Lumen® SASE Solutions with Fortinet FortiManager

FortiManager provides automation-driven centralized management of your Fortinet devices from a single console. This enables full administration and visibility of your network devices through streamlined provisioning and innovative automation tools.

Integrated with the Fortinet Security Fabric advanced security architecture and automation driven network operations capabilities provide a solid foundation to secure and optimize your network security.

Single-Pane Management streamlines centralized policy and object management, automatic revision history and control, and enhanced role- based access control (RBAC) features for script management and IPS management with role separation.

Security Fabric Automation simplifies the ZTP deployment process for SD- Branch (FortiGates and access devices) with powerful templates that directly utilize meta-variables for scalable provisioning to thousands of sites.

NOC Cloud Services offer the FortiManager platform as a service with new management extensions that can be pulled and installed from the cloud.

Key Features

- **Centrally manage network and security policies** for thousands of FortiGate NGFWs and Secure SD-WAN. Plus FortiSwitches, FortiAP, and FortiExtender. Provide signature updates to FortiGate, FortiMail, FortiSandbox, and FortiClient.
- **Get centralized distribution of security content** and signatures through the use of the built-in FortiGuard module.
- **Simplify configuration, deployment and maintenance for secure SD-WAN at-scale.** Accelerate FortiExtender Wireless WAN connectivity with centralized management across distributed sites.
- **Reduce complexity and costs by leveraging automated REST API**, scripts, connectors,and automation stitches.
- **Automate workflows and configurations** for Fortinet firewalls, switches, and wireless infrastructure.
- **Separate customer data and manage domains** leveraging ADOMs to be compliant and operationally effective.
- **High availability to automate backups** for up to five nodes with streamlined software and security updates for all managed devices.

Feature highlights

Single-Pane Management

Single pane management provides centralized management and provisioning strategy for Fortinet devices. Our devices integrated into the Fortinet Security Fabric to apply access control, segmentation, and consistent protection of devices, applications, and users.

Device configuration and provisioning

FortiManager expands the network administrator's capabilities with a rich set of tools to centrally manage up to 100 000 devices including FortiGate NGFWs, FortiExtender, FortiSwitch switches, FortiAP access points, Fortinet Secure SD-WAN, and more.

You can collectively configure device settings and use new enhanced CLI templates with variables, and provisioning templates to assign firmware and policy packages from a single console, including policy and object revision history for auditing.

FortiManager includes extended SSL and certificate support for enhanced ssl-ssh-profile configuration, as well as Restricted IPS Admin Profiles to support customers that are transitioning and upgrading from dedicated IPS solutions to Fortinet products.

Automated device configuration backups and revision control make daily administrative tasks easy. It includes change tracking in the enhanced Event Log view for review of configuration and change detail for auditing and compliance.

FortiManager also now enables admins to configure and assign custom commands on FortiSwitch and configure MCLAG from the FortiSwitch Manager.

Multi-tenancy and role-based administration

FortiManager provides granular device and role-based administration for clear visibility of every device and user on the network. This facilitates zero-trust, multi-tenancy deployments for large enterprises and a hierarchical objects database for re-use of common configurations to serve multiple customers.

ADOMs (administrative domains) are used to manage independent security environments, each with its own security policies and configuration database. The intuitive GUI makes it easy for admins to view, create, clone, and manage ADOMs, define global Objects, Policies, and Security Profiles across ADOMs, with Health Check to ensure ADOMs are in sync.

FortiManager's zero-touch deployment utilizes templates to provision devices for quick mass deployments. It also supports firmware version enforcement for defining firmware requirements for installs and upgrades.

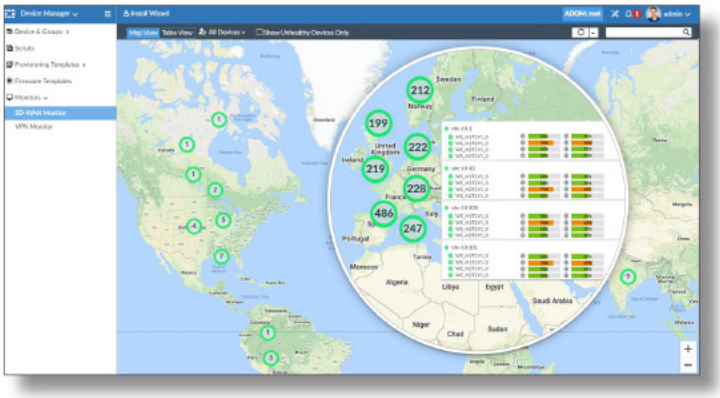
The IPS admin is a restricted user role for performing only IPS related object configuration and installations. Admin users can also be assigned per-admin UI background themes for unique visual associations.

