Cambium Networks™ | XIRRUS

SOLUTION BRIEF

Xirrus EasyPass Access Services

Laptops, tablets, smart phones, wearables, printers, sensors, etc.—the massive number of Wi-Fi devices and the frequency with which we use them today necessitates an easy way to connect to a network. Xirrus EasyPass combines security with simplicity, allowing guests, visitors, and employees/students quick access while giving IT administrators the ability to track user activities and protect data.

Xirrus EasyPass simplifies administration and management of secure access for bring your own devices (BYOD) and Internet of Things (IoT) devices, streamlining IT operations while significantly simplifying the user experience. EasyPass does not require changes to your current network and its services can be easily integrated with existing user databases and application ecosystems systems such as Microsoft Office 365 and Google Apps, as well as point of sale, student directories, and ticketing systems.

In the current world of BYOD and IoT, access to information is vital to positive business outcomes. Mobile and cloud-based enterprise applications are deployed at a feverish pace. Every monolithic application adds complexity for users, forcing them to utilize unique credentials every time they access and adversely impacting productivity. Xirrus EasyPass Access solutions help companies address these challenges.

> *Because there will be multiple devices brought to office environments more frequently, network designers must select solutions that offer ease of onboarding new devices and their many operating systems.*
>
> *- Christian Canales, Bjarne Munch*

(Gartner Research Paper G00262687 - Mobile Device Proliferation Is Forcing Network Leaders to Redesign Enterprise Wireless LANs)

Challenges in the Wi-Fi World

Connected living has become a way of life for both business and leisure mobile users. Guests, employees, students, contractors, temporary workers, fans at a stadium, attendees at a convention, patrons at a concert – the list goes on – all demand access to information from wherever they are.

On one hand, performing job functions from personal devices has become easier with business applications moving to the cloud. In fact, business executives consider connectivity a competitive advantage and critical to the success of an operation because access has proven to increase revenues by improving employee productivity and customer satisfaction.

But as users carry multiple computing devices, wearable devices, and IoT sensors (soon expected to exceed 25 billion[1]), IT executives are challenged with providing secure connectivity for an increasing number of devices while protecting corporate assets and intellectual property.

Drawbacks of Existing Solutions

There are a number of solutions available to enable guest/employee/student access and onboarding of personal devices. These solutions are typically offered as hardware appliances hosted in the core of the network or integrated within a Wi-Fi controller. There are also solutions that provide complete network access control across wired and wireless access layers. All these solutions suffer serious drawbacks, namely:

- Current solutions are expensive and require dedicated hardware and software, which creates additional operational overhead for IT staff.
- Existing solutions are complex to administer and require deep technical knowledge of not just the access services but also the configuration of holistic infrastructure.
- Solutions in the market today are predominantly based on captive portals, which are cumbersome to manage and administer. Most IoT sensors are rather unsophisticated low cost devices that do not support web browsers and cannot use captive portals.
- Independent access solutions are often not integrated with IT infrastructure, requiring users to repeatedly provide user credentials to get on the Wi-Fi network as well as to access different applications.
- VPN based solutions are organization-specific, requiring VPN clients be installed on every mobile device and a gateway infrastructure within the organization to provide secure connectivity. It requires significant operational support to sustain both VPN infrastructure and VPN clients because of the myriad of mobile platforms and mobile operating systems.
- BYOD users complain that Wi-Fi access solutions are too complex for non-technical persons to maneuver through application downloads, agent installation, and configuration of certificates. It's not uncommon that solutions require 10-15 steps to achieve access. As a result, users often circumvent security by connecting to simpler open guest networks, thereby putting employers at risk.

[1] Gartner Press Release: http://www.gartner.com/newsroom/id/2905717

Impact on Businesses

Exposure from bypassing security

To ensure protection against corporate espionage or hacking, employee communications transmitted from personal devices must be encrypted and validated as an authorized user. The more complex the solution, the more likely it is that users bypass security constraints laid down by IT or avoid connecting altogether, which reduces productivity.

Increased IT workload

IT must support access and resolve issues related to personal devices and IoT sensors. Unlike company issued devices, which typically have standardized platforms, operating systems and applications, personal devices present varied hardware platforms and operating systems. Having IT create and manage the accounts and access rights to enable these devices can add significant operational workload to network administrators.

