DATA SHEET

FortiPortal

Available in:

Virtual Machine

FortiPortal is a comprehensive end-user self-service portal designed for enterprises, education Institutions, and governments — specifically optimized for service providers.

It provides Cloud-Based Security Policy Management and Analytics and enables MSSPs to assign common firewall configuration and monitoring tasks to users in different geographies, while easily integrating cyber security management products to provide organization services for security management, configuration, and analytics.

Service Provider Portal

FortiPortal enables service providers to delegate configuration tasks and analytics to end-customers, business units, and departments in a multi-tenant environment, allowing them to monitor the clients and monetize through automation. This easy-to-deploy, turnkey portal delivers organization and device views that streamline the tasks of adding clients and devices.

With an informative dashboard containing intuitive widgets, service providers can quickly see license usage, license distribution, top 10 organizations, and other useful summaries, while self-branding theme enables service providers to retain their own brand on the UI. FortiPortal assists service providers in delivering the quickest time to market services by avoiding the need to develop their own costly portal.

Customer Self-Serve Portal

FortiPortal Organizations provides end-users with an easy-to-use self-service customer portal giving them access to security capabilities and monitoring such as SD-WAN monitoring and configuration, policies and firewall objects, analytical dashboards, reports, WiFi or switch monitoring, audit, and additional resources like documentation and links.

Key Features

- Delivers secure SD-WAN configuration and monitoring of SD-WAN interfaces with an intuitive map
- Empowers service providers to delegate end-user control, allowing users to view and understand the impact of their security policies
- Promotes multi-tenancy with granular RBAC to expose only the desired configuration options and analytics
- Provides simplified access to dashboards, monitors, log views, and reports
- Supports APIs for integration with service providers, existing IT infrastructure, and auto on-boarding clients
- Accommodates customization of the user interface to match the service provider brand
- Enables service providers to add links to other resources in the GUI and provide a complete portal for end-users
- Leverages FortiPortal low Total Cost of Ownership and fast time-to-market while reducing complex development and maintenance costs
- Enhances reliability and scalability with a Scalable Cluster solution where all FortiPortal instances within the cluster actively serve requests
- Permits end-customers to have access control on their portals with the per-tenant SSO configuration

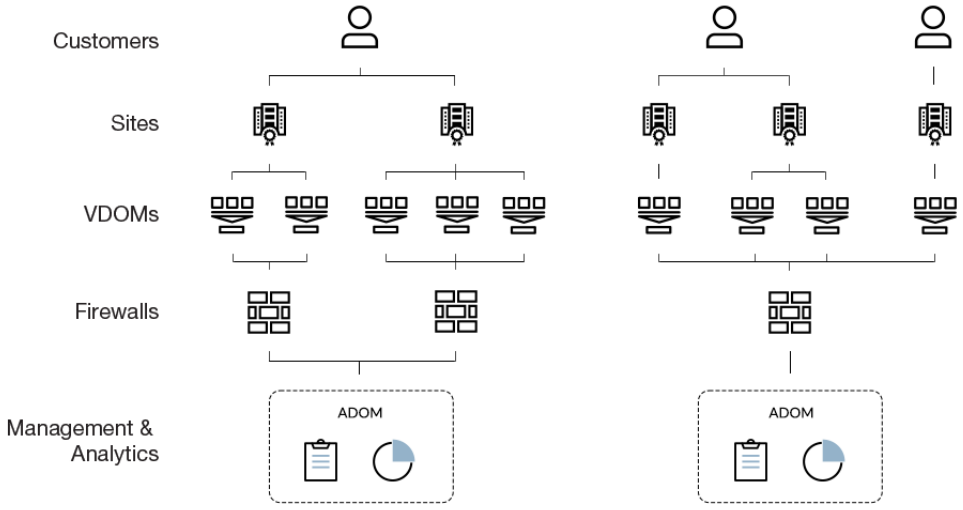
ARCHITECTURE

FortPortal architecture provides end-users with many options and functional network management capabilities without the need for on-site infrastructure. FortiPortal provides out-of-the-box integration with FortiManager, FortiAnalyzer, FortiGate, FortiSwitch, and FortiAP for simplified management of devices, configuration, and analytics with real-time visibility and reporting for traffic, application, attacks, and web usage.

