with hardware switch chipset can be configured in Routing Mode using the same setup and configuration as is used to set up all other Cloud Edge models.

Wireless Networks in Routing Mode

The following figure depicts a typical network topology for a Cloud Edge gateway with wireless network access in Routing Mode:

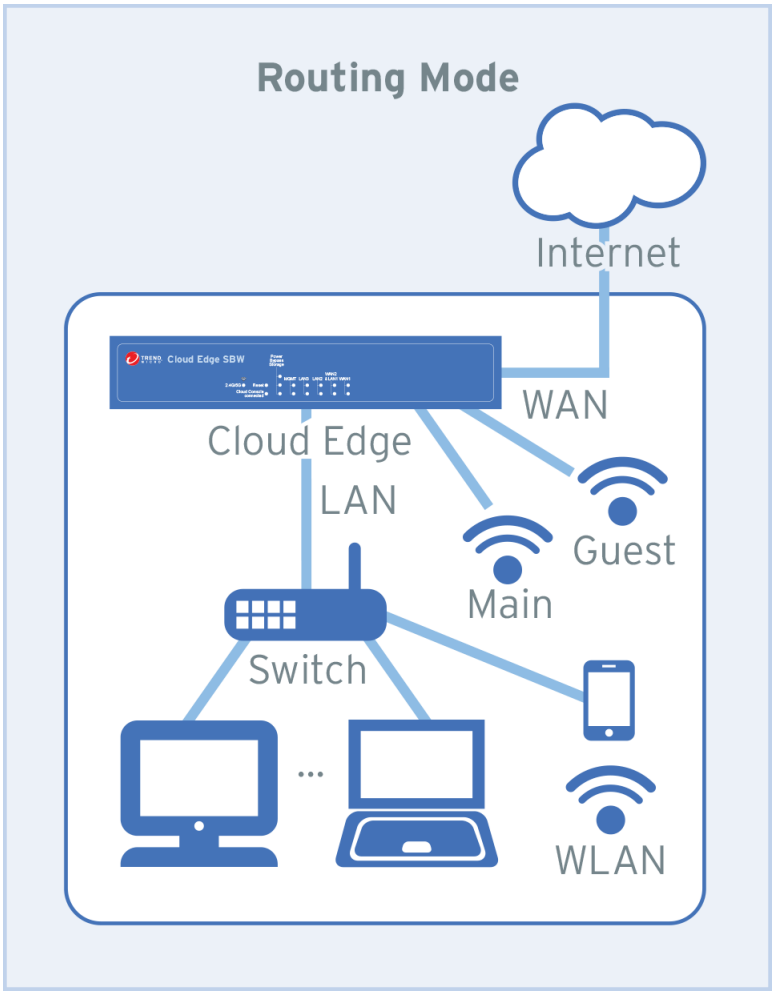


FIGURE 7-2. Cloud Edge with wireless access in Routing Mode

For Cloud Edge gateways that support wireless network access, you can configure a main wireless access point and a guest wireless access point. Full security functionality is provided for the wireless networks. You can control wireless network access using MAC address filtering. You can configure other services on the wireless networks such as DHCP services, bandwidth control, NAT, and VPNs.

HA Groups in Routing Mode

For Cloud Edge gateway models running Cloud Edge 6.0 SP1 or later in Routing Mode, you can configure an high-availability group (HA group) to avoid a single point of failure and to increase network availability.

You must configure HA groups using the Cloud Edge Cloud Console. For information about this topology and how to configure this deployment, see *Creating an HA Group on page 6-16*.

Bridge Mode Network Topology

In Bridge Mode, Cloud Edge acts as a layer 2 bridge between network devices (switch, router, or firewall). The Cloud Edge gateway scans all traffic that passes through it for malware.

The following figure depicts a typical network topology for Cloud Edge in Bridge Mode:

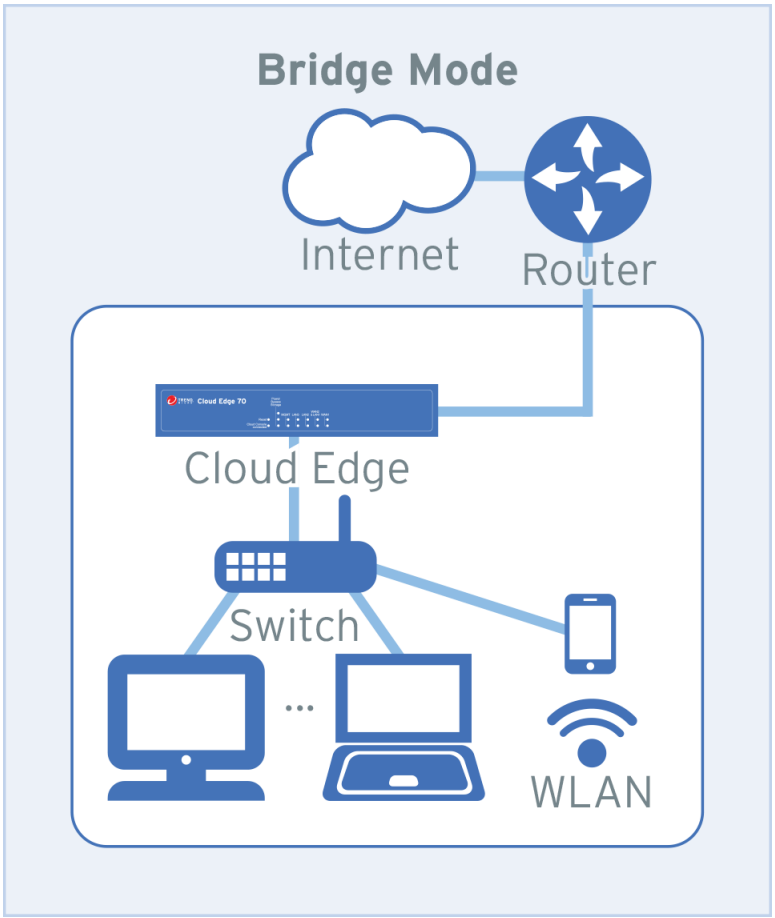


FIGURE 7-3. Cloud Edge in Bridge Mode

To configure Bridge Mode, you must connect cables to the WAN interface and LAN1 interface. Similar to using a network bridge, the WAN and LAN interfaces must be on the same subnet.

Since the Cloud Edge gateway in Bridge Mode relies on layer 2 networking, connected interfaces are not assigned IP addresses. However, you must configure an IP address on the bridge interface (br0) to register the Cloud Edge gateway with Cloud Edge Cloud Console. The IP address assigned to the bridge interface (br0) is used for cloud-based Cloud Message Scan (CMS), to manage Cloud Edge for scheduled pattern updates, and to leverage the real-time security information power of the Trend Micro™ Smart Protection Network™ in the cloud.

Configure Bridge Mode when Cloud Edge operates on a private network behind an existing firewall or router so that Cloud Edge can perform all scanning functions transparently.

Software Switch Network Topology

In a Software Switch configuration, Cloud Edge acts as a software switch between network devices (switch, router, or firewall) and end points. Configure a Software Switch deployment when Cloud Edge operates on a private network behind an existing firewall or router and you want to connect end points directly to the Cloud Edge gateway.

When configured as a Software Switch, the Cloud Edge gateway scans all traffic that passes through it for malware.

The following figure depicts a typical network topology for Cloud Edge in a Software Switch configuration:

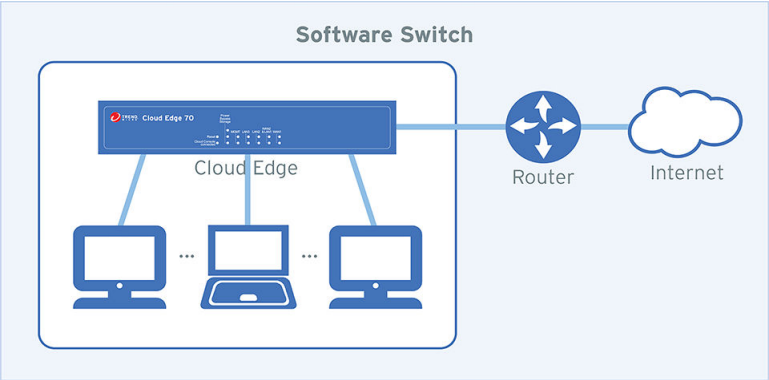


FIGURE 7-4. Cloud Edge in Software Switch Configuration

- The Cloud Edge deployment switch is set to **Bridge**; however, the deployment steps that you use will configure the gateway as a software switch instead of a transparent bridge.
- To configure the Cloud Edge gateway as a software switch, you must connect cables to a minimum of three ports.
  - The WAN interface and LAN1 interface are required.
  - You must connect at least one of the LAN2 or LAN3 ports.
  - You can connect both LAN2 and LAN3 if desired.
- You must be mindful of network topology when connecting cables.
  - The interfaces must be on the same subnet.
  - The WAN interface is connected as the uplink to the router (either directly or through an upstream switch).
  - LAN1, LAN2, and LAN3 ports are connected to endpoints on the internal network.
- Since a Software Switch configuration relies on layer 2 networking, connected interfaces are not assigned IP addresses.

- You must configure an IP address on the bridge interface (br0) to register the Cloud Edge gateway with Cloud Edge Cloud Console.

  The IP address assigned to the bridge interface (br0) is used for cloud-based Cloud Message Scan (CMS), to manage Cloud Edge for scheduled pattern updates, and to leverage the real-time security information power of the Trend Micro™ Smart Protection Network™ in the cloud.

Bridge Mode Network Topology (With Switch Chipset)

The Cloud Edge gateway with hardware switch chipset is a fully functional security device, but can also function as a hardware switch while in Bridge Mode. In Bridge Mode, the gateway serves as a hardware switch between network devices (switch, router, or firewall) and endpoints. The gateway has expanded the number of LAN ports to eight (LAN1-LAN8). LAN1-LAN7 can be directly connected to endpoints. LAN8 is used for bypass functions and is not used to connect to an endpoint.

The following figure depicts a typical network topology for Cloud Edge gateways with hardware switch chipset in Bridge Mode:

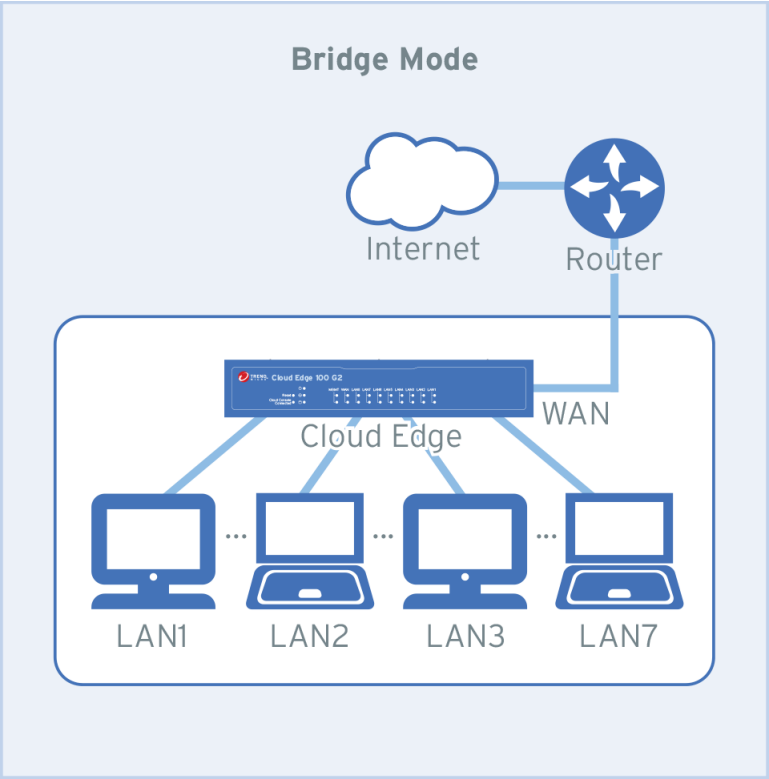


FIGURE 7-5. Cloud Edge with hardware switch chipset in Bridge Mode

Deploy the Cloud Edge gateway with hardware switch chipset in Bridge Mode when Cloud Edge operates on a private network behind an existing firewall or router and you want to connect up to seven endpoints directly to the Cloud Edge gateway.

The gateway scans all traffic that passes through the WAN interface and provides full security functionality.

The security provided for internal traffic (LAN to LAN traffic) depends on the security mode that you choose when configuring the gateway.

To configure Bridge Mode, you must connect cables to the WAN and LAN1 interfaces. You can additionally connect cables from LAN2-LAN7 to internal endpoints. The WAN and LAN interfaces must all be on the same subnet.

Since the gateway in Bridge Mode relies on layer 2 networking, connected interfaces are not assigned IP addresses. However, you must configure an IP address on the virtual switch interface (sw0) to register the Cloud Edge gateway with Cloud Edge Cloud Console. You also configure additional switch related settings on the switch interface (sw0).

The IP address assigned to the switch interface (sw0) is used for cloud-based Cloud Message Scan (CMS), to manage Cloud Edge for scheduled pattern updates, and to leverage the real-time security information power of the Trend Micro™ Smart Protection Network™ in the cloud.

Even though the WAN and LAN1-LAN8 interfaces are L2 interfaces that do not have IP addresses, there are a number of interface setting that you can configure that pertain to a hardware switch configuration.

Bypass Ports on Gateways with Hardware Switch Chipset

The Cloud Edge gateway with hardware switch chipset provides enhanced bypass functionality on certain ports that allows traffic to traverse the gateway even during events that can prevent scanning such as reboots, system issues, and power off. Before you configure your Cloud Edge gateway with hardware switch chipset, you should understand how the bypass ports work so that you can choose which ports to use for specific business needs.

There are two bypass modes:

- Bypass Mode 1:

  The gateway bypasses all traffic between WAN and LAN1-LAN7. LAN8 is unavailable during bypass. After the gateway is powered on, Bypass Mode 1 works if necessary during system failure, system on boot, upgrades, and so on. The gateway must be powered on for Bypass Mode 1 to be effective.

  When the gateway is powered off, Bypass Mode 1 does not work.

This mode is implemented by gateways with hardware switch chipset, so other Cloud Edge models do not have this bypass mode.

- Bypass Mode 2:

  The gateway bypasses traffic between WAN and LAN1.When the gateway is powered off, Bypass Mode 2 still works.

  This is the same bypass action shared with other Cloud Edge models. And if Cloud Edge gateways with the hardware switch chipset are powered on, Bypass Mode 2 does not work because Bypass Mode 1 takes effect.