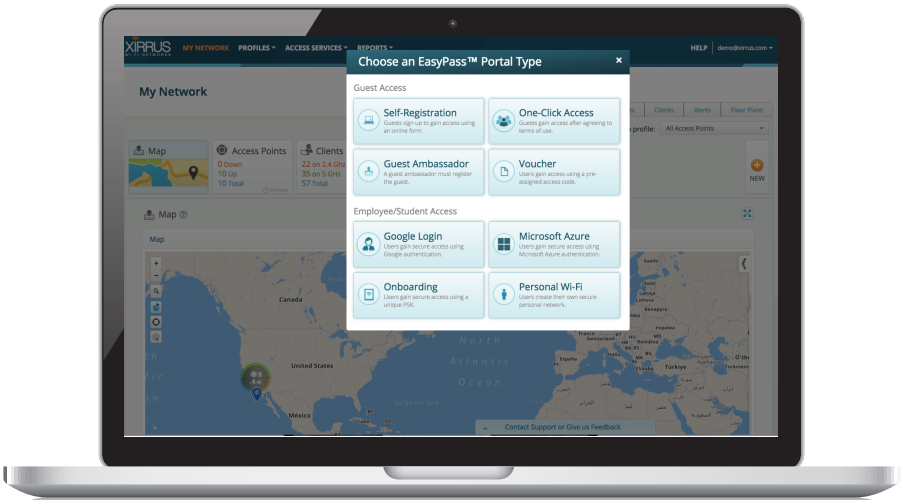
Loss of productivity

Access solutions have to be easy even for non-technical users. Many devices and sensors do not have a wired connectivity option making wireless access the only means of network connectivity. Therefore, Wi-Fi solutions must be robust and simple so businesses don't suffer productivity loss from employees who are unable to connect and access business critical information.

Xirrus...The Better Solution

Xirrus EasyPass

EasyPass Access solutions are cloud hosted Wi-Fi access services integrated with popular federated ID management systems such as Google Apps and Microsoft Azure . EasyPass is integrated with cloud and on-premise Xirrus Management System (XMS-Cloud, XMS-Enterprise) that provides IT a single dashboard to provision, manage, and control user and BYOD access



Capabilities and Benefits of EasyPass

Ease of Setup

Hosted in the cloud, IT staff can easily configure EasyPass and manage user privileges anywhere, anytime using a browser-enabled device. This solution provides IT administrators with the latest and greatest functionality immediately upon release of new software.

Simplicity of Administration

EasyPass does not require any changes to the local network infrastructure so IT staff can deploy services quickly and easily. With a few clicks, guest and BYOD access can be enabled across the entire network.

Control and Visibility

Access to the network is controlled. The account validation process can be integrated with sponsor workflows and user domains to ensure only authorized users are provided access.

Ease of Access

Simplified for even non-technical users, access to the network takes just a few clicks, and user experience can be highly customized with a consistent experience across any device and any operating system.

Simple Integration

EasyPass can be integrated with existing user databases and application systems such as Microsoft Office 365 (Azure), Google Apps for work and Google Apps for Education, as well as point of sale, property management systems, student directory services and ticketing systems.

24x7 Protection

Easily implement enterprise grade security for BYOD users while allowing users to onboard their own devices. Safeguard communications by creating protected personal Wi-Fi networks from public Wi-Fi.

Data Analytics

Information about guests can be exported into analytics systems to develop deeper visitor insights helpful to marketing and operations departments.

