DATA SHEET

Fortinet Connect

Available in:

Appliance | Virtual Machine | Hosted | Cloud

Simplified Guest Access, BYOD Onboarding, and Policy Management

Fortinet Connect allows network administrators to quickly and easily provide Wireless Guest Access. It also gives tools to enable role and policy management and reporting throughout the BYOD life-cycle.

For any user on any network with any device

Packaged in a simple, wizard driven application, all facets of managing IT workload in deploying BYOD are addressed effectively:

- Onboarding for web and 802.1X authentications, abstracted across multiple OSs and devices (laptops, smart phones, and tablets) with iOS, Android™, Microsoft® Windows®, Apple® MacOS X®, and Linux®
- Wired and wireless network vendor-agnostic user access, device onboarding, policy and access management
- Role (visitor, temporary user, and employee) and device based policy management
- Integrated reporting and auditing
- Integration across vertical-specific applications (property management systems and payment gateways) for ease of deployment
- Retrieval and verification of identity and group based policies across multiple identity stores (LDAP, RADIUS, social networking identities, and other databases)
- Integrated policy and reporting across specialized policy enforcement devices like firewalls
- Integration with leading MDM vendors to define policies based on device compliance
- Enterprise grade clustering for scalability and high-availability
- Tailored to run on Fortinet Service Appliances or virtualized environments running VMWare

Highlights

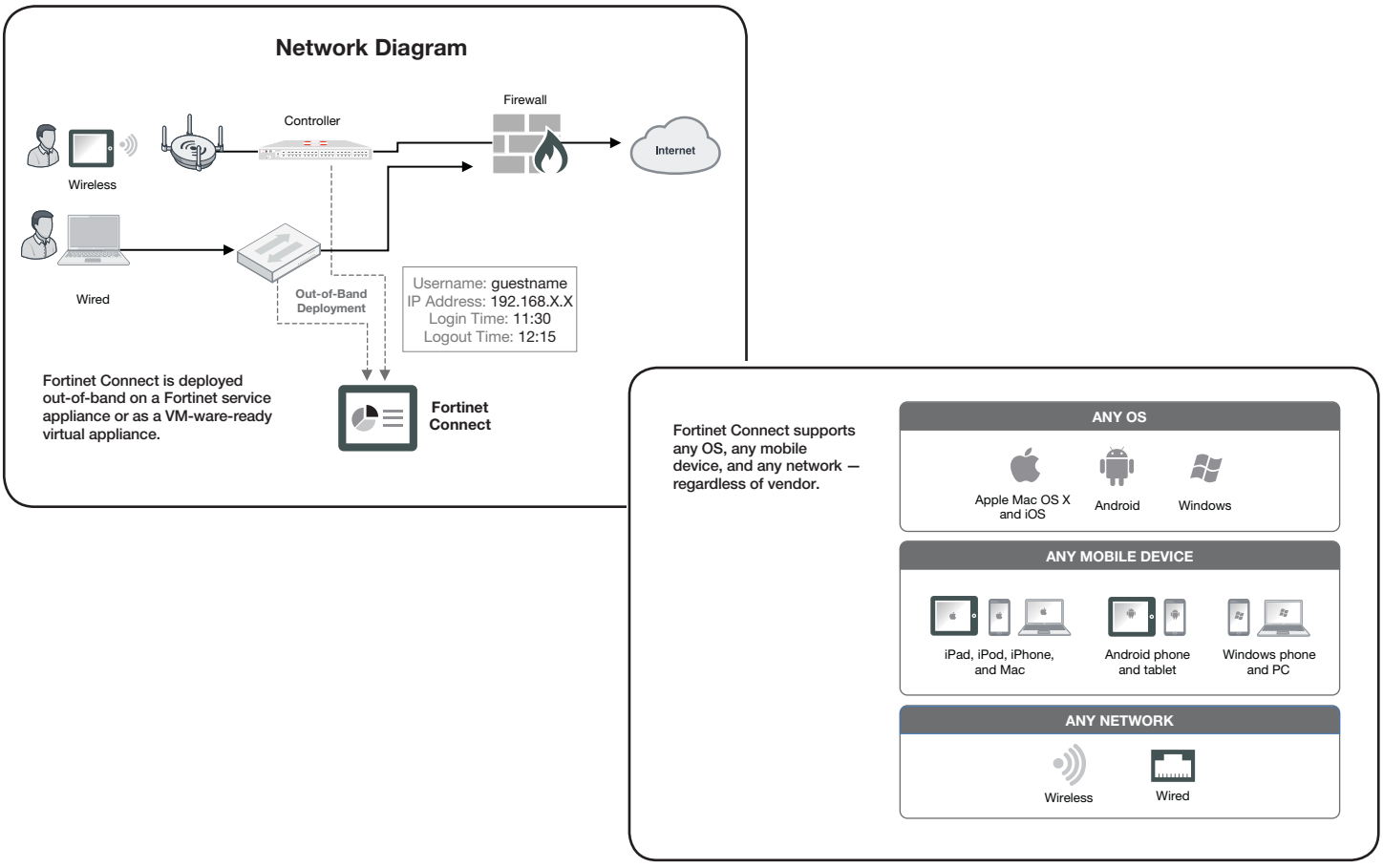
- Seamless integration with multi-vendor network infrastructure and client platforms
- Policy and role-based provisioning of wireless/ wired network access
- Optimized for ease-of-use for both IT staff and end users
- Enterprise-strength authentication and encryption
- Dramatically reduces IT workload
- Supports existing infrastructure and employee devices
- Protects the network and sensitive data
- Enterprise-strength 802.IX authentication
- Integrated RADIUS server for quick and easy deployment of AAA services
- Dynamic network access control with RADIUS CoA

