Omada by tp-link Enterprise Solution

Quick Installation Guide

Fusion Gateway

Note: Fusion gateways are for enterprise installation and use. Fusion 2.5G is used as an example throughout the guide. Images may differ from your actual product.

Preface

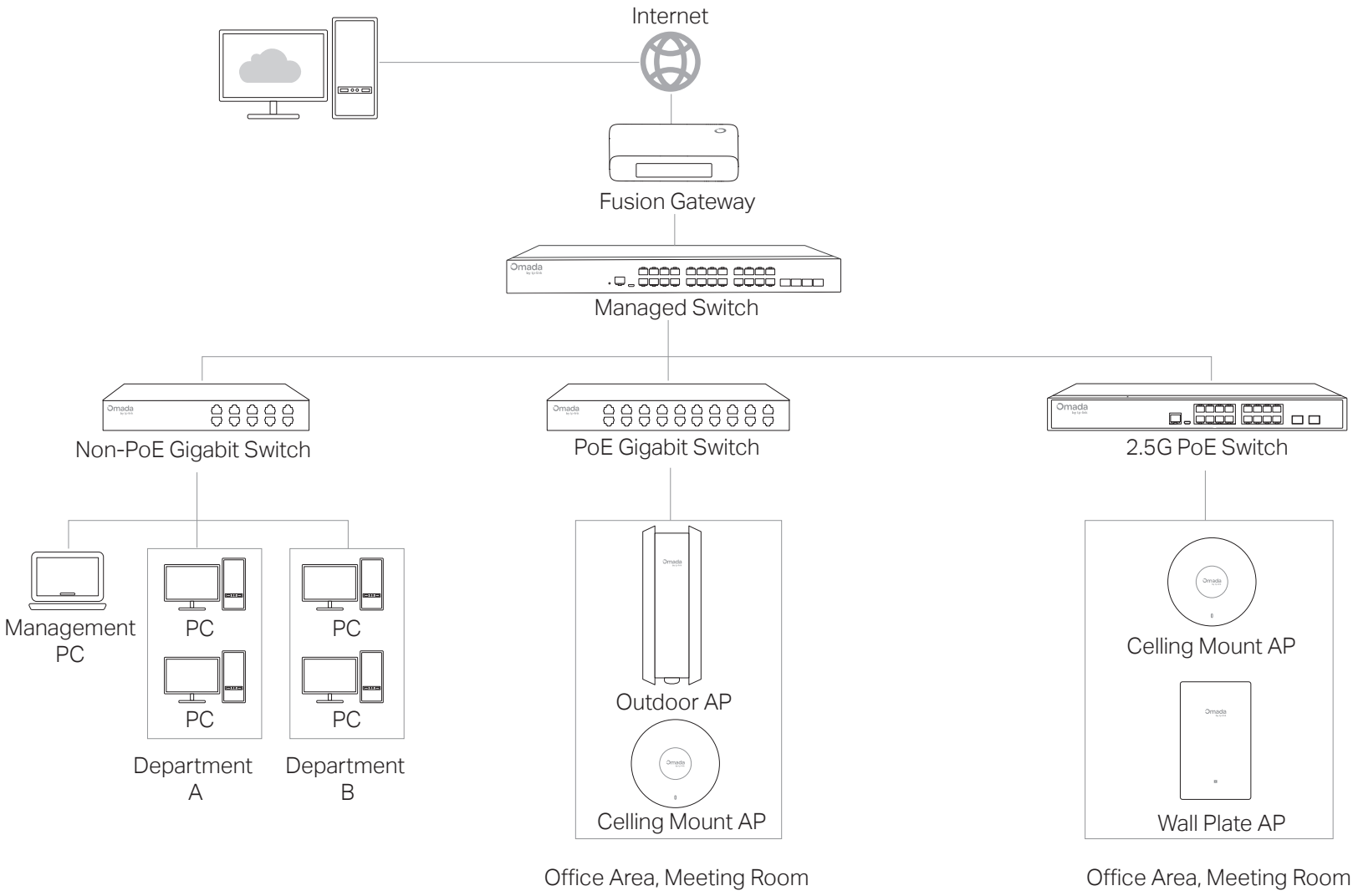
The Fusion gateway delivers an all-in-one solution for networking and centralized management on a single device, featuring a built-in controller for the entire Omada ecosystem. It is ideal for small businesses across single or multiple sites.

