



UniFi OSS for
Enterprise Guest Access



Security, convenience, and ease of operations are among the primary requirements for enterprise IT managers as they prepare their wireless networks for guest access. Besides the employees, IT managers have to support controlled access for business partners, suppliers, vendors, and other frequent visitors to the network. And it has to be easy for visiting executives and special guests to access the network.

Employees also demand additional flexibility into how they access the wireless network. More often than not, employees demand access associated with their identity, instead of the devices they use. Sometimes, IT requirements dictate access control that include the device, the user, and other corporate IT security standards such as virus checks, automatic VPN connectivity, etc. Above all, these networks are required to be regulated in terms of per-user bandwidth allocation with traffic prioritization for employees and executives, partners and guests, etc.

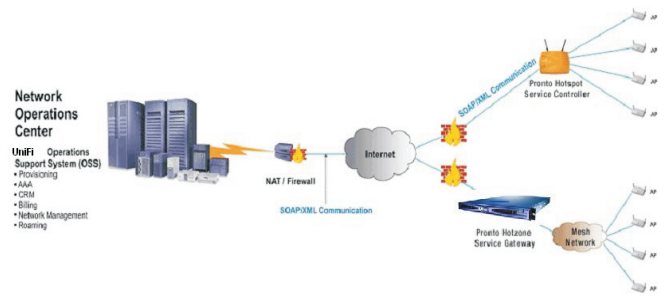
These capabilities are now expected to operate transparently over the new wireless as well as the existing wireline network.

Pronto Networks' UniFi OSS for Enterprise Guest Access allows IT managers to solve these issues while providing additional flexibility in their enterprise deployment. Some of the highlights of the offering are listed here.

Enterprise Guest Access Network Features:

Guest Access Network Capabilities:

- The internal wireless and wireline network can be logically partitioned using VLANs (or with SSIDs) to provide separate network bandwidth partitions.
- The same solution can be made applicable to both the enterprise wireless and wireline network.
- The solution allows for registered access that is approved by a employee sponsor or the IT manager.
- The administrator can control or restrict the number of simultaneous visitors/guests that are allowed on the enterprise network.
- An easy access method is now available for unregistered employees, or visitors, or business partners, suppliers etc.. Once obtaining the access codes, the visitor simply invokes the Internet browser on his device, and enters the credentials on a login page that is presented. Successful authentication by this login page allows the visitor to have the regulated access to the network.



- Optionally, a thin bandwidth regulated pipe for minimal access can be provided, thus alleviating the need for administered access.

Employees can be provided flexible access methods as well:

- The primary objective of continued secure access for employees throughout the enterprise, wireless or wireline, is maintained.
- If desired, employees can be authenticated separately from their devices. This is useful where the access devices (laptops, workstations, kiosks, etc.) are shared among a number of employees.
- The solution also enables both employees and guests to access the network from the same physical terminal, but with different security and bandwidth considerations.
- Employee access can be authenticated against an existing employee database, locally or network wide for multi-location enterprise deployments.

Some of the guest registration and access options available are as follows:

- An employee could sponsor a visitor, creating an access account on their behalf. This account information can then be provided to the guest/visitor automatically via email, or manually by the sponsor.
- A set of visitor access accounts can be created and provided to the reception desk. Users would be required to provide some specific information before they are allowed to access the network.
- Access to the network can be limited by the administrator and/or the employee sponsor. The enterprise IT manager may choose to specify the limits of the access, i.e. a day pass, a 2 hour access, etc. Different types of guests can be provided different levels of access.



- The enterprise can allow for the creation of a vendor pass that would enable access at all the enterprise locations. Optionally, the IT manager can restrict access on a per location basis.
- For executive access, a set of accounts can be created/maintained (like guest accounts) by the IT manager, that is then provided to the executive guest, making it that much more convenient for the executive visitor.
- Branded USB keys can also be created and distributed to visitors. These USB keys contain encrypted credentials that allow guests to access the enterprise network by simply invoking their browser and accessing the Internet with the USB key inserted in their laptop or PDA. The system allows for the easy deactivation and deletion of the keys by the Enterprise IT manager.
- Reports can be created / maintained, etc. to track creation, usage of these accounts, and the access history details.

Pronto Technology Highlights

The primary features of the UniFi solution that are leveraged in the above examples are:

- IP based secure authentication for controlled and registered access to the network: Regardless of the user or device, this feature ensures that each entity that attempts to access and transmit data across the wireless network is an authorized user. Besides the employees of the enterprise that can have their credentials validated automatically, this authentication also applies to devices such as servers, kiosks, etc., and users that avail themselves of the minimal access bandwidth provided by the “guest access” model.
- Partitioning of wireless network traffic, based on types of users, applications, and priorities: Different sets of users can be partitioned into bandwidth pipes, logically defined in the network, so that each user is restricted to bandwidth in their own pool, and high priority users, such as IT managers, executives, or some set of employees, are always guaranteed their bandwidth, regardless of the number of other types of users on the network. In addition, the network can be carved into VLANs for an added level of bandwidth partitioning.

- Customized registration portal: Various options presented for the Enterprise Manager that allows guests to register themselves, or have pre-registration done on their behalf by a sponsoring employee, etc. Enterprise managers can also create guest access codes for distribution from the reception or directly to the guests.
- User access control and content filtering before and after authentication: For the “guest access” users, and to



support multiple levels of access, the UniFi OSS allows for the configuration of white-listed sites, or “walled-garden” sites, that are accessible to users before authentication. Optional content filtering capabilities are also available that allows the enterprise to deploy a per user-type based content filtering mechanism to meet the access control needs for the different types of users in the network.

Managed Services Platform and Software License options

Besides a UniFi OSS software license purchase, Pronto offers a Managed Services Platform (MSP) option to its customers. In the MSP model, Pronto provides the back office operations functions, including network monitoring, 24/7 customer service, billing and revenue distribution, reports, and system maintenance. Depending upon their preferred business model, enterprises may wish to either invest one's time and take complete ownership, or spread the ownership over time and seek Pronto's services in the maintenance and management of the network. Enterprises may also choose to purchase the UniFi OSS license and carry out the NOC operations for their own internal users as well as for their commercial partners as a service or for other business reasons.



Pronto Networks Corporate Headquarters
4637 Chabot Drive, Suite 350
Pleasanton, CA 94588
925 227 5500