Refer to the following tables to determine how bypass functions interact in various scenarios:

Power on

Turning Point	→ DC In	→ Boot	→ Install Bypass Module	→ Initialize Complete	
System Phase	DC out	BIOS	OS Start	Initialization	Normal
Bridge Mode	WAN and LAN1 bypass	WAN and LAN1-LAN7 bypass	WAN and LAN1-LAN7 bypass	WAN and LAN1-LAN7 bypass	Bypass off / Scan on
Routing Mode	No bypass	No bypass	No bypass	No bypass	No bypass / Scan on

Reboot

Turning Point	Input Reboot Command	→ Restart	→ Boot	→ Install Bypass Module	→ Initialize Complete	
System Phase	Normal	Preparation	BIOS	OS Start	Initialization	Normal

Bridge Mode	Bypass off / Scan on	WAN and LAN1-LAN7 bypass	WAN and LAN1-LAN7 bypass	WAN and LAN1-LAN7 bypass	WAN and LAN1-LAN7 bypass	Bypass off / Scan on
Routing Mode	No bypass / Scan on	No bypass	No bypass	No bypass	No bypass	No bypass / Scan on

Kernel Panic

Turning Point	Panic	→ WDT Timeout (80s)	→ Restart	→ Boot	→ Install Bypass Module	→ Initialize Complete	
System Phase	Normal	Kernel panic	Power off (0.2s)	BIOS	OS Start	Initialization	Normal
Bridge Mode	Bypass off / Scan on	WAN and LAN1-LAN7 bypass	WAN and LAN1 bypass	WAN and LAN1-LAN7 bypass	WAN and LAN1-LAN7 bypass	WAN and LAN1-LAN7 bypass	Bypass off / Scan on
Routing Mode	No bypass / Scan on	No bypass	No bypass	No bypass	No bypass	No bypass	No bypass / Scan on

Deployment Mode Switch

The Cloud Edge gateway has three deployment types: Routing Mode, Bridge Mode, and Software Switch (a special Bridge Mode configuration). These configurations control how the Cloud Edge gateway routes network packets and interfaces perform forwarding decisions.

The default deployment mode for all Cloud Edge gateway models is Bridge Mode.

A switch on the back panel of the Cloud Edge gateway controls the deployment mode. To change the deployment mode, move the switch to the

desired mode. After changing the deployment mode, you must manually reboot the gateway.

Note

If you want to deploy the Software Switch configuration, set the deployment switch to **Bridge**. This is because the Software Switch configuration is a variation of the Bridge Mode.

FIGURE 7-6. Deployment Mode Switch

Note

The image shown in this manual might differ slightly from your Cloud Edge gateway.

Note

The Cloud Edge 300 does not have a deployment mode switch on the back panel. To change the deployment mode, you must use the on-premises console. To deploy a Software Switch configuration, choose Bridge Mode.

Pre-deployment Checklist

Laptop requirements

TABLE 7-2. Laptop Requirements

REQUIREMENT	DETAILS

Laptop with Ethernet port	A computer that has the following software installed:
	• Adobe™ Flash™ 10 or later
	• Supported web browser
	  • Firefox™ 70 or later
	  • Google™ Chrome 78 or later
	  • Microsoft Edge™ (Chromium) 85 or later

Deployment Requirements

TABLE 7-3. Bridge Mode Requirements

REQUIREMENT	DETAILS
Ethernet cables (3 cables)	Connect to the MGMT port (management) and the WAN and LAN1 data ports.
IP addresses (1 address)	• Obtain the information about connecting to the WAN from your Internet Service Provider (ISP): DHCP or Static. You will use this information to configure the bridge interface (br0) or switch interface (sw0) for gateways with hardware switch chipset.
DNS settings	• Your network DNS server IP addresses.

TABLE 7-4. Routing Mode Requirements

REQUIREMENT	DETAILS
Ethernet cables (3 cables)	Connect to the MGMT port (management) and the WAN and LAN1 data ports. **Note** In this configuration, the LAN1 port is used to connect to the internal local area network. For gateways with hardware switch chipset: You will connect LAN1 to an internal endpoint.
IP addresses (2 addresses)	• Obtain the information about connecting to the WAN from your Internet Service Provider (ISP): DHCP, Static, or PPPoE. • Obtain your IP address information for the internal LAN1 connection (Static) • For gateways with wireless functionality: If you enable the main wireless network during initial deployment, you will need a third IP address for the wireless network interface.
DNS settings	• Use either automatic DNS settings assigned by the ISP's DHCP or obtain your network DNS server IP addresses.

TABLE 7-5. Software Switch Requirements

REQUIREMENT	DETAILS
Ethernet cables (4-5 cables)	Connect to the MGMT port (management), WAN, LAN1, LAN2 and optionally LAN3. • WAN is the uplink that connects to the external network (either directly or through an upstream switch). • LAN1, LAN2, and LAN3 (optional) connect to end points on the internal local area network. **Note** The Software Switch configuration requires three connected interfaces. You must connect WAN and LAN1 and at least one other LAN interface.
IP addresses (1 address)	• Obtain the information about connecting to the WAN from your Internet Service Provider (ISP): DHCP or Static. You will use this information to configure the bridge interface (br0) as an L3 interface. **Note** Other interfaces used in the Software Switch configuration are configured as L2 interfaces, which cannot have IP addresses assigned to them.
DNS settings	• Your network DNS server IP addresses.

Note

Bridge Mode and Routing Mode: If you connect additional LAN ports to other internal networks or endpoints, you might need additional cables and IP addresses.

Routing Mode: The LAN1 port can be configured as a secondary, redundant WAN connection. If this is the case, you can configure the remaining LAN ports as internal networks. For more information, see *Managing Routing on page 7-89*.

Installation and Initial Configuration

Trend Micro™ Cloud Edge is a next generation security solution for MSPs (Managed Service Providers) that combines on-premises and cloud-based security features. Perform the installation and initial configuration of your Cloud Edge gateways on-premises and the MSP can remotely manage your network through the cloud.

Procedure

1. Set up the hardware.

   Setting up the Hardware on page 7-22

2. Log on to the on-premises console from the MGMT port.

   Logging on the On-Premises Console from the MGMT Port on page 7-24

3. Perform the initial configuration.

   Performing the Initial Configuration on page 7-25

4. Register the gateway (if not already registered).

   Registering Gateways on page 7-44

5. Perform additional configuration to meet your business needs.

   Performing additional configuration on page 7-46

Setting up the Hardware

Before the Cloud Edge gateway can connect and register with Cloud Edge Cloud Console, you must set up the hardware.

Note

Do not power on the Cloud Edge gateway until instructed.

Procedure

1. Toggle the switch on the back panel to select the deployment mode.

   By default, Cloud Edge gateways are configured for Bridge Mode.

   Note

   The image shown in this manual might differ slightly from your gateway.

   Note

   The Cloud Edge 300 does not have a deployment mode switch on the back panel. To change the deployment mode, you must use the on-premises console. The default is Bridge Mode.

2. Connect the gateway to a power source.
3. Connect the gateway to the network.
   a. Connect the gateway WAN port to a wide area network (i.e. Internet).
   b. Connect the gateway LAN1 port to an internal local area network, such as a segment of your network.

      If deploying a Software Switch configuration or if you are deploying a Cloud Edge gateway with hardware switch chipset in Bridge Mode, connect LAN1 to an appropriate endpoint.
4. Perform the appropriate action, depending on the deployment configuration.
   - **Bridge Mode**: Optionally connect the gateway's remaining LAN ports to other internal networks.

- **Bridge Mode (With Switch Chipset)**: Optionally connect the gateway's LAN2-LAN7 ports to endpoints on the internal network.

  Gateways with hardware switch chipset have unique bypass capabilities in Bridge Mode during events such as upgrades, restarts, power off, and system panic. The bypass capabilities are determined by the port. To help you determine how to assign endpoints to each port, see *Bypass Ports on Gateways with Hardware Switch Chipset on page 7-15*.

- **Software Switch**: Connect the gateway LAN2 port and optionally LAN3 to other endpoints.

  You must have a minimum of three connected ports in a Software Switch configuration. WAN and LAN1 are required. Connect one or both of the remaining LAN2 and LAN3 ports.

- **Routing Mode**: Optionally connect the gateway's remaining LAN ports to other internal networks.

5. Power on the gateway.

   If the WAN interface uses DHCP and if the gateway has been pre-registered, the gateway will automatically connect to Cloud Edge Cloud Console.

What to do next

If the WAN interface uses PPPoE or uses a static IP address, you must log on to the Cloud Edge gateway on-premises console and configure the WAN interface before the gateway can connect to Cloud Edge Cloud Console.

Logging on the On-Premises Console from the MGMT Port

Procedure

1. Connect a computer to the Cloud Edge gateway **MGMT** port using an Ethernet cable.
2. Configure the computer to automatically obtain an IP address on the Ethernet interface used to connect to the MGMT port.

3. Open a supported web browser.
4. Go to the following URL:

   `https://192.168.252.1:8443`
5. Specify the logon credentials.

   Default administrator account credentials:

   User name: `admin`

   Password: `adminCloudEdge`
6. Press Enter or click **Log On**.

   The Cloud Edge on-premises console **Quick Setup** page appears.

Performing the Initial Configuration

After logging in to the Cloud Edge on-premises console for the first time, the **Quick Setup** screen opens automatically.

Trend Micro recommends using the **Quick Setup** screen to configure the WAN uplink settings and to specify system settings.

Note

The **Quick Setup** screen automatically appears only when a Cloud Edge gateway is unregistered or offline. To view the **Quick Setup** screen when the device is online, click the **Quick Setup** link at the top-right of the screen.

Perform one of the following initial configurations, depending on the chosen deployment mode.

- *Initial Configuration for Bridge Mode on page 7-26*
- *Initial Configuration for Bridge Mode (With Switch Chipset) on page 7-28*
- *Initial Configuration for Software Switch on page 7-31*
- *Initial Configuration for Routing Mode on page 7-35*

- *Initial Configuration for Routing Mode (Wireless) on page 7-38*

You can run tests from the **Quick Setup** screen to confirm the deployment configuration:

- *Tests to Confirm Deployment Configuration on page 7-42*

Related information

- *Deployment Mode Overview*
- *Deployment Mode Switch*

Initial Configuration for Bridge Mode

Use the **Quick Setup** screen to configure basic Bridge Mode deployment settings for your Cloud Edge gateway. After you have configured basic deployment settings, you can use the on-premises console to configure additional settings.

Procedure

1. Log on to the Cloud Edge on-premises console.
2. In the **Uplink configuration** section, specify the following details to configure network information for the bridge interface (br0):

Option	Description
Deployment mode	Read-only field set to `Bridge Mode`. Deployment mode is configured by setting the deployment mode switch on the gateway's back panel to **Bridge**. See *Deployment Mode Switch on page 7-17*. **Note** For the Cloud Edge 300 gateway, you can change the deployment mode to Bridge Mode with this option.
Type	Select **Bridge**.

Option	Description
Interface 1 and **Interface 2**	These fields display only in Bridge Mode and are not configurable because all interfaces are layer 2 interfaces. You cannot assign an IP address to a layer 2 interface.
Mode	Assign an IP address to the bridge interface (br0) using one of the following: • **DHCP** • **Static**: Specify **IPv4 address**, **IPv4 netmask**, and **IPv4 default gateway**. **Note** The Cloud Edge gateway must be able to access Internet resources using the assigned IP address.
Primary DNS	Specify the IP address of the DNS server. This is a required setting if you select **Static** in the **Mode** field.
Secondary DNS **Tertiary DNS**	Optionally, specify IP addresses for a secondary and tertiary DNS server.

3. In the **System settings** section, configure the host name and time and location settings for the Cloud Edge gateway.

Option	Description
Host name	Specify a host name.
Enable NTP server	Select this option if you want to synchronize with the NTP server, and then add the NTP server IP address in the **NTP server** field.
Manually set time	Select this option if you want to set the time manually, and specify the current time in the **Local time** field in the following format: `yyyy-mm-dd hh:mm:ss`. For example, `2015-01-16 13:03:28`.

Option	Description
Location and **City**	Set the appropriate time zone by selecting the location and city closest to the Cloud Edge gateway. If the **Location**/**City** is not Asia/Tokyo, the time zone information will be synchronized from Cloud Edge Cloud Console to the time zone of the company to which the gateway is registered.

4. Click **Start Configuration Test** to verify the network uplink configuration.

   For more information, see *Tests to Confirm Deployment Configuration on page 7-42*.

   Note

   If the device is not registered prior to initial configuration, the registration test and the dependency service check do not succeed. This is normal. After registration, you can return to the **Quick Setup** screen and rerun the configuration test to verify registration status and verify that the dependency services tests succeed.

5. (Optional) If the test takes too long, you can stop it before it completes by clicking on **Stop Configuration Test**.

   The recommendation is to let the test complete to ensure that the configuration and services are all functioning properly.

6. Click **Save & Register**.

   Note

   After the Cloud Edge gateway is registered successfully with Cloud Edge Cloud Console, the button text changes to **Save Settings**.

Initial Configuration for Bridge Mode (With Switch Chipset)

Use the **Quick Setup** screen to configure basic Bridge Mode deployment settings for your Cloud Edge gateway with hardware switch chipset. After you

have configured basic deployment settings, you can use the on-premises console to configure additional settings, including hardware switch settings.

Note

To configure certain switch interface (sw0) settings, you must use Cloud Edge Cloud Console.

Procedure

1. Log on to the Cloud Edge on-premises console.
2. In the **Uplink configuration** section, specify the following details to configure network information for the switch interface (sw0):

Option	Description
Deployment mode	Read-only field set to `Bridge Mode`. Deployment mode is configured by setting the deployment mode switch on the gateway's back panel to **Bridge**. See *Deployment Mode Switch on page 7-17*.
Intranet Security mode	Read-only field set to **High Security**. This is the initial default setting. After completing initial setup, you can change the Intranet Security mode using Cloud Edge Cloud Console. See *Security Protections Provided by Each Intranet Security Mode on page 6-61*
Interfaces	Read-only field set to `WAN`, `LAN1–LAN8`. The WAN, LAN1-LAN8 L2 interfaces are automatically included in the hardware switch configuration and cannot be removed or disabled. They cannot be changed to L3 interfaces.

Option	Description
Mode	Assign an IP address to the switch interface (sw0) using one of the following: • **DHCP** • **Static**: Specify **IPv4 address**, **IPv4 netmask**, and **IPv4 default gateway**. **Note** The Cloud Edge gateway must be able to access Internet resources using the assigned IP address.
Primary DNS	Specify the IP address of the DNS server. This is a required setting if you select **Static** in the **Mode** field.
Secondary DNS **Tertiary DNS**	Optionally, specify IP addresses for a secondary and tertiary DNS server.

3. In the **System settings** section, configure the host name and the time and location settings for the Cloud Edge gateway.

Option	Description
Host name	Specify a host name.
Enable NTP server	Select this option if you want to synchronize with the NTP server, and then add the NTP server IP address in the **NTP server** field.
Manually set time	Select this option if you want to set the time manually, and specify the current time in the **Local time** field in the following format: `yyyy-mm-dd hh:mm:ss`. For example, `2015-01-16 13:03:28`.

Option	Description
Location and **City**	Set the appropriate time zone by selecting the location and city closest to the Cloud Edge gateway. If the **Location**/**City** is not Asia/Tokyo, the time zone information will be synchronized from Cloud Edge Cloud Console to the time zone of the company to which the gateway is registered.

4. Click **Start Configuration Test** to verify the network uplink configuration.

   For more information, see *Tests to Confirm Deployment Configuration on page 7-42*.

> **Note**
> If the device is not registered prior to initial configuration, the registration test and the dependency service check do not succeed. This is normal. After registration, you can return to the **Quick Setup** screen and rerun the configuration test to verify registration status and verify that the dependency services tests succeed.

