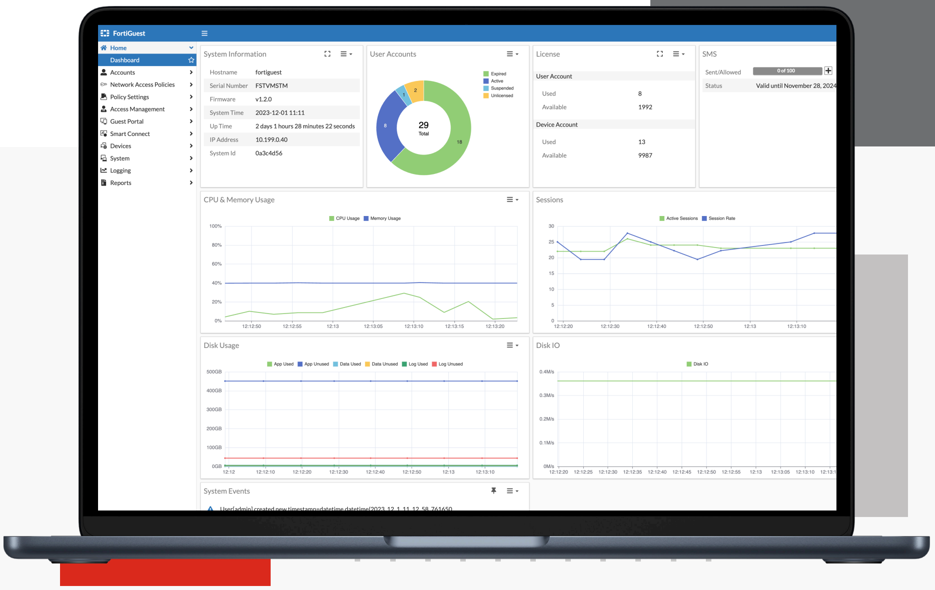
FortiGuest



System Information

Hostname fortiguest
Serial Number FSTVMSTM
Firmware v1.2.0
System Time 2023-12-01 11:11
Up Time 2 days 1 hours 28 minutes 22 seconds
IP Address 10.199.0.40
System Id 0a3c4d56

License

User Account
Used 8
Available 1992

Device Account
Used 13
Available 9987

SMS

Sent/Allowed 0 of 100
Status Valid until November 28, 2024

Highlights

- Seamless integration with multi-vendor network infrastructure and client platforms
- Policy- and role-based provisioning of wireless/wired network access
- Ease of use for both IT staff and end users
- Enterprise-strength authentication and encryption
- Reduced IT workload
- Easily deployed payment options
- Integrated RADIUS server for quick and easy deployment of AAA services
- Dynamic network access control with RADIUS CoA
- RADIUS and LDAP Authentication

Simplified Guest Access, BYOD Onboarding, and Policy Management

FortiGuest is a sophisticated network security solution specifically designed to address the challenges of guest access in modern environments. By providing a seamless and secure method for granting temporary network access to visitors, contractors, and partners, FortiGuest streamlines the process while maintaining the highest level of network integrity.

With its advanced authentication protocols, comprehensive access controls, and real-time monitoring capabilities, FortiGuest ensures that guest users can enjoy a hassle-free and protected experience. Whether it's controlling bandwidth usage, preventing unauthorized access, or safeguarding sensitive data, FortiGuest offers a robust and reliable solution for managing guest access while prioritizing network security.

Deployment

Available in

Virtual

For Any User On Any Network With Any Device

Packaged in a simple, wizard-driven application, FortiGuest addresses all aspects of deploying BYOD and managing IT workloads effectively, including:

- Onboarding for internet access with 802.1X authentications, across multiple operating systems (iOS, Android, Microsoft Windows, Apple Mac OS X, ChromeOS) and devices (laptops, smart phones, tablets)
- Vendor-agnostic, wired and wireless network user access, device onboarding, policy and access management
- Role- (visitor, contractor, employee) and device-based policy management
- Integrated reporting and auditing
- Retrieval and verification of identity- and group-based policies across multiple identity stores (LDAP/AD, RADIUS, SAML, RadSEc, External DB, and social networking identities)
- Integrated policy and reporting across specialized policy enforcement devices like firewalls
- Optimization for running on virtualized environments

Key Features and Benefits

- Fully-integrated platform for policy- and role-based provisioning of wireless and wired network access
- Seamless integration with multi-vendor network infrastructure and client platforms
- Simplified secure user access and BYOD
- Support for existing infrastructure and employee or visitor devices

