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 end-customer 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 client bandwidth usage and monetize through automation. This easy-to-deploy, turnkey portal delivers customer and device views that streamline the tasks of adding clients and devices.

With an audit view and a customizable dashboard containing intuitive widgets, customers can quickly see usage, traffic, and other useful summaries, while self-branding enables customer 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 portals.

**Customer Self-Serve Portal**

FortiPortal provides end-users with an easy-to-use self-service customer portal, giving them access to their secure SD-WAN capabilities, such as SD-WAN monitoring and templates, Policies and Objects, Analytical Dashboards, Views and Reports, WiFi, 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 view
- 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's low Total Cost of Ownership and fast time-to-market, while reducing complex development and maintenance costs
**ARCHITECTURE**

FortiPortal’s 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, and FortiAP, for simplified management of devices, configuration and analytics with real-time visibility and reporting for traffic, application, attacks, and web usage.

FortiPortal's 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 and access points across multiple customers 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 end-customer can contain multiple sites, and each site can contain one or more virtual domains (VDOMs), and VDOMs map to administrative domains (ADOMs) which are mapped to the customer. FortiPortal provides a single user interface across multiple instances and versions of FortiManager and FortiAnalyzer.

![Architecture Diagram]

**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 FortiAnalyzer and FortiManager through a simplified and easy-to-use interface, reducing complexity for both service providers and customers alike.

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

Dashboard

FortiPortal’s customer 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 predefined time ranges or specify a time period to display and investigate.

New Device Health dashboard provides insightful widgets for monitoring Device Uptime, Device Status and Policy Package Status with drill-down, Top CPU Load, Top Memory Usage, Top Number of Sessions and more.

Device Manager

Use the Device Manager tab to configure VPN IPSec, routers, and secure software-defined wide area network (SD-WAN). Authentication servers support LDAP with password reset support, Radius, Tacacs, and local authentication. Users also have the ability to view and manage their DHCP servers.

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, and vendor selection 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.

FortiPortal’s enhanced one-page SD-WAN Monitoring dashboard centralizes both secure SD-WAN data and SD-WAN monitor data from the device manager for a consolidated view of SD-WAN enabled devices, 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.

Views

FortiPortal’s View page provides comprehensive visibility into device and network configurations. It displays security and event information by application, source or destination, with filters and controls that allow easy navigation.

Customers gain meaningful insights into network activity and threats in the Monitors view with new secure SD-WAN widgets, VPN with History timelines for both SSL and Dialup, and Site-to-Site IPsec. Top Threats, Top Sources, Top Destinations, as well as Top Application, Top Browsing Users and Top Website Domain views provide intuitive FortiViews that can be filtered and searched with “text search” and predefined or custom time ranges.

Users can research further in Log View with FortiGate Event and UTM data, Traffic, IPS, Antivirus, DNS, Application Control, Web Filter, Event and Sandbox Logs, and allow users to filter by log type, site, date and time, as well as edit the settings to choose from many columns and fields. Users can now also export Log View results to a CSV file for a more thorough analysis, sharing of results or for auditing and compliance purposes.
FEATURE HIGHLIGHTS

Policy and Objects

Policy and Objects views allow users to centrally manage and configure the devices managed by the FortiManager unit. This function includes the basic network settings to connect the device to the corporate network, antivirus definitions, intrusion protection signatures, access rules, and managing and updating firmware for the devices.

FortiPortal’s Policy and Objects views provide 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 shows policy packages associated with either one or more FortiGate devices or VDOMs, or all devices within an ADOM.

Objects view enables users to view and manage items such as zone / interface, Firewall Objects like addresses, schedules, services, and Virtual IPs, as well as User Definitions and User Groups. Users can also now search URLs under Web Filter Profiles to easily narrow down results.

Reports

FortiPortal Reports provides administrators with the ability to easily create and assign reports to users. The Reports page displays a list of available FortiPortal or FortiAnalyzer reports and allows users to select reports, set filters, run reports, and search reports based on the roles assigned by the service provider.

Audit

The Audit tab displays a log of user activity on the administrative web interface by date, which can be searched by level, user, type, IP, or message description and then exported 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.

WiFi

Use the WiFi tab for updating or deleting managed access points (APs), monitoring rogue access points, Fortinet access points (FAPs), and SSIDs, and updating or deleting access point profiles and SSIDs.
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.

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

<table>
<thead>
<tr>
<th>System Requirements</th>
<th>FORTIPORTAL SERVER</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Version</td>
<td>VMware ESXi Version 5.5.X, 6.0.X, 6.5.X and 6.7.X</td>
</tr>
<tr>
<td>KVM Version</td>
<td>2.6.X</td>
</tr>
<tr>
<td>Recommended Minimum vCPU per Portal</td>
<td>2</td>
</tr>
<tr>
<td>Recommended Minimum Memory per Portal</td>
<td>4 GB</td>
</tr>
<tr>
<td>Recommended Minimum Storage per Portal</td>
<td>100 GB</td>
</tr>
</tbody>
</table>

**Supported Devices**

FortManager, FortiAnalyzer, VDOM/VM/FortiGate/FortiWiFi security instances, and FortiAP

---

## ORDER INFORMATION

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

<table>
<thead>
<tr>
<th>PRODUCT</th>
<th>SKU</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiPortal-VM Base License</td>
<td>FPC-VM-BASE</td>
<td>Customer self-service portal. Base license supports 10 managed devices (security instances): VDOM/V/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.</td>
</tr>
<tr>
<td>FortiPortal-VM Upgrade License</td>
<td>FPC-VM-10-UG</td>
<td>Upgrade license for adding 10 devices to FortiPortal-VM Base.</td>
</tr>
<tr>
<td></td>
<td>FPC-VM-100-UG</td>
<td>Upgrade license for adding 100 devices to FortiPortal-VM Base.</td>
</tr>
<tr>
<td></td>
<td>FPC-VM-1000-UG</td>
<td>Upgrade license for adding 1,000 devices to FortiPortal-VM Base.</td>
</tr>
<tr>
<td></td>
<td>FPC-VM-5000-UG</td>
<td>Upgrade license for adding 5,000 devices to FortiPortal-VM Base.</td>
</tr>
<tr>
<td>FortiPortal-VM Subscription License with Support</td>
<td>FC1-10-PCVMS-25B-01-DD</td>
<td>FortiPortal subscription license for 10 managed devices / virtual domains. FortiPortal software and FortiCare support contract is included. This SKU can be purchased in increments of 10 devices at a time.</td>
</tr>
</tbody>
</table>

---

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet discloses all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet’s internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.