5. (Optional) If the test takes too long, you can stop it before it completes by clicking on **Stop Configuration Test**.

   The recommendation is to let the test complete to ensure that the configuration and services are all functioning properly.

6. Click **Save & Register**.

> **Note**
> After the Cloud Edge gateway is registered successfully with Cloud Edge Cloud Console, the button text changes to **Save Settings**.

Initial Configuration for Software Switch

To perform the initial basic setup for your Cloud Edge gateway with a Software Switch configuration, you must first configure certain settings using

the on-premises console and then use the **Quick Setup** screen to complete the initial configuration. After you have configured basic settings, you can use the on-premises console to configure additional settings.

Important

The deployment mode switch must be set to **Bridge** to set up a Software Switch configuration. See *Deployment Mode Switch on page 7-17*.

Procedure

1. Log on to the Cloud Edge on-premises console.

   The **Quick Setup** screen opens. Because you must configure certain initial Software Switch settings using the on-premises console, you must now open the on-premises console.

2. Click on the **Cloud Edge On-Premises Console** link on the top-right side of the screen.

   The **Cloud Edge On-Premises Console** screen opens.

3. Go to **Network** > **Bridge**.

4. In the name column, click on **br0**.

   The **Add/Edit Bridge** screens opens.

5. Specify the following:

Option	Description
Type	Change the type from **Bridge** to **Software Switch**. After selecting **Software Switch**, the available options change. The **Interface 1** and **Interface 2** fields are replaced by the **Switch Interfaces** field.

Option	Description
Switch Interfaces	Select which interfaces to include in the Software Switch configuration. • The **Switch Interfaces** field appears with **WAN** and **LAN1** preselected. You cannot deselect them. Because the configuration must have a minimum of three interfaces, you must select at least one additional interface. Select either **LAN2** or **LAN3** or select both interfaces. • These are L2 interfaces. You cannot assign IP addresses to them.
Mode	Assign an IP address to the bridge interface (br0) using one of the following: • **DHCP** • **Static**: Specify **IPv4 address**, **IPv4 netmask**, and **IPv4 default gateway**.  **Note** The Cloud Edge gateway must be able to access Internet resources using the assigned IP address.

6. Click **Apply**.
7. Click on **Quick Setup** in the top-right corner.

   The **Quick Setup** screen opens.
8. In the **Uplink configuration** section, specify the following to configure DNS for the bridge interface (br0):

Option	Description
Primary DNS	Specify the IPv4 address of the DNS server. This is a required setting if you selected **Static** in the **Mode** field.

Option	Description
Secondary DNS **Tertiary DNS**	Optionally, specify IPv4 addresses for a secondary and tertiary DNS server.

Note

The **Deployment mode**, **Type**, and **Interfaces** fields are read-only in the **Quick Setup** screen.

9. In the **System settings** section, configure the host name and time and location settings for the Cloud Edge gateway.

Option	Description
Host name	Specify a host name.
Enable NTP server	Select this option if you want to synchronize with the NTP server, and then add the NTP server IP address in the **NTP server** field.
Manually set time	Select this option if you want to set the time manually, and specify the current time in the **Local time** field in the following format: `yyyy-mm-dd hh:mm:ss`. For example, `2015-01-16 13:03:28`.
Location and **City**	If needed, set the appropriate time zone by selecting the location and city closest to the Cloud Edge gateway. If the **Location**/**City** is not Asia/Tokyo, the time zone information will be synchronized from Cloud Edge Cloud Console to the time zone of the company to which the gateway is registered.

10. Click **Start Configuration Test** to verify the network uplink configuration.

    For more information, see *Tests to Confirm Deployment Configuration on page 7-42*.

Note

If the device is not registered prior to initial configuration, the registration test and the dependency service check do not succeed. This is normal. After registration, you can return to the **Quick Setup** screen and rerun the configuration test to verify registration status and verify that the dependency services tests succeed.

11. (Optional) If the test takes too long, you can stop it before it completes by clicking on **Stop Configuration Test**.

    The recommendation is to let the test complete to ensure that the configuration and services are all functioning properly.

12. Click **Save & Register**.

Note

After the Cloud Edge gateway is registered successfully with Cloud Edge Cloud Console, the button text changes to **Save Settings**.

Initial Configuration for Routing Mode

Use the **Quick Setup** screen to configure basic Routing Mode deployment settings for your Cloud Edge gateway. After you have configured basic deployment settings, you can use the on-premises console to configure additional settings.

Procedure

1. Log on to the Cloud Edge on-premises console.
2. In the **Uplink configuration** section, specify the following details to configure network information for the WAN interface that connects to the Internet.

Option	Description
Deployment mode	Read-only field set to `Routing Mode`. Deployment mode is configured by setting the deployment mode switch on the gateway's back panel to **Routing**. See *Deployment Mode Switch on page 7-17*. **Note** For the Cloud Edge 300 gateway, you can change the deployment mode to Routing Mode with this option.
WAN interface	This is a read-only field that is set to WAN and is only available if the Cloud Edge gateway is deployed in Routing Mode. This field cannot be modified in the **Quick Setup** screen.
Mode	Assign an IP address to the WAN interface using one of the following: • **DHCP** • **PPPoE**: Specify the **User name** and **Password**. This option is only available in Routing Mode. • **Static**: Specify **IPv4 address**, **IPv4 netmask**, and **IPv4 default gateway**. **Note** The Cloud Edge gateway must be able to access Internet resources using the assigned IP address.
Primary DNS	Specify the IP address of the DNS server. This is a required setting if you select **Static** in the **Mode** field.
Secondary DNS **Tertiary DNS**	Optionally, specify IP addresses for a secondary and tertiary DNS server.

3. In the **System settings** section, configure the host name and time and location settings for the Cloud Edge gateway.

Option	Description
Host name	Specify a host name.
Enable NTP server	Select this option if you want to synchronize with the NTP server, and then add the NTP server IP address in the **NTP server** field.
Manually set time	Select this option if you want to set the time manually, and specify the current time in the **Local time** field in the following format: `yyyy-mm-dd hh:mm:ss`. For example, `2015-01-16 13:03:28`.
Location and **City**	Set the appropriate time zone by selecting the location and city closest to the Cloud Edge gateway. If the **Location**/**City** is not Asia/Tokyo, the time zone information will be synchronized from Cloud Edge Cloud Console to the time zone of the company to which the gateway is registered.

4. Click **Start Configuration Test** to verify the network uplink configuration.

   For more information, see *Tests to Confirm Deployment Configuration on page 7-42*.

Note

If the device is not registered prior to initial configuration, the registration test and the dependency service check do not succeed. This is normal. After registration, you can return to the **Quick Setup** screen and rerun the configuration test to verify registration status and verify that the dependency services tests succeed.

5. (Optional) If the test takes too long, you can stop it before it completes by clicking on **Stop Configuration Test**.

   The recommendation is to let the test complete to ensure that the configuration and services are all functioning properly.

6. Click **Save & Register**.

Note

After the Cloud Edge gateway is registered successfully with Cloud Edge Cloud Console, the button text changes to **Save Settings**.

7. Configure the LAN1 interface using the on-premises console.
   a. Click on the **Cloud Edge On-Premises Console** link on the upper-right corner of the **Quick Setup** screen.
   b. Go to **Network** > **Interfaces**.
   c. Click the LAN1 interface to edit its setting.
   d. From the **Type** drop-down list, select **L3**, and then configure the IP address settings.
      - **DHCP**: Specify **MTU**/**MSS** if desired.
      - **Static**: Manually enter address information for IPv4 (**IPv4 address**, **IPv4 netmask**) and optionally a gateway address. Specify **MTU**/**MSS** if desired.
   e. Click **Apply**.
8. Optionally, configure additional LAN interfaces using Cloud Edge Cloud Console.

Routing Mode: Editing Network Interfaces on page 6-51

Initial Configuration for Routing Mode (Wireless)

Use the **Quick Setup** screen to configure basic Routing Mode deployment settings for your Cloud Edge gateway with wireless network access. After you have configured basic deployment settings, you can use the on-premises console to configure additional settings, including wireless network settings.

Note

To configure wireless network access control settings, you must use Cloud Edge Cloud Console.

Procedure

1. Log on to the Cloud Edge on-premises console.
2. In the **Uplink configuration** section, specify the following details to configure network information for the WAN interface that connects to the Internet.

Option	Description
Deployment mode	Read-only field set to `Routing Mode`. Deployment mode is configured by setting the deployment mode switch on the gateway's back panel to **Routing**. See *Deployment Mode Switch on page 7-17*.
WAN interface	This is a read-only field that is set to WAN and is only available if the Cloud Edge gateway is deployed in Routing Mode. This field cannot be modified in **Quick Setup**.
Mode	Assign an IP address to the WAN interface using one of the following: • **DHCP** • **PPPoE**: Specify the **User name** and **Password**. This option is only available in Routing Mode. • **Static**: Specify **IPv4 address**, **IPv4 netmask**, and **IPv4 default gateway**. **Note** The Cloud Edge gateway must be able to access Internet resources using the assigned IP address.

Option	Description
Primary DNS	Specify the IP address of the DNS server. This is a required setting if you select **Static** in the **Mode** field.
Secondary DNS **Tertiary DNS**	Optionally, specify IP addresses for a secondary and tertiary DNS server.

3. In the **Wireless settings** section, specify the following details to configure wireless network access for the Cloud Edge gateway.

Option	Description
Enable Wireless AP	Select to enable wireless network access. This option enables the main wireless network. It does not enable the guest wireless network.
Frequency	Select either the **2.4GHz** or the **5GHz** option.
SSID	Enter the SSID you want to assign to the wireless network. The default SSID is `CloudEdge-XXYY` (2.4 GHz) or `CloudEdge-GUEST-XXYY` (5 GHz) XXYY is the first four digits of the gateway's serial number.
Security settings	Select either the **Open** or the **WPA-PSK[TKIP]+WPA2-PSK[AES]** option. Additional security settings options are available. After initial setup, you can use the on-premises console to modify the wireless network configuration including the security settings. Trend Micro recommends using security for the wireless network and not using the **Open** option.

4. In the **System settings** section, configure the host name and the time and location settings for the Cloud Edge gateway.

Option	Description
Host name	Specify a host name.
Enable NTP server	Select this option if you want to synchronize with the NTP server, and then add the NTP server IP address in the **NTP server** field.
Manually set time	Select this option if you want to set the time manually, and specify the current time in the **Local time** field in the following format: `yyyy-mm-dd hh:mm:ss`. For example, `2015-01-16 13:03:28`.
Location and **City**	Set the appropriate time zone by selecting the location and city closest to the Cloud Edge gateway. If the **Location**/**City** is not Asia/Tokyo, the time zone information will be synchronized from Cloud Edge Cloud Console to the time zone of the company to which the gateway is registered.

5. Click **Start Configuration Test** to verify the network uplink configuration.

   For more information, see *Tests to Confirm Deployment Configuration on page 7-42*.

Note

If the device is not registered prior to initial configuration, the registration test and the dependency service check do not succeed. This is normal. After registration, you can return to the **Quick Setup** screen and rerun the configuration test to verify registration status and verify that the dependency services tests succeed.

6. (Optional) If the test takes too long, you can stop it before it completes by clicking on **Stop Configuration Test**.

   The recommendation is to let the test complete to ensure that the configuration and services are all functioning properly.

7. Click **Save & Register**.

Note

After the Cloud Edge gateway is registered successfully with Cloud Edge Cloud Console, the button text changes to **Save Settings**.

8. Configure the LAN1 interface using the on-premises console
   a. Click on the **Cloud Edge On-Premises Console** link on the upper-right corner of the **Quick Setup** screen.
   b. Go to **Network** > **Interfaces**.
   c. Click the LAN1 interface to edit its setting.
   d. From the **Type** drop-down list, select **L3**, and then configure the IP address settings.
      - **DHCP**: Specify **MTU**/**MSS** if desired.
      - **Static**: Manually enter address information for IPv4 (**IPv4 address**, **IPv4 netmask**) and optionally a gateway address. Specify **MTU**/**MSS** if desired.
   e. Click **Apply**.
9. Optionally, configure additional LAN interfaces using Cloud Edge Cloud Console.
   a. Log on the Cloud Edge Cloud Console.

      Logging on the Cloud Console on page 6-2
   b. Configure the interfaces as needed.

      Routing Mode: Editing Network Interfaces on page 6-51

      Routing Mode: Editing Wireless Network Interfaces on page 6-52

Tests to Confirm Deployment Configuration

After you complete the initial deployment configuration, Cloud Edge can perform a series of tests to confirm that the gateway can connect to the Internet, that the gateway status is registered, and to verify that various required services are available. If one test fails, subsequent tests are not

performed. You must remedy any issue that causes a test to fail and rerun the tests.

The following tests are performed in order:

Order	Test	Description	Test fails if...
1	WAN check	Check WAN and LAN1 interface statuses (up or down).	Both interfaces are down.
2	DNS check	Check DNS configuration. Check whether DNS request succeeds.	DNS is not configured. One DNS check fails.
3	WAN router check	Check router configuration. Check to see if can successfully connect to outside websites.	No route to WAN exists. Cloud Edge cannot connect to outside website.
4	Registration status check	Check registration status.	Gateway is not registered.
5	Cloud Edge cloud services check, including the following: • ActiveUpdate • Cloud Scan • Cloud Mail Scan • Email Reputation • Log upload • Web Reputation • Smart Scan • Predictive Machine Learning	All services are checked.	Each service is checked individually and each service is marked as succeeded or failed individually. The overall dependency check fails if all service checks fail.

Registering Gateways

If you have not already registered the Cloud Edge gateway using Cloud Edge Cloud Console, you must register it to deploy security policies.

Procedure

1. Log on to the Cloud Edge Cloud Console.
2. On Cloud Edge Cloud Console, go to **Gateways**.
3. Click **Register New Gateway**.
4. Specify the gateway settings.

Option	Description
Display name	Specify the name that appears in Cloud Edge Cloud Console for the new gateway.
Model	Specify the Cloud Edge gateway hardware model.
Serial number	Specify the Cloud Edge gateway serial number. Find the serial number on the gateway itself or on the gateway packaging. The serial number is alphanumeric with 12 digits separated by hyphens (example: 4C80-9315-3A0B).

5. Click **Save**.

   It may take a few minutes for registration to complete.

   After registration, Cloud Edge Cloud Console deploys policies to the gateway. After registration is complete, you can view log statistics through Cloud Edge Cloud Console dashboard widgets, log analysis, and reports based on live traffic sent by the Cloud Edge gateway.

6. Verify successful registration.

   Verifying the Registration on page 6-14.

Verifying the Registration

Trend Micro recommends verifying each gateway after registration. The following procedure explains how to use the Cloud Edge on-premises

console to check that the gateway correctly registered with Cloud Edge Cloud Console.

Procedure

1. Log on to the Cloud Edge on-premises console.
2. Do one the following:
   - Navigate to **Dashboard** > **System Information (widget)**, and check the information under **Cloud management status**.
   - Navigate to **Administration** > **Device Management** > **Cloud Management (tab)** and verify the information shown.
3. Verify connectivity by following procedure *Verifying Connectivity on page 7-45*.