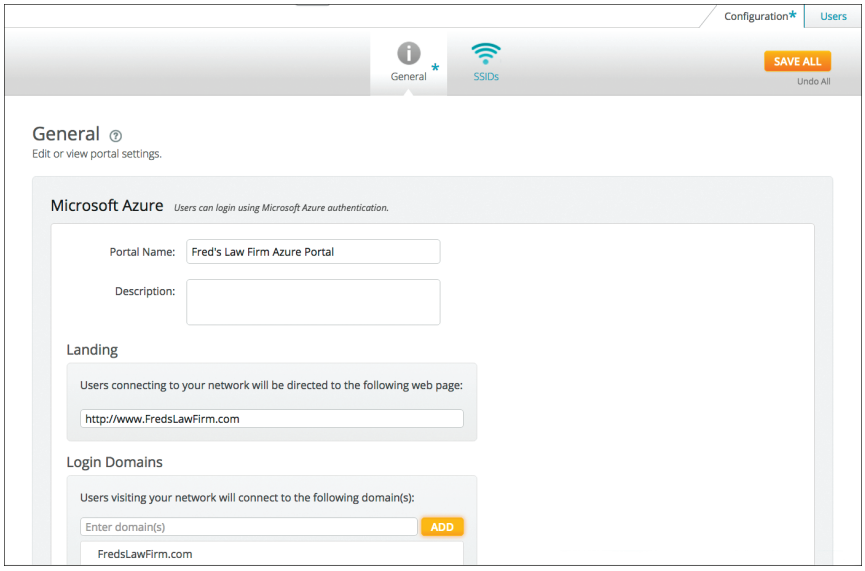
EasyPass Modules

EasyPass Access Service includes:

- EasyPass Microsoft Azure/Google Login – Single Sign-On with Microsoft or Google credentials to access Wi-Fi and and Microsoft Office 365 and Google Applications
- EasyPass Onboarding – self onboarding of BYOD devices without the use of captive portals
- EasyPass Self-Registration/Guest Ambassador – self registering or non-IT administered guest access
- EasyPass Voucher – voucher-based guest access with time control and restriction on number of guest devices
- EasyPass One-Click – Simple guest access with single click to accept usage terms and gain access
- EasyPass Personal – user-created secure personal Wi-Fi networks

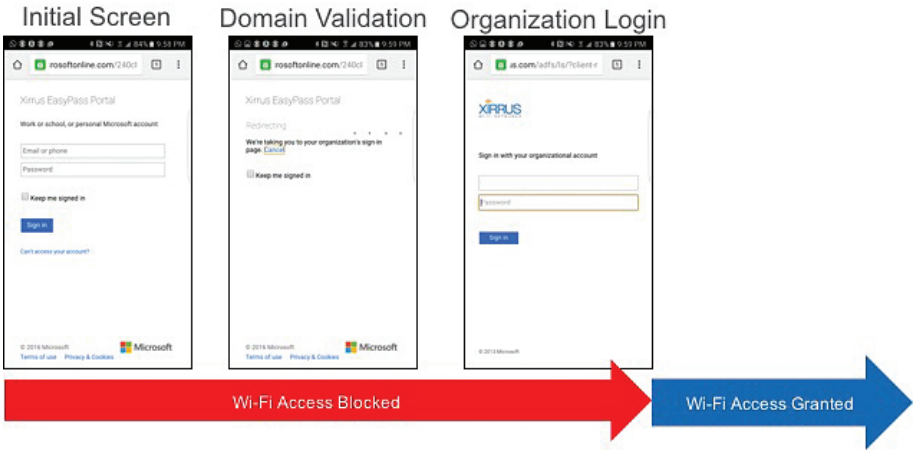
EasyPass Microsoft Azure/Google Login

With the integration to the Microsoft and Google application ecosystems, employees and students no longer need to use separate log in credentials to connect to the Wi-Fi network and gain access to domain resources. EasyPass simplifies access by integrating with popular federated ID management platforms such as Microsoft Azure and Google, eliminating the need for separate AAA systems, for example RADIUS servers, hosted on-premise.



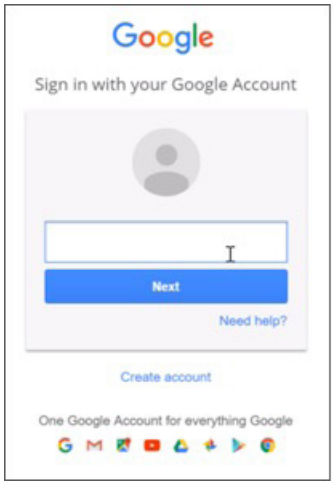
Single Sign-On (SSO)

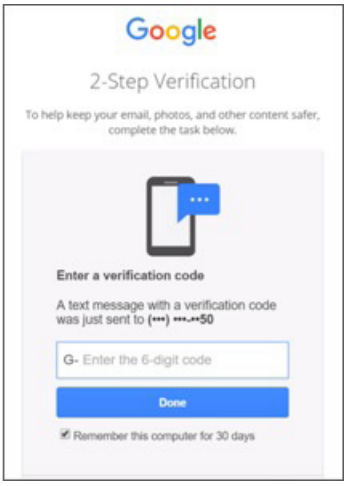
Administrators can simplify user access to the network and business application by integrating with federated ID management. Users can use their Microsoft Office 365 and Google Apps credentials to log into Wi-Fi (Single Sign-On) and access their applications



Secure Communication

Users are blocked from network access via Wi-Fi until authenticated against the Microsoft Azure or Google systems. By enabling encryption on the SSID with federated access, administrators can ensure protected data communication. A two factor authentication can also be enabled to provide a secondary level of use validation.