The easy-to-use graphical user interface is designed to simplify device and firmware updates, making policy modifications, and deploying new customers and locations. Its scalability and multi-tenancy offers a complete solution for managed service providers (MSPs) to manage hundreds of FortiGates, FortiSwitches, and access points across multiple organizations with complete data isolation and control over users. End-customer FortiGate devices are managed by one or more FortiManagers. Optionally, logs from the FortiGate devices can be gathered by one or more FortiAnalyzers.

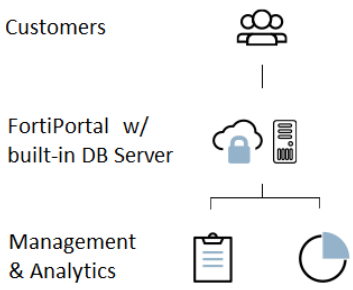
Concept

A FortiPortal Organization can contain multiple sites and each site can contain one or more virtual domains (VDOMs). VDOMs map to administrative domains (ADOMs) which are mapped to the organization. FortiPortal provides a single user interface across multiple instances and versions of FortiManager and FortiAnalyzer.



Deploying FortiPortal

FortiPortal has a database containing configuration information which relies on the FortiManager and FortiAnalyzer APIs for security configuration and security analytics, respectively.



FortiPortal delivers real-time analytics and meaningful insights, as well as simplified configuration and management of network devices powered by FortiAnlayzer and FortiManager through a simplified and easy-to-use interface, reducing complexity for both service providers and customers alike.

The intuitive interface includes the ability to provide organizations with a customized portal for management of devices, APs, policies, objects, along with dashboards, reports, and custom views for comprehensive security updates, real-time analyses, and a response which is unique to their needs.

FEATURE HIGHLIGHTS

Insights

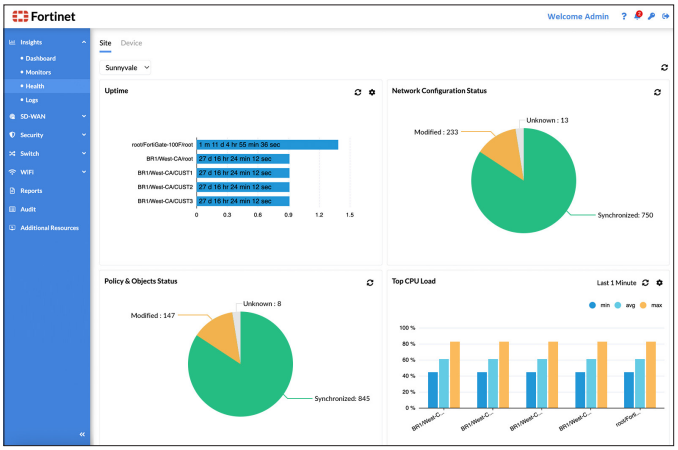
FortiPortal Insights provides a centralized location for organizations to view important security and device information with intuitive charts and tables, allowing users to get a real-time picture of their network traffic and security posture, and assisting with comprehensive analysis and investigation of applications, devices, policies, and network resources.

Dashboard provides helpful visualizations to give users a first glimpse and overall picture of their network traffic and security posture including filter-able and intuitive widgets for Top Countries, Top Threats, Top Sources, Top Destinations, Top Applications, and Policy Hits as well as graphics to show Admin Logins, System Events, and Resource Usage. Users can drill-down on the widgets to explore and investigate further and select a predefined time range or specify a time to display and investigate.

Monitors delivers comprehensive visibility into devices and network resources. The monitors display historical timelines on security and event information by application, source, or destination with controls that allow easy navigation. There are Top Threats, Top Sources, Top Destinations, Policy Hits as well as Top Application, Top Browsing Users, and Top Website Domain views providing intuitive FortiViews that can be filtered with predefined or custom time ranges.

Customers can also gain meaningful insights into network activity for SSL and Dialup, and Site-to-Site IPsec VPNs.