Verifying Connectivity

Verify connectivity and test your deployment to make sure that the Cloud Edge gateway has registered with Cloud Edge Cloud Console and can correctly route traffic based on the policies.

Procedure

1. Review the following table to understand the LED status.

LED	Status
No light	The Cloud Edge gateway cannot communicate with the Internet.
Solid green light	The Cloud Edge gateway is registered and communicating with Cloud Edge Cloud Console.
Blinking green light	The Cloud Edge gateway is not registered or cannot communicate with Cloud Edge Cloud Console.

2. If Cloud Edge registration was successful, try accessing the Internet from an internal endpoint.

Cloud Edge succeeds when you can access the Internet.

Note

Contact Trend Micro if you cannot verify the deployment.

Performing additional configuration

You can perform additional configuration steps to meet your business requirements. Use either the Cloud Edge on-premises console or Cloud Edge Cloud Console as directed in each of the following steps.

Procedure

1. For Cloud Edge gateways with wireless network functionality, configure wireless settings.
   - Wireless network configuration, including configuring the guest wireless network: (on-premises console):

     Managing Wireless Networks on page 7-68
   - Wireless access control: (Cloud Edge Cloud Console):

     Configuring Access Control for the Wireless Networks on page 6-108
   - Wireless interface configuration (Cloud Edge Cloud Console):

     Routing Mode: Editing Network Interfaces on page 6-51
2. Configure interfaces to act as DHCP servers for clients on the connected network.
   - WAN or LAN1 interfaces (on-premises console):

     Modifying DHCP Service Settings on page 7-98
   - Additional LAN interfaces or the MGMT interface (Cloud Edge Cloud Console):

     Editing DHCP Settings on page 6-71

For Cloud Edge gateways with wireless network access functionality, you can configure DHCP on the main and guest wireless networks.

3. Add policy-based routes (on-premises console).
   - *Adding a Policy-based Route on page 7-93*
4. Add static routes (Cloud Edge Cloud Console).
   - *Adding a Static Route on page 6-80*
5. Configure NAT on Cloud Edge gateway interfaces (Cloud Edge Cloud Console).
   - *Adding a Destination NAT Rule on page 6-84*
   - *Adding a Source NAT Rule on page 6-86*
   - *Changing NAT Rule Priorities on page 6-86*
6. Configure the on-premises console timeout setting (on-premises console).
   - *Configuring the On-premises Console Timeout on page 7-102*
7. Manage administrative access to the Cloud Edge gateway (Cloud Edge Cloud Console).
   - *Enabling Administrative Access on page 7-104*
8. Configure monitoring hosts for WAN and LAN1 interfaces (on-premises console).
   - *Configuring Monitoring Hosts On an Interface on page 7-65*

Management

Managing Network Settings

You can manage network settings to process and identify network traffic.

Managing Network Interfaces

Before you register the Cloud Edge gateway to Cloud Edge Cloud Console, you can view and modify all autodetected network interfaces from the Cloud Edge on-premises console.

After registering the gateway, you can view or modify configurations for the following interfaces using the Cloud Edge on-premises console:

Note

After registration, the MGMT interface must be configured using Cloud Edge Cloud Console.

- **Bridge Mode: bridge interface (br0)**
  - The virtual bridge interface (br0) is the only available L3 interface when using Bridge Mode.
  - You can use static or DHCP IPv4 addressing when configuring this interface.

    PPPoE is not supported on the bridge interface (br0).
  - VLANs are not supported on the bridge interface (br0).

Note

You can edit certain L2 settings on the physical interfaces, such as MTU. Use the on-premises console to edit the WAN and all LAN L2 interfaces.

- **Bridge Mode (With Switch Chipset): switch interface (sw0)**
  - The virtual switch interface (sw0) is the only available L3 interface when using Bridge Mode.
  - You can use static or DHCP IPv4 addressing when configuring this interface.

    PPPoE is not supported on the switch interface (sw0).

- VLANs are not supported on the switch interface (sw0).
- The WAN and LAN1-LAN8 interfaces are automatically added to the switch configuration.
  - You cannot remove any of these interfaces from the switch configuration or change them to L3 interfaces.
  - You can disable the LAN2-LAN7 interfaces.
  - You cannot disable the WAN, LAN1, or LAN8 interfaces.
  - You can connect endpoints to the LAN1-LAN7 interfaces. You should not connect an endpoint to the LAN8 interface because it is used for bypass functions.

Note

You can edit certain L2 settings on the physical interfaces, such as MTU and flow control. Use the on-premises console to edit the WAN and LAN1-LAN8 interfaces.

- **Software Switch: bridge interface (br0)**
  - The virtual bridge interface (br0) is the only available L3 interface when deploying a Software Switch configuration.
  - You can use static or DHCP IPv4 addressing when configuring this interface.

    PPPoE is not supported on the bridge interface (br0).
  - You must add at least three L2 interfaces for use as a software switch.

    You must add WAN and LAN1. You can add one or both of LAN2 and LAN3 to the Software Switch configuration.

    You can add an L3 interface to the Software Switch configuration. Cloud Edge automatically changes the L3 interface to an L2 interface after it is added to the software switch.

    You might see this situation when the gateway was first deployed in Routing Mode, but was later changed to Bridge Mode and deployed

as a Software Switch. In this case, existing L3 interfaces are not converted to L2 interfaces unless they are added to the switch configuration.

Note

You can edit certain L2 settings on the physical interfaces, such as MTU. Use the on-premises console to edit the WAN and all LAN L2 interfaces.

- **Routing Mode: WAN and LAN1**
  - You can configure static, DHCP, and PPPoE IPv4 addressing on the WAN or LAN1 interfaces.

Note

PPPoE might be used on LAN1 if the interface is used as a redundant WAN connection.

  - The WAN interface provides connectivity to the Internet.
  - The LAN1 interface can be configured as either a second WAN interface that provides a redundant connection to the Internet or as a LAN interface that connects to the internal network.

    For more information about dual WAN configurations, see *Automatic Failover for Multiple ISP/WAN Environments on page 7-92*.

Note

You can edit WAN and LAN1 using the on-premises console. To edit other interfaces, you must use Cloud Edge Cloud Console.

You can add L3 VLANs to the WAN and LAN1 interfaces using the on-premises console; however, L2 VLANS are not supported on gateways running Cloud Edge 6.0 and later.

Supported Network Interface Configurations

Cloud Edge gateways support the following network L3 interface configurations:

- **Static IP addresses (Static)**
  - Routing Mode: Supported on all L3 interfaces
  - Routing Mode: Supported on wireless network interfaces
  - Bridge Mode and Software Switch: Supported on the bridge interface (br0)
  - Bridge Mode (With Switch Chipset): Supported on the switch interface (sw0)
  - All modes: Supported on the MGMT port
- **Dynamic Host Configuration Protocol (DHCP)**
  - Routing Mode: Supported on WAN or LAN1 L3 interfaces
  - Bridge Mode and Software Switch: Supported on the bridge interface (br0)
  - Bridge Mode (With Switch Chipset): Supported on the switch interface (sw0)
  - All modes: Not supported on the MGMT port
- **Point-to-point Protocol over Ethernet (PPPoE)**
  - Routing Mode: Supported on WAN and LAN1 L3 interfaces
  - Bridge Mode and Software Switch: Not supported on the bridge interface (br0)
  - Bridge Mode (With Switch Chipset): Not supported on the switch interface (sw0)
  - All modes: Not supported on the MGMT port

Information About Changing to Software Switch Deployment

There is certain information you should know when changing a Cloud Edge gateway to a Software Switch deployment.

- All interfaces except the management interface (MGMT) can be added to the software switch.

Three interfaces are required. WAN and LAN1 are required. You can add either LAN2 or LAN3 as the third interface. You can add both LAN2 and LAN3 to the software switch if desired.

- Fail-safe access for the WAN and LAN1 interfaces:
  - Even though a gateway deployed as a software switch acts like a multiport bridge, Cloud Edge provides fail-safe access using the WAN and LAN1 interfaces.
  - The WAN and LAN1 interfaces act as bypass ports to support access through the LAN1 port even if the gateway is offline. Internet-dependent devices should be connected through the LAN1 interface.
- For any interface added to a Software Switch configuration:
  - The interface is automatically enabled.
  - Any L3 interface is automatically changed to L2.
  - DHCP service on the interface is disabled.
  - Any related SNAT rule is deleted.
  - You cannot change an L2 interface to an L3 interface while it is part of a software switch.
  - You cannot disable an L2 interface while it is part of a software switch.
- The following rules apply when configuring software switch settings:
  - You can change only the MTU and bandwidth settings of an L2 interface added to the software switch.

    You can change both the software switch MTU (1438 default) and the port MTU (1504 default). Cloud Edge prevents you from making the software switch MTU larger than the port MTU.
  - You must configure a Software Switch deployment using the on-premises console.
- The following applies to mail scanning for software switch deployments:

- In Bridge Mode, Cloud Edge performs mail scanning only for traffic between the WAN interface and the LAN1 interface.

  Mail scanning is not done for traffic between LAN interfaces.

- In Software Switch deployments, Cloud Edge performs mail scanning for traffic between the WAN interface and all LAN interfaces.

  Mail scanning is done for traffic between LAN interfaces.

- When switching between Software Switch and Routing Mode deployments, keep the following in mind:
  - If you change the configuration from Software Switch to Routing Mode, the Software Switch configuration is lost.
  - If you change the configuration from Routing Mode to Software Switch, LAN2 and LAN3 configurations and related NAT rules are lost.

Enabling or Disabling Interfaces

Certain of the Cloud Edge gateway's interfaces might be enabled or disabled by default, depending on the deployment mode. In certain configurations, you might not be able to disable some interfaces.

Note

You cannot disable the MGMT port in any deployment mode.

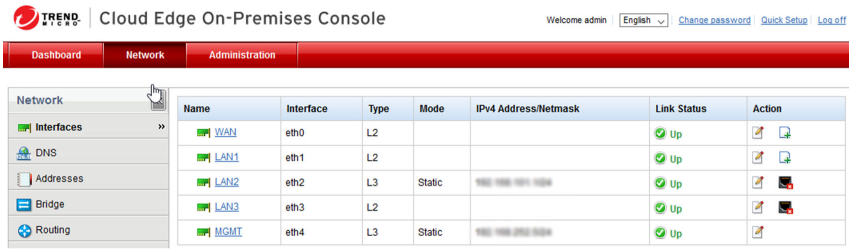


FIGURE 7-7. Example: Cloud Edge 70 in Routing Mode

You enable or disable interfaces from the Cloud Edge on-premises console.

- Routing Mode: LAN2 and LAN3 are enabled by default.

  You can disable or re-enable these interfaces at any time.

- Bridge Mode: LAN2 and LAN3 are disabled by default.

  You can enable or disable these interfaces at any time.

- Software Switch: LAN2 and LAN3 are automatically enabled when you add them as a software switch interface.

  You cannot disable an interface if it is part of a Software Switch configuration.

Note

The Cloud Edge 300 gateway does not have the LAN3 interface.

Cloud Edge Gateways with Hardware Switch Chipset

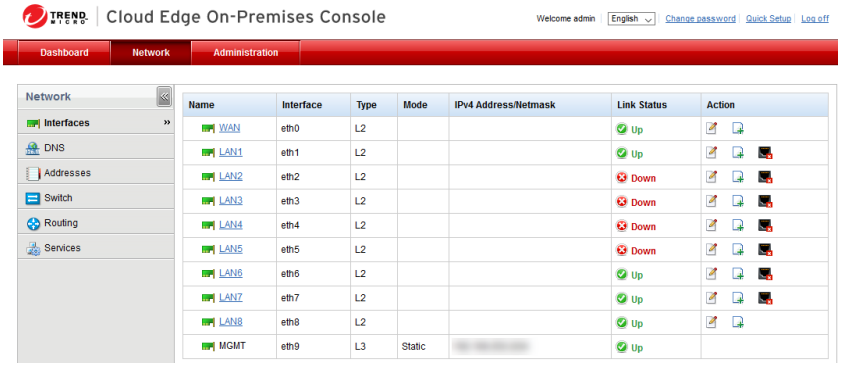


FIGURE 7-8. Example: Cloud Edge 100 G2 in Bridge Mode

All ports are enabled by default. You cannot disable the WAN, LAN8, or MGMT interfaces.

- Routing Mode

  You can disable the LAN1-LAN7 interfaces.

- Bridge Mode

  The WAN and LAN1-LAN8 interfaces are automatically selected as ports for the hardware switch. These ports cannot be removed from the hardware switch configuration; however, you can disable the LAN1-LAN7 interfaces.

Cloud Edge Gateway with Wireless Network Functionality

You cannot enable or disable wireless network interfaces from the **Interfaces** page.

The main wireless network is automatically enabled when you enable wireless access and guest wireless network is automatically enabled when you enable the guest wireless network. The wireless network interfaces are automatically disabled if you disable the corresponding wireless network.

Procedure

1. From the Cloud Edge on-premises console, go to **Network** > **Interfaces**.
2. Do one of the following:
   a. For the interface that you want to enable, click the **Enable** icon ( ).
   b. For the interface that you want to disable, click the **Disable** icon ( ).

Editing Network Interfaces for Bridge Mode/Software Switch

You can configure the MTU on physical L2 interfaces on Cloud Edge gateways in Bridge Mode or in the Software Switch configuration. You must use the on-premises console for this procedure.

Note

For the procedure to follow when configuring physical interfaces for Bridge Mode (With Switch Chipset), see *Editing Network Interfaces for Bridge Mode (With Switch Chipset) on page 7-56*.

For the procedure to follow when configuring physical interfaces for Routing Mode, see *Editing Network Interfaces for Routing Mode on page 7-61*.

Procedure

1. Go to **Network** > **Interface**.
2. Click the name of the L2 interface that you would like to edit.

   The **Add/Edit Interfaces** screen opens.
3. For **MTU**, enter the desired MTU.

   Range is 576-1504. The MTU configured on the physical interface is separate from the MTU configured on the bridge interface (br0). You cannot configure an MTU on the bridge interface (br0) that is lower than the MTU configured on a physical interface.
4. Click **Apply**.

Editing Network Interfaces for Bridge Mode (With Switch Chipset)

When in Bridge Mode, you can configure the physical L2 interfaces (WAN, LAN1-LAN8) on the Cloud Edge gateways with hardware switch chipset. You must use the on-premises console for this procedure. You can configure settings such as MTU, storm control, and flow control, depending on the interface and the Intranet Security mode.

Gateways with hardware switch chipset have unique bypass capabilities in Bridge Mode during events such as upgrades, restarts, power off, and system panic. The bypass capabilities are determined by the interface. To help you determine how to assign endpoints to each interface, see *Bypass Ports on Gateways with Hardware Switch Chipset on page 7-15*.

Note

For the procedure to follow when configuring physical L2 interfaces for Bridge Mode or Software Switch, see *Editing Network Interfaces for Bridge Mode/ Software Switch on page 7-55*.

For the procedure to follow when configuring physical L3 interfaces for Routing Mode, see *Editing Network Interfaces for Routing Mode on page 7-61*.