EasyPass Onboarding

More and more employees are bringing their own devices to the workplace to perform work functions. This, however, poses serious operational and security challenges for IT as this myriad of mobile devices utilizes a diverse set of operating systems. EasyPass Onboarding validates users and their devices before allowing restricted access to the network.

Validating a device and encrypting the communication between the device and the wireless access point requires a key. EasyPass Onboarding provides the security-equivalence of 802.1x while providing the simplicity of pre-shared keys, giving you the best of both worlds.

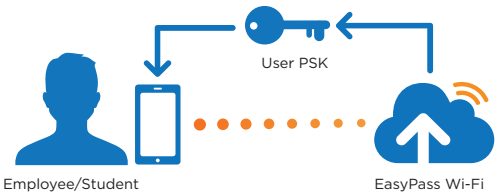
Pre-shared keys are simple to implement, but the drawback is that every user uses the same key. Implementing 802.1x automated key generation is safer but more complex for users to set up 802.1x on their personal devices, requiring support calls to IT. Most IoT devices do not support browsers and captive portal based onboarding is not an option. These devices need a solution that does not rely on captive portals and browsers to connect to the network yet provide the necessary protection for data communication.

Simplified Device Onboarding with User-Based Pre-Shared Keys

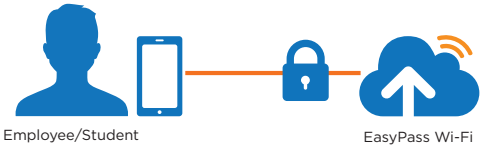
EasyPass Onboarding combines the benefits of both approaches — simplicity of the pre-shared key with security of the 802.1x authentication. Users can connect using their own User Pre-Shared Key (UPSK) to validate the device and establish an encrypted communication. With UPSK, network administrators can associate a user with a specific key. If a UPSK is compromised, the key can be individually revoked or regenerated without impacting all users.

Network administrators can also limit the number of devices per user with the use of UPSK and provide users the ability to manage their allocated number of devices without involving IT. Additionally, UPSK based onboarding eliminates captive portals and does not require a web browser, thereby enabling secure onboarding of headless IoT devices.

1. Obtain Personal Key



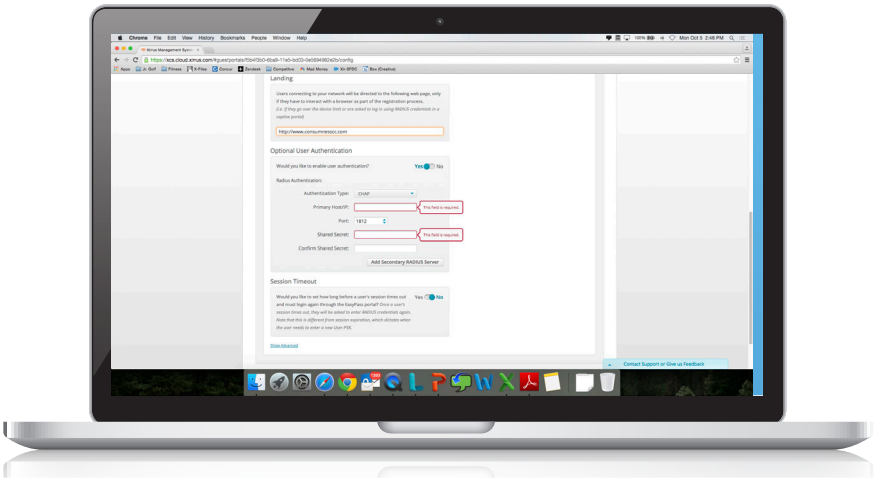
2. Access Secure Wi-Fi



UPSKs can be manually created or automatically generated in bulk by importing user information such as student ID, employee ID or a unique identifier via CSV format. These UPSKs can also be exported in a CSV file and integrated with other systems such as the employee HR system.