Social media option for user onboarding

Access policy gated by both user and device

- Enterprise-strength authentication and encryption
- Comprehensive activity monitoring and reporting
- Protection of the network and sensitive data
- Appropriate use and audit support

Highlights

User Roles

FortiGuest looks at a variety of device and role trust relationships to provide unique access across common scenarios found in enterprises, schools, universities, hotels, and other places of business. They can be summarized as follows:

	DEVICE TYPES	
USER ROLES	CORPORATE OWNED (TRUSTED)	EMPLOYEE OWNED (UNTRUSTED)
Employee (Trusted)		
Hotel managers, engineers, doctors, nurses, teachers, faculty	Trusted access; Tightly controlled corporate identity server (AD, LDAP). Full access to resources allowed by role.	Onboarding required; restricted access based on policy. Possibly, restricted access to resources allowed by role.
Contractor (Trusted)		
Consultants, temporary workers, vendors at event, students, conference staff	Trusted access; Tightly controlled corporate identity server (AD, LDAP). Full access to resources allowed by role.	Onboarding required; restricted access based on policy. Possibly, restricted access to resources allowed by role.
Guest / Visitor (Untrusted)		
Patients, ticketed audience, parents	Untrusted access – Self provisioning or sponsored visitor access. Internet only access.	

Highlights

User Access

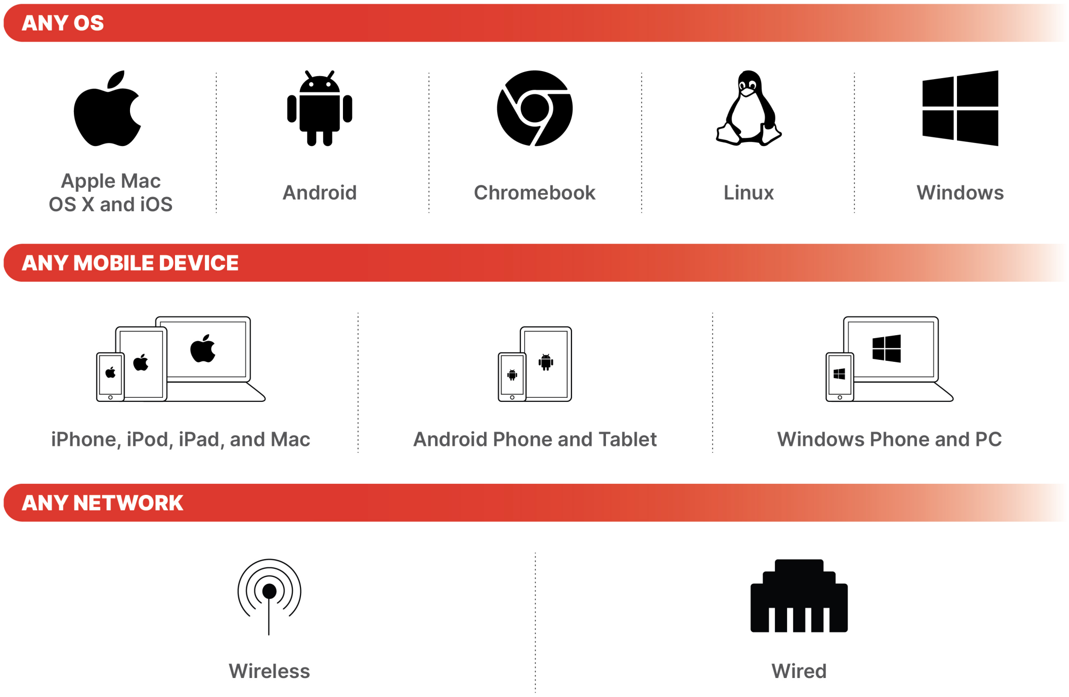
User access offers both sponsored and self-provisioned user or visitor account creation. Multiple accounts can easily be created by uploading account information into FortiGuest or creating accounts in bulk with random usernames and passwords. With FortiGuest, account management functions, creation, updates, password changes, notifications, deletion, and reports, are all customizable based on a variety of types of sponsors. These options include self-sign, front desk at a hotel, front desk at a carpeted enterprise, and security at a company.

User access is optimized for ease of use, for both administrators utilizing SAML and end users. It is client-platform agnostic and supports any platform with a web browser, including iOS, Android, Apple Mac OS X, and more.

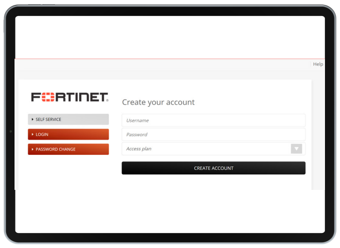
Using social identity (Google, Facebook, Linux, and Twitter accounts) for network access is becoming a larger trend for unpaid access. This situation creates a win-win for the provider and the subscriber. For providers requiring paid access, multiple credit card billing services are natively supported and easy to deploy.