Health provides insightful widgets for monitoring Device Uptime, Network Configuration Status and Policy and Object Status with drill-down, and Top CPU Load, Top Memory Usage, and Top Number of Sessions on multiple devices. Device tab also shows historical information on Bandwidth usage, Session, and Session rate on individual device.

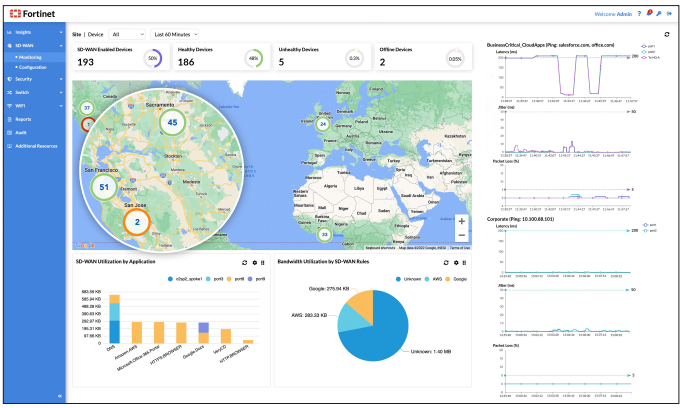


Logs allows users to research further with FortiGate Event and UTM data such as Traffic, IPS, Antivirus, DNS, Application Control, Web Filter, Event, and Sandbox logs. Insights' Logs allow users to filter logs by type, site, date, and time as well as filters to choose data from many columns and fields. Users can also export filtered log results into a CSV file for allowing a more thorough analysis, sharing of results, or auditing and compliance purposes.

Secure SD-WAN

SD-WAN helps organizations evolve beyond traditional WAN architectures and archaic MPLS services and open their networks to direct internet access, simplified management, increased options for connection types with vendor selections at reduced costs.

FortiPortal makes it easy for enterprises and service providers to configure and monitor secure SD-WAN by enabling organizations to modernize their traditional WAN networks to meet the growing needs of the digital evolution.



SD-WAN Monitoring dashboard provides centralized monitoring for both secure SD-WAN Sites and SD-WAN Devices for a consolidated view of the SD-WAN network including a map view and widgets for Healthy Devices, Unhealthy Devices, and Offline Devices with drill-down to intuitive tables by device for diagnostic visibility of Interface, Performance SLA, Jitter, Latency, Packet Loss, Sessions, and Bandwidth.

SD-WAN Configuration allows ease of management of SD-WAN configurations on a single device or multiple devices with templates containing essential settings such as SD-WAN interface members, Performance SLAs, and SD-WAN rules.

FEATURE HIGHLIGHTS

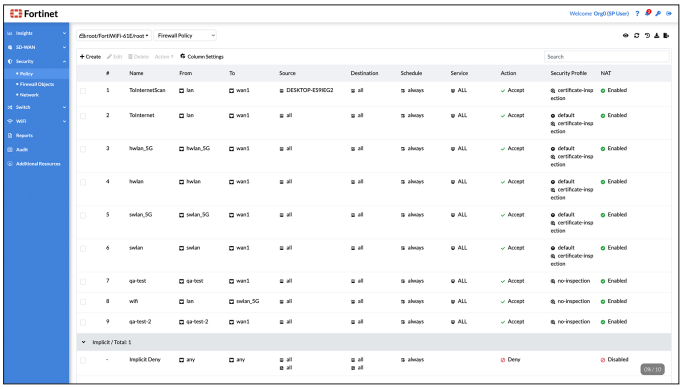
Security

The Security menu offers three different options for users to centrally manage and configure the devices managed by FortiManager units. This activity includes basic network settings to connect devices to corporate networks, and to define antivirus profiles, intrusion protection signatures, web filtering rules, application control profiles, and access rules for the devices.

Policy provides users with a transparent view and access to policies and objects for configuration tasks that were delegated by the service provider, and as defined on the FortiManager. Policy view is hierarchal and it shows policy packages associated with either one or more FortiGate devices or VDOMs, or all devices within an ADOM. Users can also export the policies to a CSV file for auditing.

Firewall Objects enables users to view and manage items such as policy objects like addresses, schedules, services, and Virtual IPs, as well as User Definitions and User Groups. Customers can also have access to UTM security profiles for services such as antivirus, intrusion protection, web filtering, and application control.