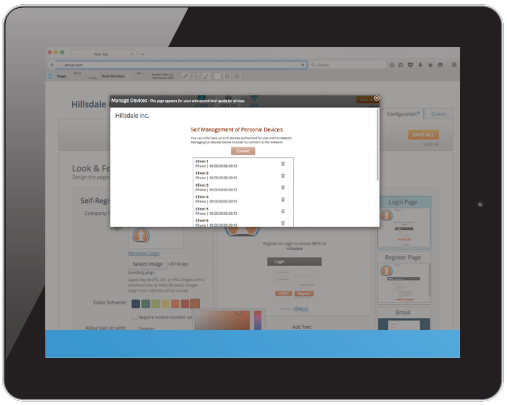
Two-Factor Authentication for Higher Level of Security

EasyPass is designed to implement two-factor authentication by integrating with domain user directory services such as Active Directory through a RADIUS server. Besides getting enhanced security, administrators can configure a session timer to control the duration of connectivity and force users to re- login to ensure devices are not compromised.



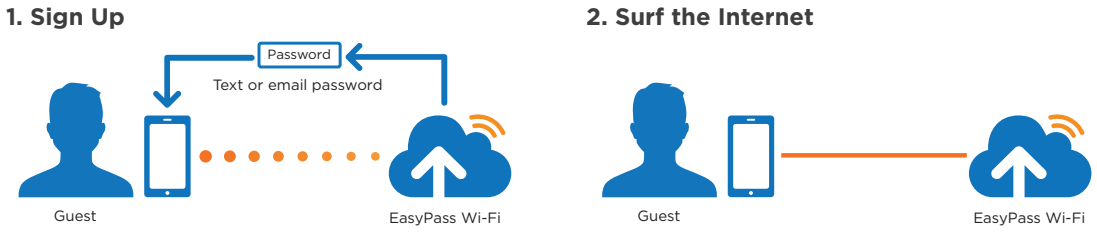
Limit Number of Personal Devices

Xirrus EasyPass Onboarding allows administrators to control the number of devices a user can onboard and issues a warning message when the user attempts to connect to the network with an excessive number of devices. The user can then delete some of their personal device accounts without involving IT.



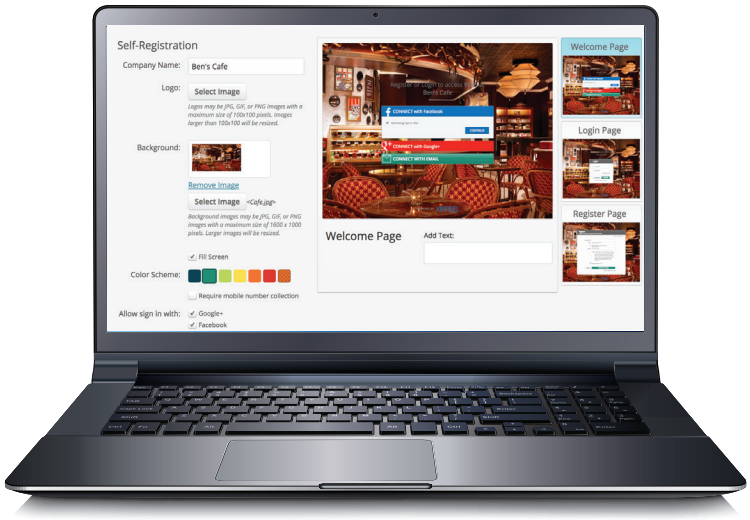
EasyPass Self-Registration/Guest Ambassador

These guest access modules validate users and allow them on to the network with controlled Internet-only access. Guests can self-register, use their social media credentials, or be approved by a sponsor to connect to the network. Visitor and guest demographic information can be accessed or exported for analytics and engagement. EasyPass guest modules allow streamlined IT operations through automated sponsor workflow and guest account management by non-IT staff such as receptionists. EasyPass is integrated with major telecom service provider SMS gateways and Twillio, a leading provider of cloud based SMS gateway to deliver guest credentials directly to the mobile devices.



Customizable Portal

EasyPass guest modules provide simple, customizable way to set up, administer and manage guest access. Users are presented with a portal page in their web browser from where they can choose how to access the network. Businesses can customize the portal to engage guests with rich, visually engaging branded experiences in localized languages.