This Quick Installation Guide is for qualified IT staff and professional installers. It covers typical network topology, basic software configuration, and descriptions of enterprise-dedicated features. For detailed instructions, refer to the user guide.

Safety Precautions

- Do not attempt to disassemble, repair, or modify the device. If you need service, please contact us.
- Do not use damaged charger or USB cable to charge the device.
- Do not use any other chargers than those recommended.
- Adapter shall be installed near the equipment and shall be easily accessible.
- Keep the device away from water, fire, humidity or hot environments.
- Do not use the device where wireless devices are not allowed.
- For enterprise installation and use only.

Typical Network Topology



Software Configuration

Initial Setup

1. Connect the Internet port (Port 1) of the gateway to the internet using the provided Ethernet cable.
2. Connect the gateway to a grounded power outlet using the provided power adapter. The touchscreen on the front panel will light up.
3. Make sure the management PC is configured to **Obtain an IP address automatically**.
4. Open a web browser and type the default management address **https://omada.local** or **https://192.168.188.1** in the address field of the browser, then press the **Enter** key.
5. Follow the setup wizard to configure the internet settings, bind the gateway to your TP-Link ID, set up the controller, and add devices.
6. After the setup wizard is complete, you will be directed to the management page. And you can configure more settings and manage your network.

For detailed information and configuration, refer to the gateway's user guide. The guide can be found on the **Documents** page of our official website:

https://support.omadanetworks.com/document/.

More Management Methods

■ **Via Omada App**

With the TP-Link Omada app, you can access and manage your Omada devices at a local site or remotely.

Download on the App Store / GET IT ON Google Play or Scan for Omada App → Download Omada App

■ **Via Omada Cloud Portal**

a. Enable **Cloud Access** on the **Settings** page on the gateway and bind a TP-Link ID to your gateway. If you have configured this in the setup wizard, skip the step.

b. Launch a web browser and enter **https://omada.tplinkcloud.com** in the address bar.

c. Enter your TP-Link ID and password to log in. A list of Fusion gateways that have been bound with your TP-Link ID will appear in the **Fusion Systems** page. Then you can launch your device to further configure the gateway.

Flip Over to Explore More

Enterprise-Dedicated Features

Fusion gateways are FCC Class A certified products with various advanced software capabilities, primarily used in business, industrial, or office environments.