Network allows users to configure essential networking settings, such as static routes and DHCP server settings. It also permits the configuration of IPSec VPN on the devices.

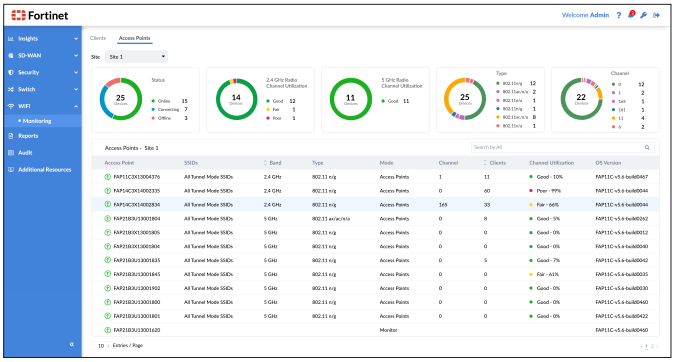


Switch

Switch Monitoring has an at-a-glance summary page on the connected clients showing important information such as VLAN, port, and client's software and hardware information. It also shows tags on clients that are on-boarded based on NAC or Dynamic Port policy. Under the Switch view, it has critical information on the Switch infrastructure such as the number of connected clients to a switch, native VLANs, allowed VLANs, PoE status, and traffic counters on each port.

WiFi

WiFi Monitoring offers information on the connected clients and access points (APs). The Clients view provides visibility on which AP a client is connected to as well as information on Signal Strength, Signal Strength to Noise Ratio, and traffic counters allowing easy troubleshooting. There are also options to view a client's traffic details and dissociate the client from an AP. With the Access Point view, it provides details on the WiFi infrastructure. It has real-time status on channel utilization and any potential interfering SSIDs on an access point.



Reports

FortiPortal Reports enables service providers to easily create and assign reports to an organization. The Reports page displays a list of available FortiAnalyzer reports and permits users to select reports, search reports, and run reports on demand based on the reports assigned to them by the service provider. Reports are available in various formats.

Audit

The Audit module displays logs on user activity with the administrative web interface by date which can be searched by level, user name, event type, IP, or message description. There is also the option to export the logs to a CSV file for further analyses.

Additional Resources

The Additional Info page provides links to important FortiPortal references and documentation added by the service provider such as manuals, reference guides, and links to important updates or information.

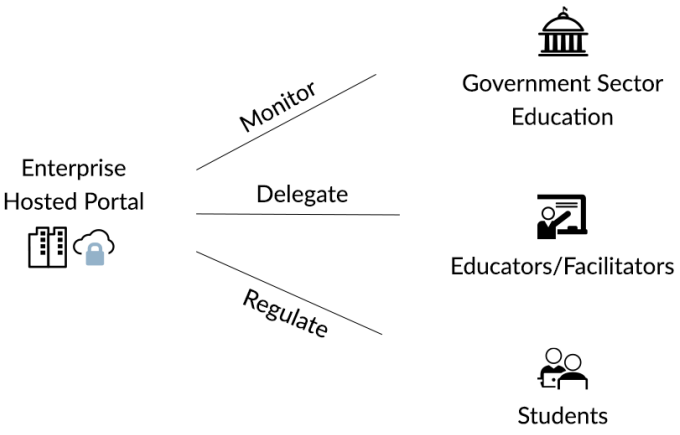
DEPLOYMENT USE CASES

FortiPortal helps MSSP partners to create new revenue streams, improve margins, and deliver differentiated services. It enables security-driven networking solutions that deliver security effectiveness, cost, and performance for use cases spanning enterprises on-premises, multi-cloud environments, branch, and remote deployments.