Procedure

1. Go to **Network** > **Interface**.
2. Click the WAN interface under **Name** and configure MTU settings.

Option	Description
Type	Read-only field. **Type** cannot be changed and the WAN interface cannot be removed from the switch configuration.
MTU	Specify a value from 576 through 1504. You cannot configure jumbo frames for the WAN interface. MTU is the only editable field on the WAN interface.

3. Click the name of the L2 interface (LAN1-LAN8) that you would like to edit under **Name** and configure the editable interface settings.

High Security mode and **Balanced** mode

Option	Description
Type	Read-only field. **Type** cannot be changed and the WAN interface cannot be removed from the switch configuration.
MTU	Range: 576-9216; Default 1504 The MTU configured on the physical interface is separate from the MTU configured on the switch interface (sw0). You cannot configure an MTU on the switch interface (sw0) that is lower than the MTU configured on a physical interface.
Storm Control Threshold	Specify the threshold (Mbps) as an integer.
Storm Control Mode	Select the packets types on which to apply storm control: • **Multicast** • **Broadcast**

High Speed mode

Note

You cannot modify MTU in **High Speed** mode. MTU is preset to accept jumbo frames.

Option	Description
Type	Read-only field. **Type** cannot be changed and the WAN interface cannot be removed from the switch configuration.
Flow Control	Select **Enable** to enable flow control.
Storm Control Threshold	Specify the threshold (Mbps) as an integer.
Storm Control Mode	Select the packets types on which to apply storm control: • **Unknown Unicast** • **Multicast** • **Broadcast**

4. Click **Apply**.

List of Interface Settings: Bridge Mode (With Switch Chipset)

Before you configure physical interfaces (WAN, LAN1-LAN8) for your Cloud Edge gateway with hardware switch chipset, you can review the available settings for each Intranet Security mode (High Security,Balanced, and High Speed). You must use the on-premises console to configure the WAN, LAN1-LAN8 interfaces.

For more information about network security provided by each mode, see *Security Protections Provided by Each Intranet Security Mode on page 6-61*.

High Security Mode

Setting	Description
Type	Set to **L2**. Read-only field in Bridge Mode. Type cannot be changed and the WAN/LAN1-LAN8 interfaces cannot be removed from the switch configuration.
MTU	Can configure for High Security and Balanced modes. Jumbo frame support for LAN1-LAN8. Range: 576-9216; Default 1504. **Note** WAN MTU range is 576-1504.
Storm Control Threshold	Can configure for all security modes. The threshold applies separately to each type of storm control. For example, if set to 20, the multicast threshold and the broadcast threshold are each set to 20.
Storm Control Mode: Multicast	Can configure for all security modes.
Storm Control Mode: Broadcast	Can configure for all security modes.

Balanced Mode

Setting	Description
Type	Set to **L2**. Read-only field in Bridge Mode. Type cannot be changed and the WAN/LAN1-LAN8 interfaces cannot be removed from the switch configuration.

Setting	Description
MTU	Can configure for High Security and Balanced modes. Jumbo frame support for LAN1-LAN8. Range: 576-9216; Default 1504. **Note** WAN MTU range is 576-1504.
Storm Control Threshold	Can configure for all security modes. The threshold applies separately to each type of storm control. For example, if set to 20, the multicast threshold and the broadcast threshold are each set to 20.
Storm Control Mode: Multicast	Can configure for all security modes.
Storm Control Mode: Broadcast	Can configure for all security modes.

High Speed Mode

Setting	Description
Type	Set to **L2**. Read-only field in Bridge Mode. Type cannot be changed and WAN/LAN1-LAN8 interfaces cannot be removed from the switch configuration.
MTU	Field not displayed when set to High Speed mode. You cannot change MTU for LAN interfaces in High Speed mode; however, MTU for LAN1-LAN8 is preset to accept jumbo frames. WAN MTU range is 576-1504.
Flow Control	Setting is for High Speed mode only.
Storm Control Threshold	Can configure for all security modes. The threshold applies separately to each type of storm control. For example, if set to 20, the unknown unicast threshold, the multicast threshold, and the broadcast threshold are each set to 20.

Setting	Description
Storm Control Mode: Unknown Unicast	Setting is for High Speed mode only.
Storm Control Mode: Multicast	Can configure for all security modes.
Storm Control Mode: Broadcast	Can configure for all security modes.

Note

The MGMT interface is configured from Cloud Edge Cloud Console.

If you deploy a gateway with hardware switch chipset in Routing Mode, configure the gateway in the same way that you configure all other Cloud Edge models that are set to Routing Mode.

Editing Network Interfaces for Routing Mode

Before registering a Cloud Edge gateway in Routing Mode, you can use the on-premises console to configure all L3 physical interfaces. After the Cloud Edge gateway is registered to Cloud Edge Cloud Console, you can edit only the WAN and LAN1 physical interfaces from the on-premises console.

Note

For the procedure to follow when configuring physical interfaces for Bridge Mode or Software Switch, see *Editing Network Interfaces for Bridge Mode/ Software Switch on page 7-55*.

For the procedure to follow when configuring physical interfaces for Bridge Mode (With Switch Chipset), see *Editing Network Interfaces for Bridge Mode (With Switch Chipset) on page 7-56*.

Procedure

1. Go to **Network** > **Interfaces**.
2. Click an interface's name.

3. Configure the interface settings based on the interface mode.

   The WAN and LAN1 interfaces can use static, DHCP, or PPPoE addressing.

   - For a static address, configure the applicable parameters:

Option	Description
Type	Select **L3**.
Mode	Select **Static**.
MTU	Specify a value from 576 through 1500.
MSS	Select **Overwrite** and specify a value from 536 through 1460.  **Note** The MSS value must not be greater than (MTU - 40).
IPv4 address	Specify the IPv4 address (example: `10.10.10.23`).
IPv4 netmask	Specify the IPv4 subnet mask (example: `255.255.254.0`).
IPv4 default gateway	Specify the IPv4 default gateway (example: `10.10.10.1`). This settings is only required for WAN configurations.

   - For DHCP, configure the applicable parameters:

Option	Description
Type	Select **L3**.
Mode	Select **DHCP**.
MTU	Specify a value from 576 through 1500.
MSS	Select **Overwrite** and specify a value from 536 through 1460.  **Note** The MSS value must not be greater than (MTU - 40).

   - For PPPoE, configure the following parameters:

Note

You cannot configure the MTU or MSS when using PPPoE.

Option	Description
Type	Select **L3**.
Mode	Select **PPPoE**.
User name	Specify the user name provided by the Internet Service Provider. **Note** You can specify up to three ISP accounts. If the Primary ISP account is unavailable, Cloud Edge automatically connects to the network using the Secondary ISP account, or the Tertiary ISP account. Cloud Edge switches back to the Primary ISP account as soon as the service through this connection is restored.
Password	Specify the password provided by the Internet Service Provider.
PPPoE Advanced Settings	Specify the following: • On-demand idle time (in seconds): This setting enables the Cloud Edge gateway to disconnect the Internet connection after it is inactive for the time specified. If the Cloud Edge gateway terminates the Internet connection due to inactivity, it restores the connection as soon as you attempt to access the Internet. This option is disabled by default. • Connection timeout (in seconds): This setting enables the Cloud Edge gateway to periodically check for the Internet connection. If the Internet connection is not available, the gateway will automatically re-establish the connection. This option keeps the gateway connected to the Internet continuously, even if the connection stays idle. This option minimizes your Internet connection response time since it will always be connected. The default value for this setting is 30 (seconds).

4. If the gateway is not registered, configure administrative access for the interfaces.

Select which management services and traffic to allow (On-Premises Console, Ping, SSH, SNMP). You can use selected services to manage the Cloud Edge gateway from the internal network. Enabling On-Premises Console management services provides log on access by authorized users to the on-premises console.

Note

You can configure administrative access from the on-premises console only if the Cloud Edge gateway is not registered. After the gateway is registered, this field is read-only, and you must configure administrative access from Cloud Edge Cloud Console.

Although you can enable management services on the Cloud Edge gateway's WAN interfaces, it is not recommended. You should enable management services and traffic on internal interfaces only.

5. Under the **Monitor Settings** section, specify the hosts (IP address or domain name) you want Cloud Edge to monitor.

   If the Cloud Edge gateway is unable to access a host, it terminates the current connection, and establishes the connection using the next ISP account configured. If any of the hosts are unavailable, Cloud Edge disables the static routes or policy-based routes associated with the interface. However, if the primary connection is restored, Cloud Edge terminates the active connection and re-establishes the primary connection.

   For more information, see *Using Monitoring Hosts to Determine if Routes Are Available on page 7-65*.

6. Under the **Bandwidth Settings** section, specify the following:

   - **Downstream**: The maximum download speed through the port. The default value is blank.
   - **Upstream**: The maximum upload speed through the port. The default value is blank.

   For more information, see *Using Interface Bandwidth Settings to Limit Traffic on page 7-66*.

7. Click **Apply**.
8. Verify the updates in the interface list at **Network** > **Interfaces**.

Using Monitoring Hosts to Determine if Routes Are Available

Monitoring Hosts

Cloud Edge checks whether a WAN works by pinging the corresponding monitor IP address or host name from each egress interface. If the monitoring hosts are unreachable, any static routes or policy-based routes associated with the interface are disabled. If the traffic matches another route, the traffic routes to other static routes or policy-based routes. If the traffic does not match another route, it is routed via the default gateway or discarded.

- To configure the monitoring hosts, see *Configuring Monitoring Hosts On an Interface on page 7-65*.
- To configure the default gateway, see *Adding a Static Route on page 6-80*.
- To configure a policy-based route, see *Adding a Policy-based Route on page 7-93*.

For information about automatic failover, see *Automatic Failover for Multiple ISP/WAN Environments on page 7-92*.

Configuring Monitoring Hosts On an Interface

Procedure

1. Go to **Network** > **Interfaces**.

> **Note**
> Prior to registering the Cloud Edge gateway to Cloud Edge Cloud Console, you can configure monitoring hosts on all interfaces. After registration, you can configure monitoring hosts only for the WAN and LAN1 interfaces.

2. Click an interface's name.
3. Click on **Monitor Settings**.

   The **Monitor Settings** section opens.
4. Select **Enable Interface Monitoring**.
5. Add the IP addresses of the hosts to monitor the interface.
6. Click **Apply**.

Using Interface Bandwidth Settings to Limit Traffic

Configure interface bandwidth settings to set the maximum thresholds for downstream and upstream traffic. Bandwidth control policies cannot exceed the interface bandwidth threshold. By default, Cloud Edge does not limit the bandwidth. Each interface can be configured with different thresholds.

Network congestion may occur when interface bandwidth settings are incorrectly allocated. Trend Micro recommends setting the interface bandwidth to the maximum thresholds allowed by that interface, and to then set bandwidth control policies that determine which traffic has higher priority.

To configure interface bandwidth settings, go to **Network** > **Interfaces**. For more information, see the Cloud Edge on-premises console topic *Editing Network Interfaces for Routing Mode on page 7-61*.

Note

Prior to registering the Cloud Edge gateway to Cloud Edge Cloud Console, you can configure bandwidth settings on all Routing Mode interfaces. After registration, you can configure bandwidth settings only for the WAN or LAN1 interfaces.

Managing VLANs

How VLANs Work

A Virtual Local Area Network (VLAN) is a group of endpoints, servers, and other network devices that communicate as if they are on the same LAN segment, regardless of their location. Endpoints and servers can belong to the same VLAN even though they are geographically scattered and connected to numerous network segments.

A VLAN segregates devices logically, not physically. Each VLAN is treated as a broadcast domain. Devices in VLAN 1 can connect with other devices in VLAN 1, but cannot connect with devices in other VLANs. Communication among devices on a VLAN is independent of the physical network.

A VLAN segregates devices by adding `802.1Q` VLAN tags to all packets sent and received by the devices in the VLAN. VLAN tags are 4-byte frame extensions that contain a VLAN identifier as well as other information.

Adding/Editing VLAN Subinterfaces

You can add L3 VLAN subinterfaces to the Cloud Edge **eth0** and **eth1** interfaces that receive VLAN-tagged packets. You must configure each L3 VLAN subinterface with a unique IPv4 address and netmask. You can edit VLAN interfaces if needed.

Note

You cannot add VLAN subinterfaces to wireless interfaces.

Procedure

1. Review the important information about how VLANs work with Cloud Edge gateways before adding a VLAN subinterface.

   How to Deploy Cloud Edge With VLANs on page 6-63

2. Go to **Network** > **Interfaces**.
3. Perform the appropriate action:
   - To add a VLAN, click the VLAN add configuration icon (⊞) in the **Action** column.

- To edit a VLAN, click the VLAN name in the **VLAN** section.

4. Specify VLAN settings.
   - **Name**: Name the VLAN interface.
   - **Type**: L3 VLAN displays automatically and is read-only.

     L2 VLANs are not supported.
   - **Mode**: Select either **DHCP** or **Static**.

     For static, specify **IPv4 address** and **IPv4 netmask**.
   - **VLAN ID**: Specify the VLAN ID, which must match the VLAN ID of the packets received by this VLAN interface.

     Each VLAN interface VLAN ID must match the VLAN ID added by the IEEE 802.1Q-compliant router or switch connected to the VLAN interface. The VLAN ID can be any number between 1 and 4094 (0 and 4095 are reserved).

     You cannot change the VLAN ID of an existing VLAN interface.

Managing Wireless Networks

Manage wireless networks using the Cloud Edge on-premises console.

Wireless Network Overview

You can configure a main wireless network and guest wireless networks on supported Cloud Edge gateways. You should understand how you can deploy and configure wireless networking and what gateway functionality is available for wireless networks.

General Information

You can use the following general information when you set up wireless networking:

- Wireless networks are supported in Routing Mode only.

If you change from Bridge Mode to Routing Mode, wireless network settings are set to default settings.

- Both the main and guest wireless networks are disabled by default.
- By default, if the guest wireless network is enabled, clients on the guest wireless network cannot access resources on the main wireless or local internal networks.

  You can enable local access if desired. You should keep in mind security considerations before allowing guest access to internal resources.
- Supports 2.4 GHz or 5 GHz network frequency (but not both simultaneously).

  Default is 2.4 GHz.
- Supports 20 wireless client connections.

Wireless Network Setup and Configuration

You can use the following methods to set up and configure wireless networks on Cloud Edge gateways:

- You can do basic setup of the main wireless network from the **Quick Setup** screen.
- After the initial setup, you can manage the wireless network configuration in the following locations:
  - Cloud Edge on-premises console: Configure general settings, the main wireless network, and the guest wireless network.
  - Cloud Edge Cloud Console: Configure wireless network access control settings and manage wireless client connections.

Note

While you can view the guest and wireless network configuration from Cloud Edge Cloud Console, you must use the on-premises console to change the configuration.

Wireless Network Interface Configuration

You can edit wireless network interfaces:

- Configure and view information about wireless interfaces from Cloud Edge Cloud Console.
- You can configure the main and guest wireless interfaces with static IP addresses from the **Interfaces** page.

  VLANs are not supported on wireless interfaces.

  Note

  If a wireless interface is not enabled, it is visible on the **Interfaces** page, but the interface status is down.

- Use the **Gateway Information** page to view information about wireless interface status and statistics.

  If wireless networking is not enabled for the main or guest wireless network, interface status is “Down” for the respective interface.