HIGHLIGHTS

Fortinet Connect 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 common 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), Fully MDM controlled. Full access to resources allowed by role.	Onboarding required; restricted access based on policy, MDM registered. 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), Fully MDM controlled. Full access to resources allowed by role.	Onboarding required; restricted access based on policy, MDM registered. Possibly, restricted access to resources.
Guest / Visitor (untrusted)		
Patients, ticketed audience, parents		Untrusted access – Self provisioning or sponsored visitor access. Internet only access.

Fortinet Connect addresses the above scenarios via built in services to integrate user end-to-end access and to securely onboard employees with personal or corporate devices under policy management.



HIGHLIGHTS

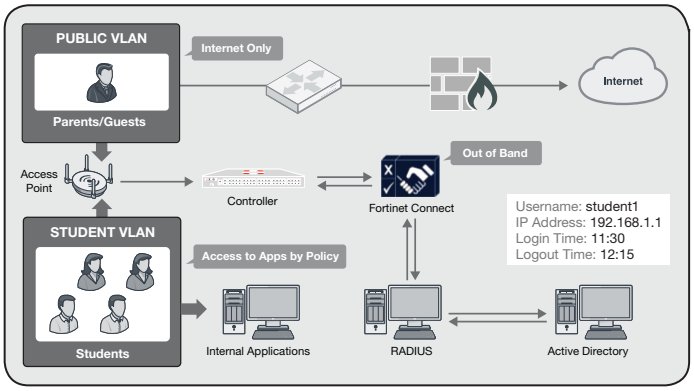
Simplify User Access for any OS on any Network

Introduction

User access is no longer a nice-to-have feature in an enterprise. Wired and WLAN user access is mandatory and web authentication due to its simplicity and ease of deployment has become the prevalent user access mechanism. User access creates a strong brand presence and in some verticals, such as hospitality and event management, has direct revenue and customer satisfaction consequences. To address the myriad of user access requirements associated with different businesses, the user access service in Fortinet Connect provides administrators, sponsors, and users a full toolset of services to provision and manage guest accounts and their activity on the network with appropriate role-based policies.

Fortinet Connect Walkthrough: User Access

User access offers both sponsor and self provisioned user/visitor account creation. Multiple accounts can be easily created by uploading account information into Fortinet Connect or bulk creating accounts with random usernames and passwords. Engaging IT staff for managing user accounts is neither practical nor economic. In some cases such as hospitals or in event centers or arenas, handing this duty to non-IT staff such as security personnel or event coordinators is cumbersome and tedious. In the carpeted enterprise, particularly security conscious enterprises, however, sponsors (such as employees hosting meetings with guests) are required to invite users and manage their accounts for full audit management. Account management functions — creation, updates, password changes, notifications, deletion and reports — are all customizable based on a variety of types of sponsors such as self-sign, front desk at a hotel, front desk at a carpeted enterprise, or security at a company.