- **Multi-Site Networking and Management:** Features an enterprise-grade SD-WAN for multi-site networking in business scenarios (e.g., chain supermarkets and chain restaurants) and Cloud Portal for managing multiple sites.
  • Sites are interconnected via encrypted tunnels, forming a unified enterprise WAN and ensuring secure and reliable communication across geographically distributed locations. All network configuration, site onboarding, and policy management are performed exclusively through a cloud management portal. Local or on-premises controllers are not supported. Branch devices support multiple WAN connections. Link availability is determined through WAN online status detection, enabling basic link redundancy and failover when a WAN connection becomes unavailable.
  • This feature is designed for enterprises with multiple branches or stores that require unified networking and centralized management. Cloud-based centralized operations significantly simplify network deployment and ongoing maintenance. This feature is focuses on manageability, scalability, and long-term network stability for business operations.
- **Centralized Management:** Facilitates unified management of all network devices (including enterprise-grade L3 switches, APs, etc.) within the enterprise network.
  • Unified Management Plane: Fusion devices run a built-in software platform that acts as the local management controller for all connected network devices within the site. Through this embedded platform, installation technicians can onboard L3 switches and wireless access points in bulk upon initial deployment, without logging into each device individually.
  In MSP large-scale deployment scenarios with numerous sites and a substantial number of devices per site, logging into each switch or AP individually for configuration is operationally infeasible. The unified management plane allows installation technicians, upon deploying a Fusion device, to onboard local L3 switches and wireless access points in bulk. LAN, WLAN, ACL, and other policies can be configured once and applied simultaneously across multiple devices. It also provides monitoring and dashboards for detecting alerts and anomalies across sites, addressing the operational requirements of professional enterprise network personnel.
- **Enterprise Network Stability Assurance:** Supports multi-WAN and failover functionality between multi-WANs.
  • The device determines link availability by monitoring the online/offline status of each WAN interface. When the primary WAN connection becomes unavailable, traffic is automatically and seamlessly switched to an available backup WAN connection based on predefined rules, without manual intervention. This provides reliable link redundancy and helps ensure uninterrupted network connectivity for business operations.
  • In enterprise environments, network connectivity serves as a foundational component for transactions, operational workflows, and customer services. Business systems are expected to remain continuously online, and even short term network failures can lead to service disruption, reduced efficiency, or direct financial loss. Therefore, multi-WAN support with automatic failover is an essential capability for commercial deployments, enabling higher network resilience and stronger business continuity.
- **Enterprise-Grade Device Configuration:** Supports professional Command Line Interface (CLI) configuration, batch port configuration across switches, and the SNMP management protocol.
  • CLI Configuration: Supports editing device configurations and enabling advanced features via CLI commands, allowing network engineers to perform granular configuration beyond what the GUI provides. In enterprise environments, CLI access is required for implementing complex network policies (e.g., advanced, policy-based routing, and protocol-level tuning) that are not fully displayed through a graphical interface. It also enables scripted and repeatable configuration workflows, which are necessary for maintaining consistency across large-scale deployments and for integration with enterprise IT automation and management process optimization.
  • Batch Port Management: Enterprise networks contain a large number of switches, each with numerous ports. The unified management plane provides a port/VLAN visualization panel with support for batch configuration deployment by port group or VLAN, reducing the operational complexity of managing ports at scale.
  • SNMP Protocol Support: Supports SNMPv1/v2c/v3 protocols, allowing third-party monitoring systems (e.g., Zabbix, PRTG, SolarWinds, etc.) to perform unified monitoring across multi-vendor devices and automatically collect metrics, including device CPU load, memory utilization, and interface traffic trends.
- **Enterprise-Grade Operation and Maintenance Management:** Features enterprise-grade network packet capture for exporting various network traffic reports with audit logs.
  • Network Packet Capture: A diagnostic tool for operations personnel, used for communication link analysis and network protocol-level anomaly troubleshooting.
  • Network Traffic Data Reports: Provides multi-site enterprises with periodic network data reports covering network status overview, traffic trend analysis, application-layer traffic distribution, and client experience scoring, serving as a basis for network capacity planning and experience optimization. Supports report generation by site, time period, and device, with PDF/CSV exports.
  • Audit Logs: Records operation history of the management system (including operator identity, timestamp, target object, and details), with support for periodic exporting and long-term archival. Required for historical operation traceability during network anomaly investigation, organizational access control management, and security auditing.
  • Firmware Management and Upgrade: Supports centralized device firmware management with batch upgrade and scheduling by site or device group. Upgrade scheduling avoids disruptions during peak business hours, maintaining firmware version consistency across the network and timely application of security patches.
- **Commercial-Grade Access/Authentication Methods*:** Offers external Portal/Voucher/RADIUS authentication, supports (Private Pre-Shared Key (PPSK), 802.1x/MAC-Based Authentication, and professional enterprise-grade L3 layer network features.
  • External Portal/Voucher Authentication: Addresses Captive Portal requirements in enterprise chain store Wi-Fi scenarios by redirecting unauthenticated clients to a Portal address for authentication. Captive Portal supports advertisements, identity authentication and network authorization, endpoint data collection, network traffic billing, and time-limited Voucher credential issuance. Supports integration with third-party Portal servers to accommodate existing enterprise authentication infrastructure (e.g., AD, RADIUS, etc.).
  • External RADIUS/802.1x Authentication: Enterprises need to differentiate endpoint identities (e.g., full-time employees, temporary staff, and guests) and enforce differentiated network authorization based on identity. Relying on a single WPA2 pre-shared key means that a password compromise exposes the entire network.
  • Private Pre-Shared Key (PPSK): Allows each device/user to use an independent static password (with VLAN binding support), addressing both dumb terminal compatibility and security isolation upon password compromise. A single key compromise affects only the associated device, not the broader network. 802.1x combined with RADIUS enables per-user authentication with dynamic VLAN assignment, which is a prerequisite for identity-based network access control in enterprise environments.
  • MAC-Based Authentication: For terminals incapable of interactiveauthentication (e.g., printers, IP phones, and IoT sensors), MAC-based authentication identifies device identity via MAC address and authorizes network access, keeping all connected endpoints within the scope of management and control.
- **Management of Professional Enterprise-Grade L3 Network Features:** Supports management of enterprise-grade L3 switches.
  • VLAN Management: Supports VLAN creation, modification, deletion, and batch deployment on L3 switches through the unified management plane, enabling unified management of network segmentation policies across sites to meet enterprise requirements for network isolation by department, business function, and security classification.
  • Static Routing and Route Management: Supports configuration and management of static routing tables on L3 switches, enabling Layer 3 routing and forwarding across VLANs and subnets, providing flexible routing policies for enterprise multi-subnet interconnection.
  • ACL (Access Control Lists): Supports granular traffic filtering rules based on source/destination IP, port, protocol, and other conditions, implementing east-west traffic security control at the switch layer to prevent unauthorized cross-segment access. In enterprise networks, different departments and business systems typically reside on separate network segments. ACLs enforce segmentation boundaries at the infrastructure level, restricting lateral movement between segments and reducing the blast radius of potential security incidents.
  • QoS (Quality of Service) Policies: Supports traffic priority marking (DSCP/CoS), queue scheduling, and bandwidth rate limiting on L3 switches, allowing prioritized transmission of latency-sensitive traffic, such as voice and video, to maintain application performance. Enterprise environments commonly run mixed traffic workloads (e.g., VoIP, video conferencing, POS transactions, and bulk data transfers) over shared infrastructure. Without QoS, bandwidth contention during peak periods can degrade the performance of business-critical applications.
  • DHCP Service Management: Supports DHCP Server/Relay configuration and management on L3 switches, enabling automatic IP address allocation and centralized management for each VLAN subnet, reducing the operational overhead of manual IP assignment. In multi-VLAN enterprise networks, centralized DHCP management on L3 switches eliminates the need for dedicated DHCP servers per subnet and provides a single point of control for IP address pool allocation, lease management, and subnet-level policy enforcement.
  • STP/RSTP (Spanning Tree Protocol/Rapid Spanning Tree Protocol): Supports Spanning Tree Protocol configuration and state monitoring to prevent network loops caused by redundant links, maintaining network topology stability. Enterprise networks typically deploy redundant uplinks and cross-connections for resilience. Without STP/RSTP, these redundant paths create broadcast storms and MAC table instability that can bring down the entire Layer 2 domain.