Security policy and objects management

FortiManager Policy and Objects views enable admins to centrally manage and configure device policies, including updating network settings, antivirus definitions, intrusion prevention signatures, access rules, and software updates.

The global policy feature allows MSSP and PaaS providers to apply ADOM level header/footer policies for updating all policy packages or select packages. Policy and Objects views now include a revision history, providing an account of admins who have made changes, change date, summary, and a mandatory change notes field to capture change reason.

The per-policy lock feature allows admins to control the policy change by implicitly locking a policy rule when a policy is changed. Admins can also group commonly used policies in a policy block and insert in different Policy Packages.



Secure SD-WAN

FortiManager offers powerful SD-WAN management capabilities using intuitive workflows and simplified provisioning at scale. Leverage application centric SD-WAN business policies to fine-tune traffic steering decisions based on performance service level agreement (SLA) targets for each WAN provider.

Admins can use the SD-WAN monitoring dashboard to keep an eye on application performance and bandwidth utilization per WAN link. FortiAnalyzer can be integrated for enhanced analytics views and SD-WAN assessment reports.

Feature highlights

Manage and monitor with deep visibility

The FortiManager Device Manager provides full visibility, access, and management of Fortinet managed devices, interfaces, scripts, templates, automation, users, settings, and more. Install, edit, and delete policies. Monitor the health of FortiGate devices through customizable dashboards and widgets to see resource usage, network status of DHCP, IPsec and SSL VPN, routing, traffic shapers, and more.

Easily navigate the hierarchical tree with categories for managed devices, logging devices, unauthorized devices, and customize to display as a table, folder, or a map view.

Use Fabric View to check Security Fabric ratings and configurations of FortiGate devices or groups. Access vital security and network statistics, as well as real-time monitoring and topology information to provide visibility into network and user activity. Add a FortiAnalyzer appliance or virtual machine (VM) for powerful analytics and enhanced Fabric view with asset and identity info, additional data mining, statistical analysis, and graphical reporting capabilities.

FortiManager High Availability (HA)

FortiManager high availability (HA) provides enhanced reliability, data protection, redundancy, and operational performance. These ensure agreed-upon uptime and availability requirements are met. In the event that the operating FortiManager unit fails, a backup FortiManager (one primary and up to four secondary) unit can take the place of the failed unit, making sure that companies have seamless access to their devices and business-critical network operations.

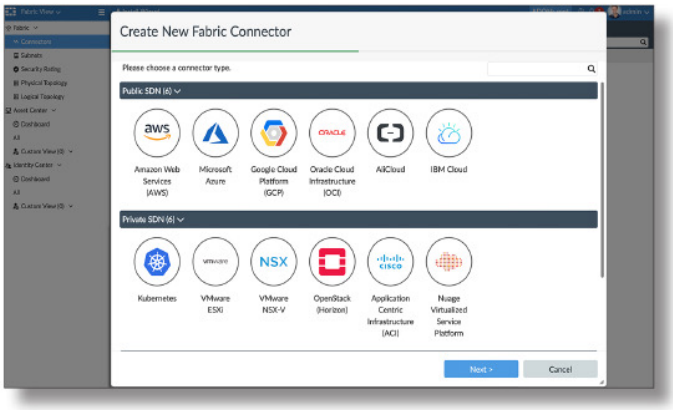
The FortiManager HA Cluster Wizard now also supports defining a hostname for each cluster member, exposing the session-pick option from the GUI, as well as the option to dedicate an interface for management of the individual cluster member.

Security Fabric Automation

Network and Security Operations visibility (NOC/SOC)

FortiManager supports NOC-SOC workflows to assist network teams in maintaining optimal performance. Automated data exchanges between security (SOC) workflows and operational (NOC) workflows, create a single, complete workflow that not only saves time, but also provides the capacity to complete additional incident response activities.