Wireless Network and Related Network Functionality

You can set up and configure related functionality for the wireless networks such as administrative access, static routes, DHCP access, NAT, bandwidth control, VPNs, and endpoint protection:

- Enable administrative access using Cloud Edge Cloud Console.

  You can enable administrative access on the main and guest wireless networks, but you should be cautious about enabling access on the guest wireless network.

- Configure static routes from Cloud Edge Cloud Console.
- Configure DHCP services from Cloud Edge Cloud Console.
  - You can configure DHCP services on the main wireless and guest wireless networks.
  - Wireless interfaces are visible on the **DHCP** page whether the respective guest or main wireless networks are enabled or disabled.

DHCP services are enabled by default with a default IP address pool.

- Configure NAT from Cloud Edge Cloud Console.
  - You can configure NAT on the main and guest wireless networks.
  - Wireless interfaces are visible on the **NAT** page whether the respective guest or main wireless networks are enabled or disabled.

    Destination NAT rules: Choose a wireless interface as the ingress interface.

    Source NAT rules: Choose a wireless interface as the egress interface.
- Configure bandwidth control.
  - You can configure bandwidth control to include the main wireless and guest wireless networks.
  - To apply bandwidth control on traffic from the wireless networks, use **Any** as the source or destination bandwidth control parameter or configure selected address objects that include the IP addresses from the wireless network on which to apply bandwidth control.
- Configure VPN Access from Cloud Edge Cloud Console.
  - You can configure user VPN or Site-to-Site on the main wireless and guest wireless networks.
  - To create VPNS on the wireless networks, create and use network objects that contain the desired wireless network IP addresses.

    A wireless network (main or guest) must be enabled to create VPNS on that wireless network.
- You can configure network access control (endpoint protection).

  Clients on the wireless networks are protected when you configure WFBSS Endpoint Protection and Endpoint Protection from Suspicious Clients for the selected gateway.

Wireless Networks and Cloud Edge Security

Wireless networks are protected by Cloud Edge security, which you can configure using Cloud Edge Cloud Console:

- Policy objects

  When configuring policy objects, you can use wireless network IP addresses or MAC addresses.

- Policies

  Use source or destination parameters to include address objects containing the main and guest wireless networks or users and groups logged on through the wireless networks.

- HTTPS Inspection Rules

  Use decryption source or destination parameters include address objects containing the main and guest wireless networks or users and groups logged on through the wireless networks.

- Approved/Blocked Lists

  The configured approved and blocked list apply to wireless network traffic.

- Security profiles

  The security profile selected for the Cloud Edge gateway applies to wireless network traffic.

- Notifications

  Notifications are sent for violations that occur on wireless network traffic.

Auditing and Diagnostic Support

Wireless networks configurations are audited and certain diagnostic capabilities are available for wireless networks.

- Cloud Edge Cloud Console audit logs: If wireless networking is enabled, the audit log contain entries about wireless configuration changes.

- Cloud Edge on-premises console diagnostics:
  - Perform packet captures on the wireless interfaces (wlan0 and wlan1) or for the wireless protocol (wifi0).

    If wireless networking (main or guest) is not enabled, the respective wireless interfaces are not visible on the packet capture page.
  - Basic Settings and Event Logs category of Diagnostic file collection includes information about wireless networks.
  - Health check provides information about main and guest wireless interface status.

Configuring General Wireless Network Settings

Configure general wireless network settings according to your wireless network requirements. Some general wireless settings apply to the main wireless network, while some settings apply to both the main and guest wireless networks as noted in the following procedure.

Procedure

1. Go to **Network** > **Wireless** > **Wireless Settings** > **General Settings**.
2. Select **Enable main wireless network**.

   Setting applies only to the main wireless network. Default is disabled.

   Selecting this option does not enable the guest wireless network. You must enabled the guest wireless network from the **Guest Network** tab.
3. Configure the following:
   - **Frequency**: Select your wireless network frequency.

     Settings applies to both the main and guest wireless networks.

     Cloud Edge wireless networking can operate at either the 2.4 GHz or 5.0 GHz frequencies. The gateway cannot operate at both frequencies simultaneously. Default is 2.4 GHz.
   - **Enable SSID broadcast**: Select this option if you want to broadcast the main wireless network's SSID.

Settings applies only to the main wireless network.

If enabled, the Cloud Edge gateway broadcasts the main wireless network's **SSID** so that nearby clients can see the network in the available wireless networks screen. Default is enabled.

- **SSID**: Specify a name for the main wireless network's access point.

  Settings applies only to the main wireless network.

  The default **SSID**s are:

  - 2.4 GHz: **CloudEdge-XXYY**
  - 5 GHz: **CloudEdge-5G-XXYY**

Note

XXYY represents the first four characters of the Cloud Edge gateway's serial number. For best security, you should enter a non-default value for **SSID**.

- **Channel**: Specify the channel number.

  Settings applies to both the main and guest wireless networks.

  Channels vary by frequency selection and country/region. The default value is **Auto**.

- **Mode**: Specify the mode.

  Settings applies to both the main and guest wireless networks.

  2.4 GHz: Options include **11bgn mixed** and **11bg mixed**

  5 GHz: Options include **11a only**, **11a/n mixed**, and **11a/n/ac mixed**

- **Security**: Specify the type of security you want to use.

  Settings applies only to the main wireless network.

  - If you select **Open**, you do not need to configure additional security settings.

- If you select the **WPA-PSK[TKIP]**, **WPA2-PSK[AES]**, or **WPA-PSK[TKIP]+WPA2-PSK[AES]** security type, you must also specify a **Pre-shared key**.

Note

The **WPA-PSK[TKIP]** security setting is available only when mode **11bg mixed** (2.4 GHz) or **11a only** (5 GHz) is selected.

- If you select the **WPA/WPA2 Enterprise** security type, you must also specify the **Radius server IP address**, **Radius server port**, and **Radius server secret**.

4. (Optional) If you selected **WPA/WPA2 Enterprise**, click **Test** and enter the user name and password to use when connecting to the radius server to verify that Cloud Edge can connect successfully.

5. Under the **Advanced Settings** section, configure the following advanced wireless settings:

   Advanced settings apply to both the main and guest wireless networks.

   - **DTIM interval**: Specify the DTIM interval. Range is 1 through 255. Default value is `3`.
   - **Beacon interval**: Specify the beacon interval in milliseconds. Range is 100 through 1000. Default value is `100`.
   - **Short preamble**: Enable or disable this option by clicking **Enable** or **Disable**.
   - **RTS threshold**: Specify the RTS threshold between 0 and 2347 bytes. Default value is `2347` bytes.
   - **Enable short GI**: Enable or disable this option by clicking **Enable** or **Disable**.
   - **Transmit power**: Specify the transmit power percentage for the access point. Range is 1 through 100. Default value is `100`.

Note

Short preamble, **RTS threshold**, and **Enable short GI** fields are only available if you choose the a network frequency of 2.4 GHz.

6. Click **Save**.

Configuring Guest Wireless Network Settings

Configure guest wireless network settings according to your wireless network requirements.

Procedure

1. Go to **Network** > **Wireless** > **Wireless Settings** > **Guest Network**.
2. Select **Enable guest network**.

   By default the guest wireless network is not enabled.

Note

The main wireless network must be enabled before you can enable the guest wireless network

3. Enable the options that you want to use for the guest network:
   - **Enable SSID broadcast**

     If enabled, the Cloud Edge gateway broadcasts the guest network's **SSID** so that nearby clients can see the guest wireless network in the available wireless networks screen. Default is enabled.
   - **Enable access to local network**

     If enabled, users on the guest wireless network can access resources on the local internal network, provided they have the appropriate permissions. Default is disabled.
4. Specify the **SSID** for the guest wireless network.

   The default **SSID**s are:

- 2.4 GHz: **CloudEdge-GUEST-XXYY**
- 5 GHz: **CloudEdge-5G-GUEST-XXYY**

Note

XXYY represents the first four characters of the Cloud Edge gateway's serial number. For best security, you should enter a non-default value for **SSID**.

5. Under **Security settings**, specify the type of security you want to use for the guest wireless network.
   - If you select **Open**, you do not need to configure additional security settings.
   - If you select the **WPA-PSK[TKIP]**, **WPA2-PSK[AES]**, or **WPA-PSK[TKIP]+WPA2-PSK[AES]** security type, you must also specify a **Pre-shared key**.

     Note

     The **WPA-PSK[TKIP]** security setting is available only when mode **11bg mixed** (2.4 GHz) or **11a only** (5 GHz) is selected in the **General Settings** tab.

   - If you select the **WPA/WPA2 Enterprise** security type, you must also specify the **Radius server IP address**, **Radius server port**, and **Radius server secret**.
6. (Optional) If you selected **WPA/WPA2 Enterprise**, click **Test** and enter the user name and password to use when connecting to the radius server to verify that Cloud Edge can connect successfully.
7. Click **Save**.

Troubleshooting Wireless Networks

View troubleshooting information for the wireless network.

Procedure

1. Go to **Network** > **Wireless** > **Wireless Settings** > **Troubleshooting**
2. Use the logs to troubleshoot the wireless network.
3. Click on the refresh icon at the top-right corner of the page to update the displayed log entries.

   The maximum number of records displayed is 100.

Managing DNS

You can view and edit the Domain Name Server (DNS) server settings for the Cloud Edge gateway.

Since environments that utilize DHCP or PPPoE to access the Internet might dynamically acquire the DNS configuration from the ISP, you might not be required to configure DNS settings in these environments.

DNS Best Practice Suggestions

Smart Protection Network (SPN) uses cloud-based services and relies on DNS queries for lookups. To ensure fast response and minimum latency, the Cloud Edge device must be configured with a DNS server. You can set up to three DNS servers.

The DNS servers must be able to support the volume of DNS requests made by Cloud Edge. In general, before Cloud Edge builds up its local DNS cache, two DNS requests will be made for each URL accessed. Make sure your DNS server is installed on a server with enough resources and performance to handle the extra DNS volume.

To reduce latency, each DNS server should have a fast network card and be installed on a fast network switch.

Trend Micro recommends on-site DNS servers versus ISP-provided DNS servers that are housed outside of the company's network. In general, ISP DNS servers have higher latency and do not support large numbers of DNS queries from a single IP address. Many ISP DNS servers have throttling

mechanisms that limit the number of DNS requests per second and can affect Cloud Edge's Web Reputation Services (WRS) performance.

To improve network response time and performance, try to place the DNS server as close to the Cloud Edge unit(s) as possible to eliminate unnecessary network hops between the devices.

WRS and URL Filtering requests are made over HTTP port 80. Do not block the Cloud Edge management IP address for these ports on the firewall.

Configuring DNS Settings

Procedure

1. Go to **Network** > **DNS**.
2. Configure applicable DNS server IPv4 addresses.

Note

If Cloud Edge dynamically acquires the DNS from an Internet Service Provider, the **Inherit DNS Information** section appears with read-only DNS information.

3. Click **Apply**.

Managing Address Objects

Address objects determine allowed IP address ranges in the internal network. By default, Cloud Edge uses the Default Internal Addresses address object, which includes all internal IP address ranges (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). Address objects are also used when configuring policy-based routing.

- You can view and edit configured IPv4 address objects on the Cloud Edge on-premises console by going to **Network** > **Addresses**.
- After gateway registration, you cannot add new address objects or delete address objects using the **Network** > **Addresses** page on the Cloud Edge on-premises console.

- You can use Cloud Edge Cloud Console to add, edit, and delete IPv4 address objects to use in network settings and in policy-based routing.

Note

You can add new IPv4 address objects when creating policy-based rules under **Routing**. Address objects added while configuring policy-based routing can later be edited from the **Network** > **Addresses** page.

IP Address Object Parameters

The following table describes the configurable parameters when adding or editing IPv4 objects from the Cloud Edge on-premises console. You can use these IPv4 address objects when configuring policy routing rules from the on-premises console.

TABLE 7-6. Address Object Parameters

PARAMETER	DESCRIPTION
Object name	Specify a name that describes the addresses. This name appears in the address list when defining rules for policy-based routing. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Type	IPv4
Addresses	Specify the IP address or network using the following notation: • `ip_address` • `ip_address_range` • `ip_address/bitmask` Example:192.168.1.1 or 192.168.1.1-192.168.1.10 or 192.168.80.0/24

Viewing Address Objects

Procedure

- Go to **Network** > **Addresses**.

Editing Address Objects

You can use the Cloud Edge on-premises console to edit the IP addresses for an existing IPv4 address object.

There is a default IPv4 address object, “Default Internal Addresses”, configured with the IP addresses 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16.

Procedure

1. Go to **Network** > **Addresses**.
2. Click on the name of the address object that you want to edit.
3. Edit the IP addresses.

   When editing settings for IPv4 address objects, Cloud Edge supports single IP addresses, '-' as a range marker, and IP address/netmask (192.168.1.1/24).

   Example: `192.168.0.1,10.0.0.1-10.0.0.4,192.168.1.1/24`
4. Click **OK**.
5. Verify that the modified address object displays the IP address modifications in the list at **Network** > **Addresses**.

Note

You can edit, but not add new IPv4 address objects on the **Network Addresses** page. However, you can add new IPv4 address objects when creating policy-based rules under **Routing**. Address objects added while configuring policy-based routing can later be edited using this procedure.

Managing Bridge/Switch Settings

You can view and manage the bridge interface (br0) for Bridge Mode/ Software Switch deployments or the switch interface (sw0) for Bridge Mode (With Switch Chipset) from the Cloud Edge on-premises console.

Procedure

1. Perform the appropriate action, depending on the Cloud Edge gateway model.
   a. Go to **Network** > **Bridge**.
   b. Go to **Network** > **Switch**.
2. Under **Name**, perform the appropriate action.
   a. Click on **br0**.
   b. Click on **sw0** for gateways with hardware switch chipset.
3. Do the following:
   - View a summary of the bridge interface (br0) or switch interface (sw0) settings.
   - Click the bridge interface (br0) or switch interface (sw0) name to view more details or to edit settings.

What to do next

Use Cloud Edge Cloud Console to configure Intranet Security mode settings for the switch interface (sw0).

To change the security mode or edit the mode settings, log on to Cloud Edge Cloud Console and go to the **Gateways** > **(Selected Gateway)** > **NETWORK** > **Interfaces** page.

See *Configuring Switch Interface (sw0) Settings on page 6-57*.

Configuring the Bridge Interface (br0)

You can configure settings on the bridge interface (br0) for selected gateways that are in Bridge Mode. The bridge interface (br0) is a virtual interface that you must configure from the Cloud Edge on-premises console.

Note

For the procedure to follow when configuring the bridge interface (br0) for Software Switch, see *Configuring the Bridge Interface (br0) for Software Switch on page 7-85*.

For the procedures to follow when configuring the switch interface (sw0) for Bridge Mode on a Cloud Edge gateway with hardware switch chipset, see the following:

- *Configuring the Switch Interface (sw0) on page 7-88* (from the Cloud Edge on-premises console)
- *Configuring Switch Interface (sw0) Settings on page 6-57* (from Cloud Edge Cloud Console)

Procedure

1. Go to **Network** > **Bridge**.
2. Click on **br0** under **Name**.

   The **Add/Edit Bridge** screen opens.
3. For **Type**, select **Bridge**.