Fortinet Connect makes it easy to authorize internal sponsors to create guest accounts. You can also enable guests to securely self-provision.

Guest access on tablets

Brand presence management is catered to through the fully customizable, mobile-adaptable login portal and walled garden. User account notification can be managed through SMS, self-service kiosk, or email creating a perfect experience for the user. Administrators can also provide a variety of portals for visitors logging into their networks based on their location, language, as well as whether or not they are using a traditional laptop, smartphone, or tablet. Fortinet Connect supports 35+ languages out of the box for customizing the user and sponsor portal to every locale that the business caters to.

Of paramount concern with networks is the enforcement of appropriate policies for visiting users. 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 the user accounts as well.

One of the major complaints against user access through a web portal is the need for users to reenter their credentials after their devices wake up from the power-save induced (for saving on battery life) sleep mode. Fortinet Connect securely addresses this concern to reconnect without having to enter credentials and still be under the same policy guidelines that you set up for the user profile.

User access is optimized for ease-of-use, for both administrators and end users. It is client platform agnostic and supports any platform with a web browser, including iOS, Android™, Microsoft® Windows®, Apple® MacOS X®, Linux®, and more.

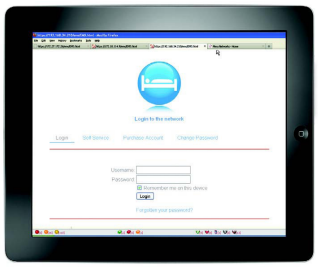
Using social identity (Twitter or Facebook accounts) for network access is becoming a larger trend for unpaid access. This trend creates a win-win for the provider and the subscriber. Capturing the identity is a great marketing asset for service provider-led targeted marketing campaigns for the users, and for users it provides exchanging your Facebook likes for unpaid access to the WiFi network.

Businesses large and small are moving their IT services (such as email, file shares, archiving, and identity services) to the cloud to providers such as Google. Fortinet Connect integrates with Google Apps to authenticate users and guests to onboard them on the network with appropriate policies.

Fortinet Connect supports networking switches, APs (and controllers) from most major vendors. Such vendor agnostic interoperability means the ability to leverage your existing investments.

BUSINESS SYSTEMS INTEGRATION

Businesses have existing authentication, billing and network infrastructure. Fortinet Connect integrates with these business systems seamlessly to avoid duplication of data, maximize appropriate use of these resources and provide a single view into reporting and policies associated with the usage.



Hospitality

In a traditional hospitality setting at a hotel, lodge, or resort, guest access is often considered a value add for individual customers. Integration with existing property management systems makes the guest experience seamless — hotel guests can gain access to the wireless network using their room number and name and if it is a paid service, charge it to the room. Due to integration with a variety of leading PMS (Property Management Systems), centralized billing and account management is easy through Fortinet Connect using either front desk provisioning or self-registration. Guests with valid accounts can get online as soon as they are in range of the wireless network without entering their credentials to have a better guest experience.

User access provides the ability to not only address all of these situations but also provide tiered access. For example, provide free internet access for a short duration of time, based on the user sharing their Facebook account name vs. providing a higher bandwidth account on a paid service.

Tiered services (e.g. paid vs. free network services, or higher bandwidth vs. restricted bandwidth network services) may also be provided by checking on a guest account's "status" against a loyalty program. Authentications can be performed not only against a local database but also against other databases such as standards-based SQL or RADIUS or LDAP identity stores.

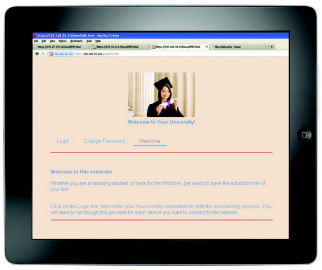
Fortinet Connect supports a wide variety of transport-related scenarios as well, such as wireless network services for cruise ships, buses, trains and airplanes. Passengers can readily gain access to the wireless network using their transportation ticket information or pay for it using a variety of payment processing systems. Other options include charging to a loyalty program, cruise ship cabin room, etc. Transportation staff can gain access to additional network, business system & IT resources based on their assigned roles and privileges.