Integration with FortiAnalyzer magnifies visibility with advanced data visualization and analytics. This helps analysts quickly connect-the-dots, identify threats, and simplify the expeditious configuration and security of managed devices.



Automation and connectors

Utilize automation and orchestration and optimize network operations with FortiManager through querying of FortiGate NGFWs and the Fortinet Security Fabric via application programming interfaces (APIs). This will actively collect and share network information and broaden end-to-end visibility and response.

FortiManager reduces complexity and cost by leveraging REST API, scripts, connectors, and FortiGate automation stitches to automate time-intensive processes and accelerate workflows. This helps NOC and SOC teams by reducing administrative tasks, and addressing talent shortages.

Admins can automate common tasks such as provisioning of FortiGate NGFWs and configuring new or existing devices.

Join the Fortinet Developer Network (FNDN) for exclusive access to articles, how-to content for automation and customization, community-built tools, scripts, and sample code.

Feature highlights

NOC cloud services

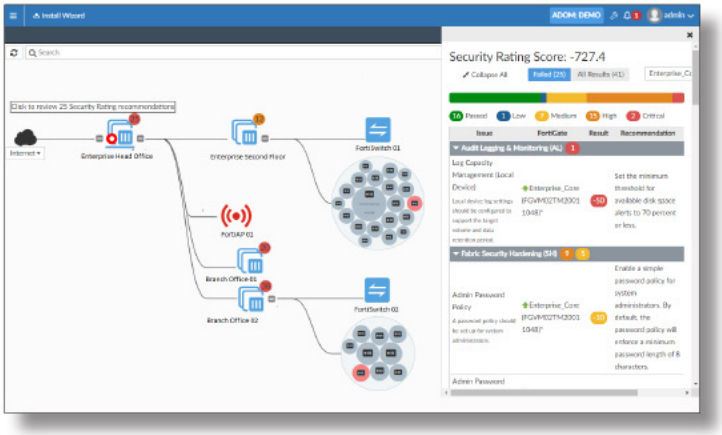
Management Extensions

The Management Extensions pane allows rapid expansion of the single pane to manage more Security Fabric products.

The built-in engine runs containerized management extension applications (MEAs) pulled from FortiGuard Labs Threat Intelligence.

FortiManager's MEAs include modules for the following:

- SD-WAN automation for network wide-configuration, management and monitoring of FortiGate NGFWs on your SD-WAN network



Dynamic cloud security

Fortinet cloud security and management solutions offer organizations a PaaS-based delivery option for central management of FortiGate devices from a cloud-based FortiManager.

FortiManager Cloud provides an automation-driven and single pane-of-glass management capability that is easy-to-implement, easy-to-manage, flexible, and scalable.

Use the single sign-on portal to manage Fortinet NGFW and SD-WAN. The built-in cloud-init service allows admins to easily customize a prepared image of a virtual installation for KVM, AZURE, and AWS. FortiManager cloud-based network management helps organizations streamline FortiGate provisioning with automation-enabled management of Fortinet devices.

With the FortiCloud Premium subscription, customers can easily enable the FortiManager Cloud service with the FortiAnalyzer Cloud with SOCaaS license, providing access to manage a range of Fortinet solutions and services for simplified network and security management. Customers can easily access their FortiManager Cloud from their FortiCloud single sign-on portal.

Security fabric and third-party integration

FortiManager integrates with ITSM to seamlessly mitigate security incidents and events, apply configuration changes, and update policies. Integration with FortiAnalyzer provides in-depth discovery, analysis, prioritization, and reporting of network security events.

Use Fabric connectors to facilitate connections with third-party vendors like vCenter, pxGrid, ClearPass, OCI, ESXi, AWS, and others to share and exchange data.

The FortiManager workflow for audit and compliance enables review, approval, and auditing policy changes. These include automating processes for policy compliance, policy lifecycle management, and enforced workflow to reduce risk.

Trusted Platform Module (TPM) encryption

FortiManager G Series features a dedicated micro-controller module that hardens physical networking appliances by generating, storing, and authenticating cryptographic keys in TPM. This hardware-based security mechanism protects users from malicious software and phishing attacks.