Self-Registration

EasyPass Self-Registration provides IT organizations with finer controls to manage how long guest accounts remain valid before having to re-login to the network. Guests can self-register by entering their contact information or use social media credentials to get online, all without IT having to create individual guest accounts. Mobile number collection is also supported. Registration can also be integrated with sponsor workflow, allowing guest access to the network only after a sponsor within the company has approved the guest account request.

Guest Ambassadors

Guest accounts can be managed by non-IT staff who can create, delete or extend the validity of guest accounts without needing skills to configure the portal itself. This allows IT managers to streamline the account creation process without wasting time on administrative tasks.

Tracking and Visibility

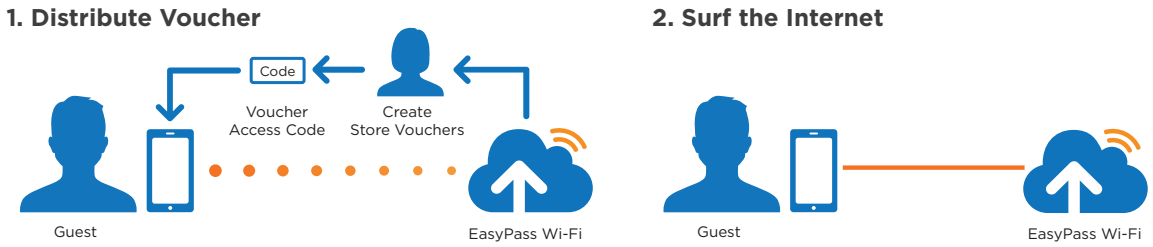
EasyPass guest modules provides complete visibility to IT with detailed information about guests including who's active on the network, duration of access, device MAC address and more.

Visitor Analytics

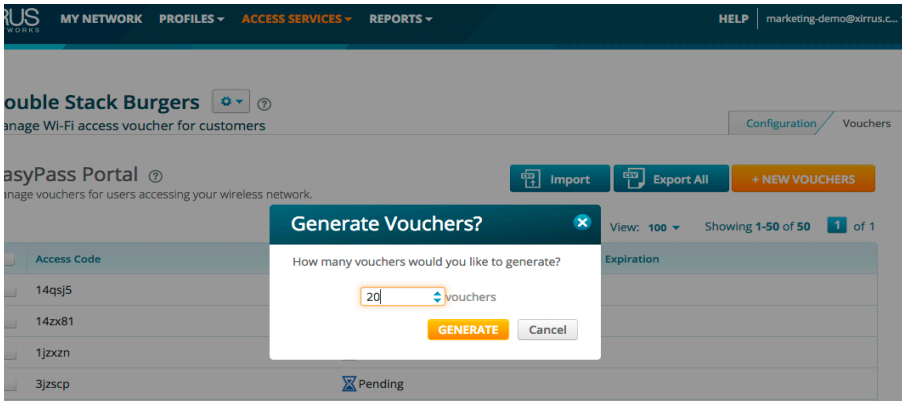
EasyPass can export demographic information when guests connect using social media credentials to gain insights about guests connecting to the network, such as their gender and age. Demographic information, along with contact data, can be exported from EasyPass to integrate into other analytics and visitor engagement engines.

EasyPass Voucher

EasyPass Voucher allows network administrators to create unique guest keys in bulk for retailers, hotels, conventions, and enterprises providing temporary visitor Wi-Fi access.



Administrators can select the number of guests who need keys and create a list of unique keys with the press of a button. These unique keys can be exported into a CSV file to integrate with other systems such as point of sale, property management, ticketing, or registration systems to name a few.