For conventions and conferences, hotels, or convention centers typically want to associate a specific event with an event code to track the users and associate policy based on the tiered service they offer. Fortinet Connect provides a simple and efficient means for such cases.

Arenas, stadiums, and other public spaces require a different set of access means. While most of these are public spaces, the access to the network could be one of:

- A simple click-though acknowledging the terms of use
- Providing some information (email address or mobile phone number) to subscribe to the network
- Logging on to the network using social media credentials such as your Facebook or Twitter account
- Paid service using credit card or PayPal based payment for network access. A full PCI report is available through the Fortinet Connect interface for all credit card based transactions.

Education



The eduroam initiative allows secure, worldwide roaming access for the research and education community. Eduroam allows students, researchers and staff from participating institutions to obtain Internet connectivity across campus and when visiting other participating institutions by simply opening their laptop. Fortinet Connect supports eduroam for authentication of visiting faculty, students and scholars.

User access for parent-teacher meetings, homecoming or other special events can be easily arranged using dedicated per-user self-registration or open access along with policy management across both wired and wireless networks. Bulk users can be created by importing a list of visitors or creating random usernames and passwords.

User access, through security policies set by the enterprise or through government regulations, requires tracking and maintaining audit information regarding the user account from its creation, activation, usage (including details on what websites/ applications were accessed) through its expiry and deletion or reactivation in the system.

User access provides integrated, exportable reports at both the administrator as well as the sponsor level. Auditing reports are generated by correlating user information across network infrastructure against the account information in Fortinet Connect.

HEALTHCARE

With the growing demand for better care for patient and their visitors in healthcare institutions outside of medical treatment, providing WiFi access has become a norm. However, with legitimate security and bandwidth management concerns, providing reliable, auditable, and self-serviced or free internet access is possible with Fortinet Connect.

User access combines the ability to self-service the user creation process via its highly customizable web portal. It also allows the administrator to automatically provision and enforce a preset bandwidth and/or data limit to each individual user so as to keep the network available for other more mission critical usage. For longer duration guests, devices and usernames can be remembered using a "remember me" feature to make the user experience better while still keeping the network secure. Customization of portals and creation of a sophisticated walled garden offers the ability to provide additional information to visitors as well as manage the branding and marketing for the institute. User access portals are available in 30+ languages out-of-the-box and with little customization can be used for a variety of patients from different ethnicities to make them feel at home and comfortable.

Features and Benefits

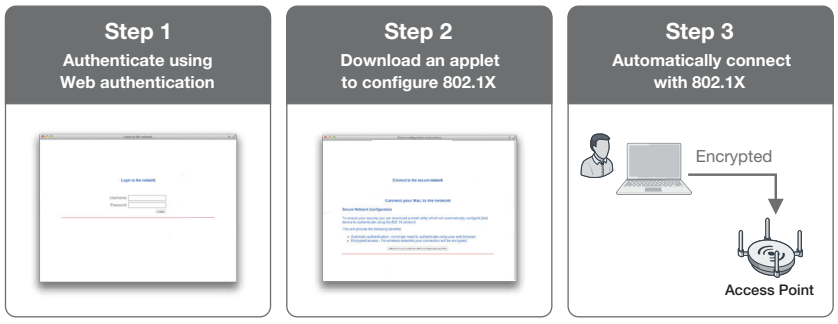
- Automated wireless/wired user management — optimized for ease-of-use
- Seamless integration with multi-vendor network infrastructure and client platforms
- Fully customizable guest portal
- Comprehensive activity monitoring and reporting
- Simplifies secure user access to dramatically reduce IT workload
- Supports existing infrastructure and visitor devices
- Promotes your brand and ensures an outstanding end-user experience on any client
- Restricts guest access to authorized users only
- Ensures appropriate use and supports audit requirements

Simplify BYOD Provisioning for any OS on any Network

Fortinet Connect 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 the untrusted devices being brought onto the network by the trusted user.

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

Fortinet Connect Walkthrough: Device Onboarding



Fortinet Connect provides a set sequence of events for non-technical employees and contractors to setup 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 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 are done without the need for a client agent residing on the device 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 both the user role, device role, and the device type.

SIMPLIFY BYOD PROVISIONING

Policy is managed using 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 to provide a complete view for that session. Fortinet Connect also integrates with leading MDM vendors to create a unique layered policy management framework to enhance the native user and device based policy with inputs from the MDM server. Using a dynamic authorization mechanism, the session attributes may be changed any time based on inputs and behavior of the session on the network.