   The **Interface 1** and **Interface 2** fields are read-only and preset as L2 interface with WAN [L2] and LAN1 [L2] preselected respectively.

4. Configure the editable interface settings.

   The bridge interface (br0) can use static or DHCP addressing.

   - For a static address, configure the applicable parameters:

Option	Description
Mode	Select **Static**.
MTU	Specify a value from 576 through 1500.
IPv4 address	Specify the IPv4 address (example: `10.10.10.23`).
IPv4 netmask	Specify the IPv4 subnet mask (example: `255.255.254.0`).
IPv4 default gateway	Specify the IPv4 default gateway (example: `10.10.10.1`). This settings is only required for WAN configurations.

   - For DHCP, configure the applicable parameters:

Option	Description
Mode	Select **DHCP**.
MTU	Specify a value from 576 through 1500.

5. If the gateway is not registered, configure administrative access for the bridge interface (br0).

   Select which management services and traffic to allow (On-Premises Console, Ping, SSH, SNMP). You can use selected services to manage the Cloud Edge gateway from the internal network. Enabling On-Premises Console management services provides log on access by authorized users to the on-premises console.

Note

You can configure administrative access from the on-premises console only if the Cloud Edge gateway is not registered. After the gateway is registered, this field is read-only, and you must configure administrative access from Cloud Edge Cloud Console.

6. Under **Advanced Settings**, optionally select **Enable Spanning Tree Protocol**.

   Cloud Edge uses the Spanning Tree Protocol to detect and prevent loops on the network where the gateway is located. Cloud Edge cannot detect loops that occur on a downstream network or downstream device.

7. Under **Advanced Settings**, optionally select **Enable Link Loss Forwarding**.

8. Click **Apply**.

Configuring the Bridge Interface (br0) for Software Switch

You can configure software switch settings on the bridge interface (br0) for selected gateways that are deployed as a Software Switch (a variation of Bridge Mode). The bridge interface (br0) is a virtual interface that you must configure from the Cloud Edge on-premises console.

- For a Software Switch deployment, the Cloud Edge gateway deployment mode switch is set to **Bridge** and you configure the bridge interface (br0) with IP address settings the same as you do with a basic Bridge Mode deployment.
- You must additionally add at least three physical interfaces to act as the L2 interfaces of a software switch. WAN and LAN1 are required ports. You can add either LAN2, and LAN3 as the third software switch interface. You can add both the LAN2 and LAN3 ports if desired.

Note

For the procedure to follow when configuring a bridge interface (br0) for Bridge Mode, see *Configuring the Bridge Interface (br0) on page 7-83*.

For the procedures to follow when configuring the switch interface (sw0) for Bridge Mode on a Cloud Edge gateway with hardware switch chipset, see the following:

- *Configuring the Switch Interface (sw0) on page 7-88* (from the Cloud Edge on-premises console)
- *Configuring Switch Interface (sw0) Settings on page 6-57* (from Cloud Edge Cloud Console)

Procedure

1. Go to **Network** > **Bridge**.
2. Click on **br0** under **Name**.

   The **Add/Edit Bridge** screen opens.
3. For **Type**, select **Software Switch**.

   Additional parameters that are used when configuring a Software Switch deployment become available.
4. Under **Switch Interfaces**, select which physical interfaces to include in the software switch.
   - **WAN[L2]** and **LAN1[L2]** are required and are preselected as read-only selections.
   - You must choose at least one of **LAN2[L2]** or **LAN3[L2]**. You can choose both **LAN2[L2]** and **LAN3[L2]**.
5. Choose the **Mode** used to configure the bridge interface (br0).

   Choose either **Static** or **DHCP**.
6. (Optional) Change the software switch **MTU**.

   The default is 1438. The range is 576-1500.

You can also modify the MTU of the physical interfaces on the Cloud Edge gateway. The MTU configured for the software switch cannot be larger than the MTU configured on the physical interfaces.

7. If **Mode** is **Static** configure the applicable IPv4 interface settings.

Option	Description
IPv4 address	Specify the IPv4 address (example: `10.10.10.23`).
IPv4 netmask	Specify the IPv4 subnet mask (example: `255.255.254.0`).
IPv4 default gateway	Specify the IPv4 default gateway (example: `10.10.10.1`). This settings is only required for WAN configurations.

8. If the gateway is not registered, configure administrative access for the bridge interface (br0).

   Select which management services and traffic to allow (On-Premises Console, Ping, SSH, SNMP). You can use selected services to manage the Cloud Edge gateway from the internal network. Enabling On-Premises Console management services provides log on access by authorized users to the on-premises console.

Note

You can configure administrative access from the on-premises console only if the Cloud Edge gateway is not registered. After the gateway is registered, this field is read-only, and you must configure administrative access from Cloud Edge Cloud Console.

9. Under **Advanced Settings**, optionally select **Enable Spanning Tree Protocol**.

   Cloud Edge uses the Spanning Tree Protocol to detect and prevent loops on the network where the gateway is located. Cloud Edge cannot detect loops that occur on a downstream network or downstream device.

10. Click **Apply**.

Configuring the Switch Interface (sw0)

You can configure settings on the switch interface (sw0) for selected Cloud Edge gateways with hardware switch chipset that are in Bridge Mode. The switch interface (sw0) is a virtual interface that you configure from the Cloud Edge on-premises console.

Note

For the procedure to follow when configuring a bridge interface (br0) for Bridge Mode, see *Configuring the Bridge Interface (br0) on page 7-83*.

For the procedure to follow when configuring a bridge interface (br0) for Software Switch, see *Configuring the Bridge Interface (br0) for Software Switch on page 7-85*.

Procedure

1. Go to **Network** > **Switch**.
2. Click on **sw0** under **Name**.

   The **Add/Edit Switch** screen opens.

   - The **Name** field is read-only and is set to **sw0**.
   - The **Intranet Security mode** field is read-only and is set to **High Security**.

     You can make changes to the Intranet Security mode using Cloud Edge Cloud Console.
3. For **Mode**, select **DHCP** or **Static**.
4. If mode is **Static**, enter the IPv4 address, IPv4 netmask, and IPv4 default gateway.
5. Optionally, configure **MTU**.

   Specify a value from 576 through 1500. Default is 1438.
6. If the gateway is not registered, configure administrative access for the switch interface (sw0).

Select which management services and traffic to allow (On-Premises Console, Ping, SSH, SNMP). You can use selected services to manage the Cloud Edge gateway from the internal network. Enabling On-Premises Console management services provides log on access by authorized users to the on-premises console.

Note

You can configure administrative access from the on-premises console only if the Cloud Edge gateway is not registered. After the gateway is registered, this field is read-only, and you must configure administrative access from Cloud Edge Cloud Console.

7. (**High Security** mode and **Balanced** mode only): Under **Advanced Settings**, optionally perform the following:
   a. Select **Enable Spanning Tree Protocol**.

      Cloud Edge uses the Spanning Tree Protocol to detect and prevent loops on the network where the gateway is located. Cloud Edge cannot detect loops that occur on a downstream network or downstream device.

   b. Select **IGMP Snooping**.
8. Click **Apply**.

What to do next

Configure additional switch interface (sw0) settings from the Cloud Edge Cloud Console, such as the Intranet Security mode.

See *Configuring Switch Interface (sw0) Settings on page 6-57*.

Managing Routing

Cloud Edge gateways work as security devices on a network, with all packets passing through them. You must understand certain basic routing concepts to configure the Cloud Edge gateway appropriately.

The Cloud Edge gateway has a pre-defined default static route. When the network traffic does not match any policy-based routing rule or a configured static route, a pre-defined static route is used as an IPv4 default gateway (static route to 0.0.0.0/0), which then applies to all traffic.

Instead of or in addition to the pre-defined default static route, you can configure the following to control how traffic is routed:

- IPv4 policy-based routes if you want to manually control how traffic is routed in your environment
- IPv4 static routes
- IPv4 default gateways on each interface

Important

You must configure at least one default gateway to connect with Cloud Edge Cloud Console.

Cloud Edge selects routes and updates its routing table dynamically based on the specified rules. Given a set of rules, Cloud Edge can determine the best route or path for sending packets to a destination.

Note

Cloud Edge does not support IPv6 routing.

Information About Where to Configure Routes

You can use the following information to configure routes that control how traffic is routed on the Cloud Edge gateway:

- IPv4 policy-based routes

  You must use the Cloud Edge on-premises console to configure policy-based routing. For more information, go to *Adding a Policy-based Route on page 7-93*.

- IPv4 static routes

You must use Cloud Edge Cloud Console to configure static routes. To configure a static route (including default routes for the gateway), go to *Adding a Static Route on page 6-80*.

- IPv4 default gateways on each interface

  To configure default gateways on the WAN or LAN1 interfaces using the Cloud Edge on-premises console, go to *Editing Network Interfaces for Routing Mode on page 7-61*.

  To configure default gateways on the other LAN interfaces and the MGMT interface using Cloud Edge Cloud Console, go to *Routing Mode: Editing Network Interfaces on page 6-51*.

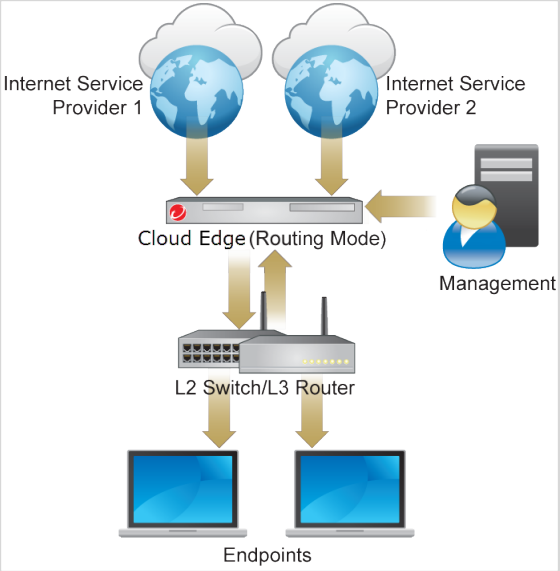
About Policy-based Route Management

In today's high performance networks, organizations need the freedom to implement packet forwarding and routing according to their own defined policies in a way that goes beyond traditional routing protocol concerns. While static and dynamic routing focus on the traffic destination for routing, policy-based routing provides a mechanism to mark packets so that certain kinds of traffic receive differentiated routing. Destination-based routing techniques make it difficult to change the routing behavior of specific traffic. Also known as “intelligent routing”, policy-based routing allows you to dictate the routing behavior based on a number of different criteria other than destination network, including source interface, source or destination address, or service type.

Consider a company that has two links between locations, one a high bandwidth, low delay expensive link and the other a low bandwidth, higher delay lower expense link. Using traditional routing protocols, the higher bandwidth link would get most if not all of the traffic sent across it based on the metric savings obtained by the bandwidth and/or delay (using EIGRP or OSPF) characteristics of the link. Policy-based routing can route higher priority traffic over the high bandwidth/low delay link while sending all other traffic over the low bandwidth/high delay link.

With policy-based routing, Cloud Edge can route traffic from multiple ISPs and WANs. The following illustration shows how to configure Cloud Edge for two ISPs using an L2 switch.

FIGURE 7-9. Policy-based Routing Example



If the monitoring IP addresses of one interface are unavailable, all policy-based routes associated with that interface are disabled. All traffic matching the policy-based routing rules is routed via the default gateway. To configure the monitoring IP addresses, go to *Monitoring Hosts on page 7-65*. If multiple default gateways are configured, then outgoing traffic is routed from these gateways using round-robin selection.

Automatic Failover for Multiple ISP/WAN Environments

Cloud Edge supports automatic failover among multiple WAN/ISP links when an ISP or WAN connection fails. Cloud Edge checks the connection every ten (10) seconds. If Cloud Edge cannot detect a connection, Cloud Edge

continues to check every two (2) seconds. After four (4) consecutive unsuccessful connection attempts, automatic failover initiates. The link automatically recovers if a connection is established later.

When a failover occurs, do the following:

- View the system event log
- Check the routing table to verify the actual traffic routing

Note

For more information about monitoring hosts, see *Monitoring Hosts on page 7-65*.

Adding a Policy-based Route

You can configure IPv4 policy-based routes if you want to manually control how traffic is routed in your environment.

Procedure

1. Go to **Network** > **Routing** > **Policy Routing**.
2. Click **Add New**.
3. Optionally enable the rule.
4. Specify a policy name between 1 and 32 characters, consisting of letters, numbers, or underlines.
5. Type an optional **Description**.
6. Under **Source Addresses**, select one of the following parameters:
   - **Any:** Includes all source addresses. (Default)
   - **Selected addresses:** Displays a selectable list of previously configured source addresses and the **Add New** icon () to add a new IPv4 address object, if needed.

     To configure a new IP address object, go to *Adding a new IPv4 Address Object for Policy Routing on page 7-94*.

7. Select the appropriate source interface from the **Source Interface** drop-down box.
8. Under **Destination Addresses**, select one of the following parameters:
   - **Any:** Includes all destination addresses. (Default)
   - **Selected addresses:** Displays a selectable list of previously configured destination addresses and the **Add New** icon () to add a new IPv4 address object, if needed.

     To configure a new IP address object, go to *Adding a new IPv4 Address Object for Policy Routing on page 7-94*.
9. Under **Service type**, select one of the following parameters:
   - **Any:** Include all services
   - **Selected:** Include only selected services
10. Select the egress interface.
11. For interfaces with static IP addresses, specify the next hop.
12. Optionally enable network masquerading.

Note

Select **Enable Network Masquerade** if internal IP addresses must be translated to the IP address of the egress interface.

13. Click **OK**.

Adding a new IPv4 Address Object for Policy Routing

You can add a new IPv4 address object when configuring a rule for policy-based routing.

Note

You cannot configure IPv6 address objects when adding an address object to a policy routing rule.

Procedure

1. Go to **Network** > **Routing** > **Policy Routing** and click **Add New** to open the **Add a Policy Routing Rule** window.
2. In the **Add a Policy Routing Rule** window, select **Selected Addresses** in either **Source Addresses** or **Destinations Addresses**.
3. Click **Add New**.

   The **Add/Edit Address Object** screen opens.
4. Specify a name for the address object.
5. IPv4 is the only option and is preselected in the **Protocol** list box.
6. Specify the IP address or CIDR network (single or comma delimited).

   When configuring settings for IPv4 address objects, Cloud Edge supports single IP addresses, '-' as a range marker, and IP address/netmask (192.168.1.1/24).

   Example: 192.168.0.1,10.0.0.1-10.0.0.4,192.168.1.1/24
7. Click **OK**.

Routing Table

In the factory default configuration, the Cloud Edge routing table contains a single static IPv4 default route. Add routing information to the routing table by defining additional IPv4 static routes. The table may include several different routes to the same destination—the IPv4 addresses of the next-hop router specified in those routes or the Cloud Edge interfaces associated with those routes may vary.

Cloud Edge evaluates the information in the routing table and selects the best route to a destination, typically the shortest distance between the Cloud Edge gateway and the closest next-hop router. In some cases, a longer route is selected if the best route is unavailable. Cloud Edge installs the best available routes in the unit's forwarding table, which is a subset of the unit's routing table. Packets are forwarded according to the information in the forwarding table.