Brand-presence management is catered through the fully-customizable, mobile-adaptable login portal and walled garden. User account notification can be managed through SMS, a self-service kiosk, or email, creating a great experience for the user. Administrators can also provide a variety of portals for visitors logging into their networks based on their locations and languages, as well as whether or not they are using a traditional laptop, smartphone, or tablet. FortiGuest supports captive portal with enhanced regional language customization.

FortiGuest supports any OS, any mobile device, and any network - regardless of vendor.



Highlights



Access Policy and Policy Management

Of paramount concern with networks is the enforcement of appropriate policies for visiting users. With FortiGuest, administrator-defined individual, group, or general policies can have customized time-based access, usage-based access, or location-based access. Access to specific resources as well as bandwidth usage restrictions may be placed on user accounts as well. In addition, FortiGuest can grant access by looking at user and device policy combined. This process means that even if the user is a trusted user, FortiGuest can still not allow access to the network due to an untrusted device that user is using. However, for a trusted device and user, full network access can be granted.

One of the major complaints against user access through a web portal is the need for users to re-enter their credentials after their devices “wake up” from the power-save induced sleep mode. FortiGuest securely addresses this concern to reconnect without having to enter credentials and still be under the same policy guidelines that were set up for the user profile.

Businesses large and small are moving their IT services such as email, file shares, archiving, and identity services to public cloud providers such as Google. FortiGuest integrates with Google apps to authenticate users and guests and onboard them into the network with appropriate policies.

FortiGuest is not vendor-agnostic for Captive portal redirection from third party WLAN vendors.

Business Systems Integration

FortiGuest integrates with existing authentication. This avoids duplication of data, maximizes appropriate use of these resources, and provides a single view into reporting and policies associated with usage.

Simplify BYOD Provisioning

FortiGuest also provides employees and other trusted users a way to onboard their trusted and untrusted devices on the secure network. It provides the administrator with flexibility to decide on the correct level of policy for untrusted devices brought onto the network by a trusted user.

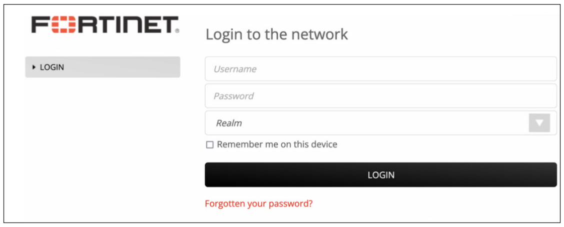
Onboarding refers to auto-provisioning of corporate- or employee-owned devices to use secure (typically 802.1X authenticated) networks. This rule could be true of wireless or wired infrastructures.

FortiGuest provides a set sequence of events for non-technical employees and contractors to set up their devices with appropriate 802.1X settings for accessing the wired or wireless network. A standard web portal (different from the secure network) is initially presented for the user to enter their corporate credentials. Once a device connects, its type is detected, the credentials are verified against a backend device, and based on the administrator’s configuration, appropriate secure network access settings are downloaded to the device. The device is then disconnected from the web portal network and reconnected to the secure network using the new secure settings.

All of the steps done without the need for a client agent, thus providing ease of deployment and scale. This workflow is very intuitive for the end users and removes their dependence on IT to onboard their devices. Also from an IT perspective, since the settings are done centrally, policies can be set effectively and uniformly based on user role, device role, and device type.

Highlights

FortiGuest Walkthrough: Device Onboarding

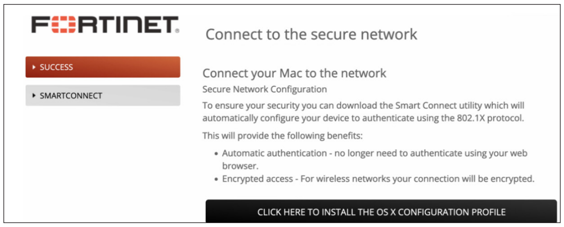


Login to the network

☐ Remember me on this device

Forgotten your password?

1. Verify login using web authentication



Connect to the secure network

Connect your Mac to the network

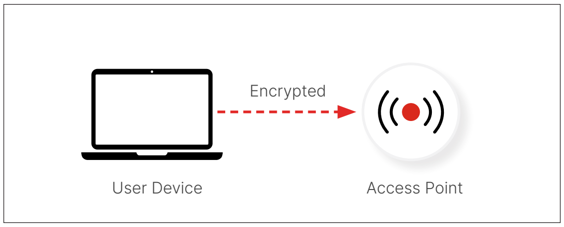
Secure Network Configuration

To ensure your security you can download the Smart Connect utility which will automatically configure your device to authenticate using the 802.1X protocol.