In schools, the beginning of a semester or school year is the busiest time. With new students coming to school new devices need to be onboarded. Using device onboarding capability drastically reduces IT time, complexity, training, and reduces errors both from a misconfiguration as well as policy management perspective saving time and resources to troubleshoot and rework client devices. With the introduction of new devices every year, rather than having a new release covering onboarding, device onboarding provides a unique capability to just update the support for the supported devices automatically.

Healthcare demands flexibility for doctors and caregivers to bring their own devices but regulations and privacy policies mandate severe restrictions on data being shared or stored on these devices. Fortinet Connect meets this challenge twofold — user and device role-based policy access, and applications that the user can access. Based on the device the user is accessing the network with, even if the user is a trusted user, Fortinet Connect can distinguish the untrusted device and not allow access to the network. However for a trusted device and user, full network access can be granted. Also, based on whether the device is registered with the MDM system and in compliance with application policies, Fortinet Connect can change the necessary privileges on the fly based on input from the MDM systems.

Secure and simple onboarding

Authentication and policy management can also be done using device onboarding for machines such as printers, connected hospital equipment (such as infusion pumps, heart monitors, and blood pressure monitors) and other devices that need to be authenticated before being let onto the network. This service is especially true of devices that are temporary or short-term leased and do not warrant being managed in the corporate identity servers.

Fortinet Connect seamlessly integrates mobile and traditional laptop platforms including Windows, Linux, MAC OS, iOS, and Android operating systems for onboarding purposes. It also supports setting up supplicants for a variety of secure 802.1X protocols including PEAP-MSCHAPv2, PEAP-GTC, EAP-TLS, as well as non-802.1X authentication mechanisms PAP and CHAP.

Key Features and Benefits

Fully integrated platform for policy- and role-based provisioning of wireless/wired network access	Simplifies secure user access and BYOD
Seamless integration with multi-vendor network infrastructure and client platforms	Supports existing infrastructure and employee/visitor devices
Enterprise-strength authentication and encryption	Protects the network and sensitive data
Comprehensive activity monitoring and reporting	Ensures appropriate use and supports audit requirements

SPECIFICATIONS

TECHNICAL	SUPPORTED
Virtual Appliance System Requirements	
Minimum hardware specifications: 2 GB memory, 50 GB disk space, 2.0 GHz CPU	✓
VMware support: ESX 4.xi and above	✓
Microsoft Hyper-V on Windows 2008 and later	✓
Client Platforms Supported	
Android 2.1 and greater	✓
Apple iOS 7.0 and greater	✓
Apple Mac OSX 10.7 and greater	✓
Windows 10, Windows 7, Vista, XP SP3	✓
Linux Ubuntu	✓
Authentication	
Active Directory	✓
LDAP	✓
RADIUS / RadSec	✓
Kerberos	✓
Facebook	✓
Twitter	✓
Google Apps	✓
SQL Database	✓
Protocols Supported	
802.1X PEAP-GTC	✓
PEAP-MSCHAPv2	✓
PEAP-TTLS WPA	✓
WPA-PSK WPA2	✓
WPA2-PSK	✓
Supported Browsers	
IE 7.0 and higher	✓
Safari	✓
Chrome	✓
Firefox	✓

Please note the range of Fortinet infrastructure access points are supported by a combination of specific controller firmware and hardware and are not designed to function with third-party controllers. Specific supported access point and controller combinations will change from time to time and such changes are detailed in the respective firmware release notes. The Fortinet range of controllers, whether they are infrastructure or integrated into FortiOS, only support Fortinet provided access points. Note that not all access points are supported by all controller types.

ORDER INFORMATION

Product	SKU	Description
Fortinet Connect	MCT-100-U	Fortinet Connect — Includes licenses for up to 100 user and device access licenses.
	MCT-1000-U	Fortinet Connect — Includes licenses for up to 1,000 user and device access licenses.
	MCT-10000-U	Fortinet Connect — Includes licenses for up to 10,000 user and device access licenses.

Support and virtual appliance or hardware appliance quoted separately

FORTINET

www.fortinet.com

CN-DAT-R5-20220517