Note

Cloud Edge does not support IPv6 routing.

Viewing the Routing Table

Procedure

1. Go to **Network** > **Routing** > **Routing Table**.
2. View the IPv4 routes.

Routing Table Indicators

The following table explains routing table indicators.

Code	Definition
K	Kernel route
C	Connected
S	Static

Managing DHCP and DDNS Services

The Cloud Edge gateway supports Dynamic Host Configuration Protocol (DHCP) and Dynamic DNS (DDNS) services.

Dynamic Host Configuration Protocol (DHCP)

You can enable Dynamic Host Configuration Protocol (DHCP) services on one or more LAN interfaces on the Cloud Edge gateway. Each interface that has DHCP services enabled acts as a DHCP server that can assign IPv4 addresses and other network settings such as a default gateway and DNS (IPv4) settings to internal clients.

You can also configure DCHP advanced server settings (IPv4 address static mappings and DHCP lease times) for each DHCP server.

Cloud Edge automatically responds to DHCP requests to interfaces configured with DHCP services.

- To configure DHCP services using the Cloud Edge on-premises console, see *Modifying DHCP Service Settings on page 7-98*.
- To configure DHCP services using Cloud Edge Cloud Console, see *Editing DHCP Settings on page 6-71*.

Dynamic DNS (DDNS)

Dynamic DNS (DDNS) automatically updates Internet DNS name servers in real-time to keep the active DNS configuration of host names, IPv4 addresses, and other information up to date.

You can configure DDNS services on the Cloud Edge gateway's WAN interfaces. You must use Cloud Edge Cloud Console to configure dynamic DNS. For details, see *Dynamic DNS on page 6-75*.

Viewing DHCP Services and Settings

Procedure

1. Go to **Network** > **Services** > **DHCP**.
2. In the table, view the parameters associated with any DHCP service:

Option	Description
Name	Name of the DHCP service (example: LAN1).
IP Address/ Netmask	The IPv4 address and subnet mask assigned to the interface.
Enable	The icon indicates the state of the service: enabled (green/on) or disabled (red/off).
IP Pools	Range of applicable IPv4 addresses that the DHCP service can lease to clients.

Option	Description
Options	The DNS server IPv4 address, the gateway IPv4 address, and the lease time. The DNS IPv4 address shows only when the DHCP server uses a specified DNS.
Action	Click the icon to edit the DHCP service settings.

Modifying DHCP Service Settings

Procedure

1. Review the following information as needed:
   - *Deployment Mode Information for DHCP on page 6-73*
   - *Default DHCP IP Address Pools on page 6-74*
2. Go to **Network** > **Services** > **DHCP**.
3. Do one of the following:
   - In the **Name** column, click the name of the DHCP server to modify.
   - In the **Action** column, click the edit icon ( ) in the row of the DHCP service to modify.
4. Configure DHCP settings.

   See *Default DHCP IP Address Pools on page 6-74* for information about the following:
   - Deployment mode specific information about interfaces you can configure as DHCP servers.
   - What IP addresses are assigned by default to each IP address pool.

Option	Description
Enable DHCP	Select to enable the service.

Option	Description
IP address / Netmask	The IPv4 address and subnet mask assigned to the interface.
Preferred DNS	Select the preferred DNS method. • Select **Use system DNS settings** to use the gateway system DNS configured at **Network** > **DNS**. • Select **Use the interface IP address** to use the interface IPv4 address as the DNS. • Select **Use specified DNS servers** to manually configure IPv4 addresses as the DNS settings.
Gateway	The DHCP server gateway automatically populates based on interface IPv4 address and netmask settings. Optionally change the IPv4 gateway address.
IP address range from and to	Specify the range of IPv4 addresses to create the IP address pool to which the DHCP configuration applies. **Note** Cloud Edge does not support IPv6 address pools.

5. Configure **Advanced Settings**.

Option	Description
Lease Time	For **Lease time**, adjust the time and date when the leased IPv4 address and netmask are no longer valid. Specify days, hours, or minutes. For example, if you specify only hours, then the lease is restricted to that number of hours.

Static Mapping	You can use static mapping to manually bind a static IPv4 address to a specific MAC address.
	For **Static mapping**, specify MAC address / IPv4 address maps. You can enter multiple maps. Example:
	`00:0C:29:A9:69:25 maps to 192.168.2.1`
	`00-FF-8A-B9-5A-49 maps to 192.168.1.1`

6. Click **Apply**.
7. Verify the settings changed at **Network** > **Services** > **DHCP**.

Performing Administration Tasks

You can perform the following administrative tasks from the Cloud Edge gateway on-premises console:

- Choose between English and Simplified Chinese language settings
- Configure global system settings
  - Configure the host name and time settings
  - Manage how users access the Cloud Edge on-premises console
  - Configure proxy settings
- Manage Cloud Edge device settings
- Perform updates
- View device logs
- Perform maintenance tasks
- Perform diagnostics tests and view health check information
- Learn how to contact support

Switching the Language Settings

The Cloud Edge on-premises console offers English and Japanese language support.

Procedure

1. Expand the drop-down list box at the upper right corner of the Cloud Edge on-premises console.
2. Select the appropriate language.

Managing Global System Settings

You can manage global system settings for the Cloud Edge gateway, such as the host name and the time and date settings. Other advanced settings include setting session timeouts for the Cloud Edge on-premises console and specifying proxy settings.

Configuring the Host Name and Time Settings

You can configure the host name and time and date settings for the Cloud Edge gateway from either the Cloud Edge on-premises console or by using the Cloud Edge gateway's **Quick Setup** screen.

Procedure

1. Log on to the Cloud Edge on-premises console.
2. Perform one of the following actions:

Option	Description
To use the Cloud Edge on-premises console	Go to **Administration** > **System Settings** > **General** tab.
To use the **Quick Setup** screen	Click the **Quick Setup** link at the top-right of the Cloud Edge on-premises screen and go to the **System settings** section.

3. Configure the following:

Option	Description
Host name	Specify a host name.
Enable NTP server	Select this option if you want to synchronize with the NTP server, and then add the server IP address in the **NTP server** field.
Manually set time	Select this option if you want to set the time manually, and specify the current time in the **Local time** field in the following format: `yyyy-mm-dd hh:mm:ss`. For example: `2015-01-16 13:03:28`
Location and **City**	Set the appropriate time zone by selecting the location and city closest to Cloud Edge gateway.

4. Perform the appropriate action.
   - If you used the **General** tab, click **Apply**.
   - If you used the **Quick Setup** screen, click **Save Settings**.

Note

If the Cloud Edge gateway is not registered with Cloud Edge Cloud Console, the button text is **Save & Register**.

Configuring On-premises Console Settings

The Cloud Edge on-premises console settings include the following options:

- **Idle Timeout:** By default, the Cloud Edge gateway disconnects administrative sessions if no activity takes place for five minutes. This idle timeout is recommended to prevent someone from using the Cloud Edge on-premises console from a PC that is logged into Cloud Edge and then left unattended. You can adjust the idle timeout as needed.
- **Certificate:** You can browse to and select an SSL certificate for the Cloud Edge on-premises console.

Configuring the On-premises Console Timeout

Procedure

1. Go to **Administration** > **System Settings** > **Console Settings** tab.
2. In the **Idle Timeout** section, set the session timeout as required.
3. Click **Apply**.

Configuring the On-premises Console Certificate Settings

Procedure

1. Go to **Administration** > **System Settings** > **Console Settings** tab.

2. In the **Certificate Settings** section, add the certificate settings.
   - SSL certificate
   - SSL password
3. Click **Apply**.

Configuring Proxy Settings

You can configure the Cloud Edge gateway to use an HTTP proxy server for product updates, license updates, Web Reputation queries, and Cloud Message Scan (CMS).

Procedure

1. Go to **Administration** > **System Settings** > **Proxy Settings** tab.
2. Select the **Use an HTTP proxy server** check box.
3. Specify the HTTP proxy server IPv4 address and port number.
4. If required, specify the user name and password required by the server.
5. Click **Apply**.

Device Management

You can configure device management settings to remotely administer and monitor the Cloud Edge gateway. You can also provide an access point to the Cloud Edge CLI.

Managing Administrative Access

You can use the Cloud Edge gateway's on-premises console to configure the gateway to allow or block specific types of management services (On-Premises Console, Ping, SSH, and SNMP) that are used to administer and monitor the Cloud Edge gateway remotely. Enabling the On-Premises Console management service provides log on access by authorized users to the on-premises console.

You can enable or disable each service on each L3 interface as needed.

Note

Although you can enable management services on the WAN interfaces, for best security, you should enable management services and traffic on internal interfaces so that you can only administer the Cloud Edge gateway from devices that originate from behind the Cloud Edge gateway.

Once SNMP is enabled, you must configure SNMP settings by going to **Administration** > **Device Management** > **SNMP Settings**. After enabling and configuring SNMP support on selected interfaces, users can obtain the supported objects information by using an SNMP manager.

You can enable administrative access on the main or guest wireless networks on Cloud Edge gateways with wireless network functionality. You should be mindful of security concerns when allowing administrative access on the guest wireless network.

Enabling Administrative Access

The Cloud Edge gateway supports administrative access using the On-Premises Console, Ping, SSH, and SNMP services. Enabling administrative access allows remote access using the selected protocols.

After the Cloud Edge gateway is registered, you must use Cloud Edge Cloud Console to enable or disable administrative access using the On-Premises Console, Ping, SSH, or SNMP services.

Procedure

1. Log on to Cloud Edge Cloud Console.
2. Go to **Gateways** > **(gateway name)** > **Administrative Access**.
3. In the field below the table, specify IPv4 addresses allowed to remotely access the gateway.

   Administrative access using IPv6 is not supported.

Note

This setting determines the IPv4 address ranges that can remotely access the gateway. Single IPv4 addresses are supported and the '-' symbol can be used as a range mark. Format the IPv4 address and netmask as `192.168.1.1/24`. If nothing is specified, all IPv4 addresses are allowed.

4. Select the services to enable for the interface.
   - **On-Premises Console**

     The On-Premises Console service provides access to the Cloud Edge gateway's on-premises console.
   - **Ping**
   - **SSH**
   - **SNMP**
5. Click **Save**.

What to do next

Once SNMP access is enabled, you must configure SNMP setting using the Cloud Edge on-premises console.

See *Configuring SNMP Settings on page 7-105*

Configuring SNMP Settings

You must configure SNMP setting using the Cloud Edge on-premises console.

Procedure

1. Log on to the Cloud Edge on-premises console.
2. Go to **Administration** > **Device Management** > **SNMP Settings**.
3. Select the **Enable SNMP** check box.
4. Specify SNMP settings.

Option	Description
Email address	Specify the email address of the contact.
Location	The location of the contact, such as “China office, IT room.”
Community name	Specify the community string required to retrieve information from Cloud Edge (default: public).

Note

Email address and location information of the contact for the Cloud Edge gateway can be viewed in an SNMP manager.

If SNMP management is enabled, users can manage the device using an SNMP manager. An SNMP manager can only manage the gateway if the Community String specified is a valid v2 community string.

Web Shell

The **Web Shell** tab provides access to the Cloud Edge Command Line Interface (CLI) for advanced configuration. It is strongly recommended that a Trend Micro Support representative work with you while using the CLI to avoid configuration errors.

Diagnostics

You can perform diagnostics testing, and view health check results to troubleshooting issues and to identify which Cloud Edge device components are healthy or unhealthy. You can also collect and download diagnostic files.

- Perform packet captures
- Perform traffic tracing
- Collect and download files
- View health check information

Viewing Health Check Information

You can view information about the health of the gateway from the on-premises console.

Procedure

1. Log on to the Cloud Edge on-premises console.
2. Go to **Administration** > **Diagnostics** > **Health Check**.
3. View information about the gateway health including the following:

Section	Entries	Description
Hardware Information	Serial Number	Read-only entry
	Cloud Edge Device Type	Read-only entry The device type is the Cloud Edge model.
	Cloud Edge Firmware Version	Read-only entry
System Resources	System Temperature	Current status displayed
	System Disk Usage	
	Data Disk Usage	
Network Interface Status	List of all Network Interfaces	Status: Up or Down Includes status for main network. Also includes status for guest wireless networks for Cloud Edge gateways that support wireless network functionality.
Service Status	Auto Register Module	Status: Running or Error
	DHCP service	Status: Running, Error, or Disable

Section	Entries	Description
	Heartbeat Module	Status: Running, Error, or N/A
	L2TP VPN Service	Status: Running, Error, Disable, or N/A
	Log Upload Module	Status: Running or Error
	Mail Scan Service	Status: Running or Error
	NTP Service	Status: Running, Error, or Disable
	Scan Service	Status: Running or Error
	System Monitor Module	Status: Running or Error
	Site-to-Site VPN Service	Status: Running, Error, Disable, or N/A
	SSL VPN Service	Status: Running, Error, Disable, or N/A
	User Auth Module	Status: Running or Error

Rolling Back a Software Patch

Procedure

1. In the on-premises console, go to **Administration** > **Updates** > **Software Patches**.
2. Select the applied patch that you want to roll back, and then click **Rollback**.

Factory Settings

Restoring factory settings resets the Cloud Edge gateway to the default network settings and erases all log and database information.

Use cases for restoring factory settings:

- Full Cloud Edge gateway hard disk.
- Use the Cloud Edge gateway at a different customer location.
- Remove data to meet compliance requirements when a customer no longer uses the Cloud Edge gateway.

Restoring Factory Settings

WARNING!

Restoring factory settings deletes all log and database information stored on the Cloud Edge gateway. This information cannot be restored.

Procedure

1. Power off the Cloud Edge gateway.
2. Press and hold the reset button located on the back panel.

   The reset button is located on the back of the Cloud Edge gateway between the AC power slot and USB ports.
3. Power back on the Cloud Edge gateway.
4. Release the reset button until the yellow LED on the gateway back starts to blink.

   The yellow LED blinks for approximately 2 minutes. The factory settings have been restored when the Cloud Edge gateway restarts.

Chapter 8

Technical Support

Learn about the following topics:

Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to https://success.trendmicro.com.
2. Select from the available products or click the appropriate button to search for solutions.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Contact Support** and select the type of support needed.

   Tip

   To submit a support case online, visit the following URL:

   https://success.trendmicro.com/smb-new-request

   A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone or email:

Address	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
Website	https://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:

  https://www.trendmicro.com/us/about-us/contact/index.html

- Trend Micro product documentation:

  https://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem

- Appliance or network information
- Computer brand, model, and any additional connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or Activation Code
- Detailed description of install environment
- Exact text of any error message received

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

https://servicecentral.trendmicro.com/en-us/ers/

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

https://success.trendmicro.com/solution/1112106

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

https://success.trendmicro.com/solution/1059565

Record the case number for tracking purposes.

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

https://global.sitesafety.trendmicro.com/

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

Download Center

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

https://www.trendmicro.com/download/

If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.

Documentation Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

https://docs.trendmicro.com/en-us/survey.aspx

Index

B

C

E

H

L

M

N

O

P

S

T

U

V

W

TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: APEM09742/230620