*These features refer to functions supported by the switches adopted by the Fusion gateway and can be configured through it.

Appendix

Frequently Asked Questions (FAQ)

Q1. Why were no APs or switches found during the initial setup?

A: During initial setup, only devices in factory mode can be detected. Otherwise, they can only be detected and adopted after setup using their original account and password.

Q2. How do I reset the Fusion gateway?

A: • Via the physical Reset button
With the device powered on, use a pin to press and hold the Reset button on the front panel for about 5 seconds until a reset prompt appears, then release. The device will restore to its factory default settings.

• Via the web management page
Go to **Settings** > **System Settings** > **OS Settings**. In the **Action** drop-down list, click **Reset** to reset the device to its factory default settings.

Q3. How do I adopt APs and switches?

A: 1. Connect the APs/switches to the same network as the gateway.
2. Access the gateway's management page at **https://omada.local** or **https://192.168.188.1**.
3. Go to **Devices**, you will find the devices displayed in the **Device List**.
4. Click **Adopt** and wait until the device's **STATUS** changes to **CONNECTED**.

More Resources

Main Site	https://www.omadanetworks.com/
Video Center	https://support.omadanetworks.com/video/
Documents	https://support.omadanetworks.com/document/
Product Support	https://support.omadanetworks.com/product/
Technical Support	https://support.omadanetworks.com/contact-support/

Warranty

For details on the warranty period, policy, and procedures, visit **https://support.omadanetworks.com/warranty-services/**.

Support

For technical support, user guides, and other information, please visit **https://support.omadanetworks.com/**, or simply scan the QR code.

EU Declaration of Conformity

TP-Link hereby declares that the gateway is in compliance with the essential requirements and other relevant provisions of directives (EU)2015/863, 2014/53/EU and 2011/65/EU.

The original EU declaration of conformity may be found at https://www.tp-link.com/en/support/ce/

UK Declaration of Conformity

TP-Link hereby declares that the gateway is in compliance with the essential requirements and other relevant provisions of the Radio Equipment Regulations 2017.

The original UK declaration of conformity may be found at https://www.tp-link.com/support/ukca/