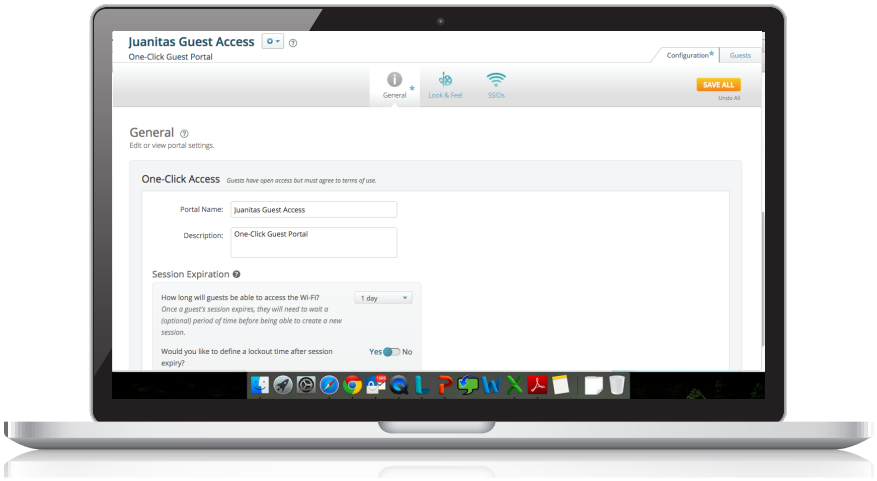


Limit Number of Personal Devices

EasyPass Voucher allows administrators to control the number of devices a guest can use with the same voucher code. The system issues a warning message when the guest attempts to connect to the network with more devices above the limit. The user can then delete some of their device accounts without involving IT.

EasyPass One-Click Access

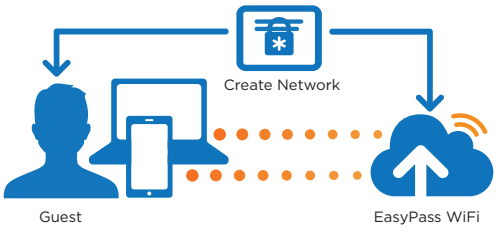
Often hotspot providers, need a simple guest access without asking for any guest information. These businesses want to ensure the users agree to acceptable use policies to mitigate any liability and business risk to the hotspot provider. EasyPass One-Click Access is just the right solution for such uses. The guest access provider can delivery all the rich brand experience with portal customization and provide a fast self-enabled access to the guests. EasyPass One-Click Access provides all the timing controls such as how long a guest can access the Wi-Fi before re-authenticating or allowing user to re-login only after a certain time has elapsed.



EasyPass Personal

EasyPass Personal enables users to dynamically create their own secure personal Wi-Fi over a public network. These personal networks can be created with the highest level of security and encryption, blocking hackers and other users of the public network from snooping on the communication. EasyPass Personal simplifies multi-device Wi-Fi connectivity by adapting to devices and does not require any configuration or changes on the mobile devices themselves. The dynamically created Wi-Fi can be active for different durations; for example, a student created personal network in a residence hall can be active for 9 months for the duration of the school year. Similarly, a business traveler created personal network in a hotel room can be active for the duration of the business stay. In the case of a patron in a café, the personal network can be active for a few hours while the patron enjoys a cup of coffee.

1. Setup Your Own Network

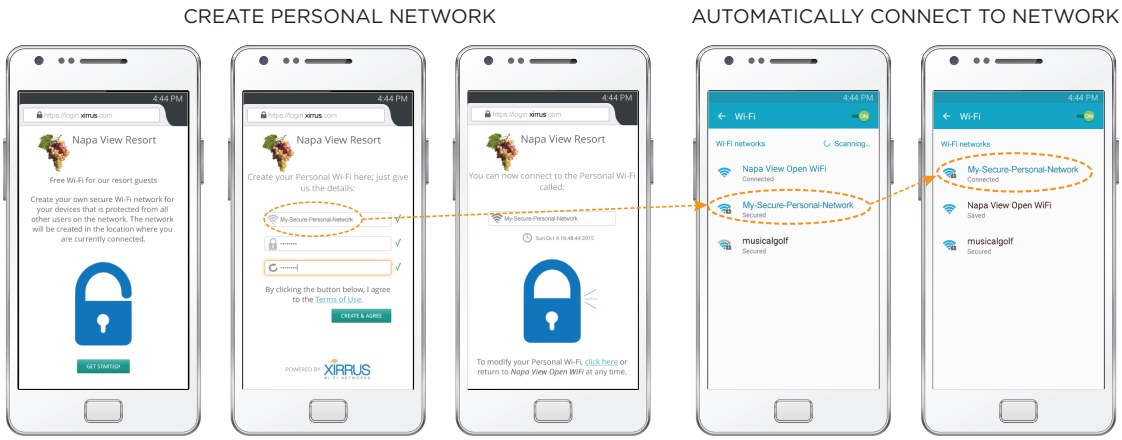


2. Access Your Secure Personal Network

Users connecting over public Wi-Fi in places such as hotels, dormitories, stadiums, coffee shops and conferences are exposed to security threats as the communication is unprotected and other users of the same public network can see the transmission. The ability to create a secure personal network from public Wi-Fi eliminates that risk.