This will provide the following benefits:

- Automatic authentication - no longer need to authenticate using your web browser.
- Encrypted access - For wireless networks your connection will be encrypted.

2. Download an applet to configure 802.1X



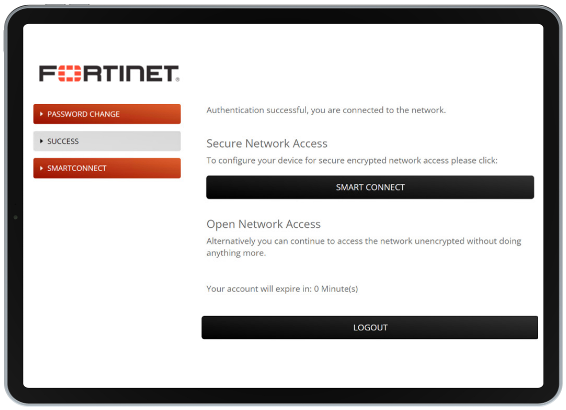
3. Automatically connect with 802.1X

Secure and Simple Onboarding

Policy is managed via user roles from the corporate identity server such as AD or RADIUS as configured, into the secure profile. The device policy is added to this profile for a complete view of that session.

Device authentication and policy management can also be done using device onboarding for devices such as printers, connected hospital equipment, and other devices that need to be authenticated before being let onto the network. This action is especially true of devices that are temporary or short-term leased and do not warrant being managed in the corporate identity servers.

FortiGuest seamlessly integrates mobile and traditional laptop platforms including Apple Mac OS, iOS, Android, Linux, and Windows operating systems for onboarding purposes. It also supports setting up supplicants for a variety of secure 802.1X protocols including PEAP-MSCHAPv2, PEAP-GTC, and EAP-TLS.



Authentication successful, you are connected to the network.

Secure Network Access

To configure your device for secure encrypted network access please click:

Open Network Access

Alternatively you can continue to access the network unencrypted without doing anything more.

Your account will expire in: 0 Minute(s)

Specifications

TECHNICAL	
VIRTUAL APPLIANCE SYSTEM REQUIREMENTS	
Minimum Hardware Specifications	4 GB memory, 500 GB disk space, 4 CPU
Hypervisor Support	ESXi 7.0.3 and above
	Microsoft Hyper-V on Windows 2008 and later
	Linux KVM virtual server version1.5.3 and above
CLIENT PLATFORMS SUPPORTED	
Smart Connect Support	Windows 10 and 11
	Android version-11,12,13
	ChromeOS 116.x
	Linux-Ubuntu version 20.04,22.04
	iOS 15,16
	macOS 12.04
SUPPORTED IDENTITY STORES	
RADIUS	
RadSec (TLS encoded RADIUS)	
Microsoft Active Directory	
SAML	
Any LDAP compliant Directory	
MySQL, Microsoft SQL, PostgreSQL, and Oracle SQL	
Built-in local store	
Facebook, Twitter, Google	
FRAMEWORK AND PROTOCOL SUPPORT	
RADIUS, RADIUS Dynamic Authorization	
RadSec (TLS Encloded RADIUS)	
802.1X-2010, 802.1X-2020	
PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)	
WPA2, WPA3	
PAP, MSCHAPv2	
Online Certificate Status Protocol (OCSP)	
BROWSERS SUPPORTED	
Safari	
Microsoft Edge	
Chrome	
Firefox	
BILLING SUPPORT	
Credit Card Billing Support	Paypal
	Authorize.net
	Peach Payment
	Secure Pay
	Secure Pay API
	Sage Pay
PMS Support	Oracle Cloud PMS
	Hobic
Guest Onboarding	SINE Core

Ordering Information

Product	SKU	Description
FortiGuest Subscription	FC1-10-STVMS-493-01-DD	FortiGuest license subscription for 25 users. Includes 24×7 support.
	FC2-10-STVMS-493-01-DD	FortiGuest license subscription for 500 users. Includes 24×7 support.
	FC3-10-STVMS-493-01-DD	FortiGuest license subscription for 2000 users. Includes 24×7 support.
	FC4-10-STVMS-493-01-DD	FortiGuest license subscription for 10 000 users. Includes 24×7 support.

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.

www.fortinet.com

December 7, 2023