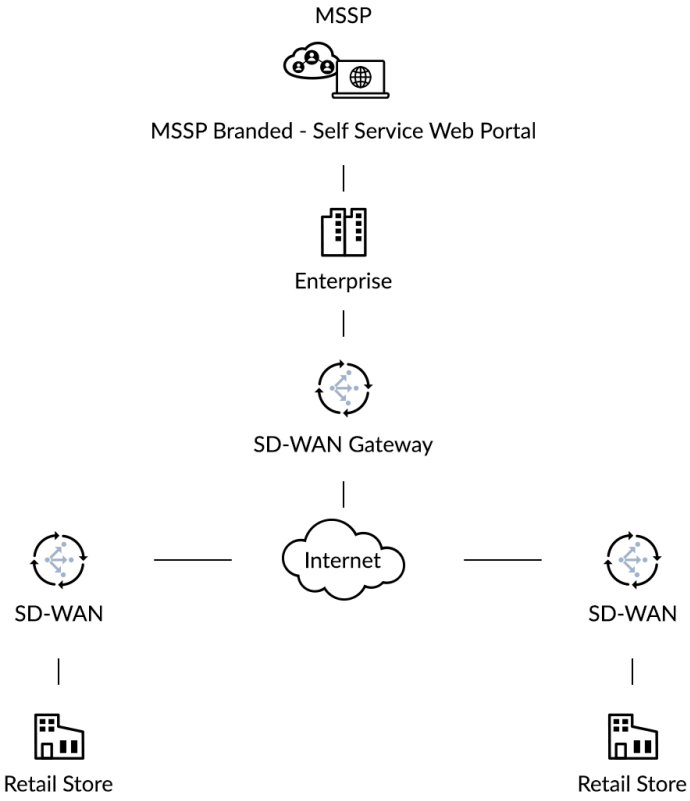
FortiPortal is built on the top of Fortinet's management platforms and allows MSSPs to delegate the common firewall configuration and monitoring tasks to their end customers such as network policy management, controlled access to configuration, management tasks, and analytics.

FortiPortal enables MSSPs, enterprises, education, and government customers to operate a cloud-based hosted security management and log retention service.

The service provides end customers with centralized reporting, traffic analysis, configuration management, and log retention without the need for the end customer to invest in additional hardware and software.



Government Deployment



SD-WAN Deployment

SD-WAN offers business application steering, cost savings, and performance for Software-as-a-Service (SaaS) applications as well as unified communication services to simplify centralized management across branch networks with increased flexibility, visibility, and lower cost of SDN.

Service providers can build new services on Fortinet products that offer the flexibility to accommodate different architectural requirements specific to MSSP environments including multi-tenancy, custom portals, comprehensive automation and orchestration support, centralized management and analytics, custom reporting, and bulk deployment capabilities.

SPECIFICATIONS

	FORTIPORTAL SERVER
System Requirements	
VMware Version	VMware ESXi Version 6.0.X, 6.5.X, 6.7.X and 7.0
Recommended Minimum vCPU per Portal	4
Recommended Minimum Memory per Portal	16 GB
Recommended Minimum free disk space per Portal	12 GB
Supported Devices	FortiManager, FortiAnalyzer, FortiGate/FortiWiFi, FortiAP, and FortiSwitch

ORDER INFORMATION

FortiPortal is available as a VM perpetual license or through a subscription license which includes a FortiCare support contract.

PRODUCT	SKU	DESCRIPTION
FortiPortal-VM Subscription License with Support	FC1-10-PCVMS-258-01-DD	FortiPortal subscription license for 10 managed devices / virtual domains. FortiPortal software and FortiCare Premium support is included. This SKU can be purchased in increments of 10 devices at a time.
FortiPortal-VM Base License	FPC-VM-BASE	Customer self-service portal. Base license supports 10 managed devices (security instances): VDOM/VM/FortiGate. Security instance sending files to a Sandbox counts as two devices. Number of access points allowed is 10X the devices licensed. Requires FortiManager and FortiAnalyzer.
FortiPortal-VM Upgrade License	FPC-VM-10-UG	Upgrade license for adding 10 devices to FortiPortal-VM-BASE.
	FPC-VM-100-UG	Upgrade license for adding 100 devices to FortiPortal-VM-BASE.
	FPC-VM-1000-UG	Upgrade license for adding 1,000 devices to FortiPortal-VM-BASE.
	FPC-VM-5000-UG	Upgrade license for adding 5,000 devices to FortiPortal-VM-BASE.

FORTINET

www.fortinet.com