Dynamically Create Protected Wi-Fi

EasyPass Personal allows users to dynamically create their own personal network with encryption protecting all communication. Users can implement military grade security using the highest level of encryption available in the industry. Other devices and users on the same public network are then prevented from seeing the interactions on the newly created personal protected Wi-Fi network.

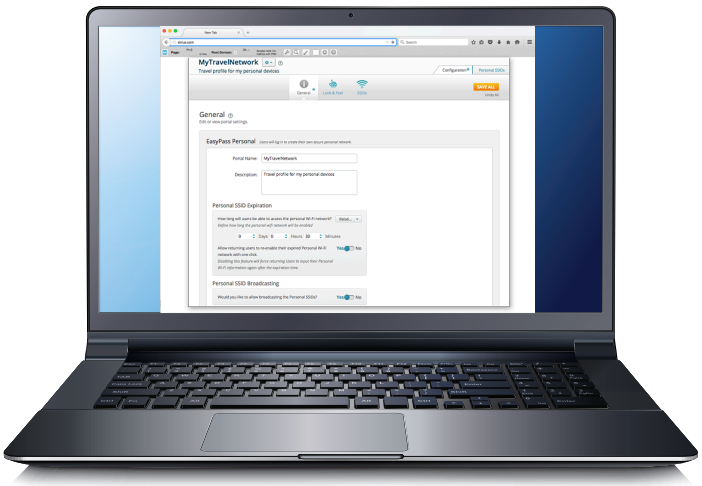


Personal Network On The Go

All personal devices can connect to the personal Wi-Fi without any device configuration. User created personal networks allows peer-to-peer communication among all personal devices having access credentials. That means, next time you're on vacation at a hotel with EasyPass enabled Xirrus Wi-Fi you can dynamically create a personal "home" network and all of your devices—laptop, tablets, iPods, smartphones, Xbox and more—can join the "home" network over the hotel network without reconfiguring devices or having to call the hotel clerk to ask for a Wi-Fi password. Xirrus EasyPass Personal allows you to take your personal "home" network with you wherever you go.

Complete Control

IT staff has complete control over how long user created networks may exist before expiring. Plus, they can allow users to re-enable an expired personal network without IT involvement. Businesses can promote user brand interaction by customizing the portal for personal Wi-Fi creation, and information obtained from user created personal networks can be exported into a CSV file for audit trails and tracking.



Conclusion

Xirrus EasyPass provides a simple suite of access solutions to administer, SSO access for employees and students, secure onboarding of headless IoT, and different types of guest access. The solution provides complete visibility to network administrators with detailed information about users and devices accessing the network, and offers multiple levels of controls to manage without additional operational overhead.

The following table summarizes the features of the EasyPass modules:

Functionality	Description	Employee/Students			Guests				
		Microsoft Azure	Google	Onboarding	Self-Registration	Guest Ambassador	Voucher	One-Click Access	Personal
Single Sign On	Access Wi-Fi and applications with same credentials	✔	✔						
Two Factor Authentication	Secondary level authentication to validate authorized user		✔	✔					
Social Integration	Login with Facebook, Google+ and pull user profile				✔				
Self-Provisioned	Users can register unassisted to gain access				✔			✔	✔
Non IT Provisioned	Receptionist or Guest Ambassador created guest access					✔	✔		
Captive Portal	Customizable web splash page and T's & C's			opt.	✔	✔	✔	✔	✔
Access Policies	Security policies centrally defined, globally enforced	✔	✔	✔	✔	✔	✔	✔	✔
Bulk Creation	Create users from imported lists, export user lists			✔			✔		
802.1x Support	Optional authentication to enterprise user directory			opt.					
Headless Devices	Connect devices with no browser interface			✔					✔
Device Limits	Control maximum number of devices per user			✔			✔		
Dynamic Wi-Fi	Wi-Fi networks created/deleted on demand								✔
Network Isolation	Create Wi-Fi networks isolated from other users								✔

EasyPass is a fully hosted service included with Xirrus Management System-Cloud and available as an add-on to the on-premise Xirrus Management System-Enterprise platform.

Global Headquarters
3800 Golf Road, Suite 360
Rolling Meadows, IL 60008
USA
Tel: +1 (888)863-5250

UK Office
Unit B2, Linhay Business Park,
Eastern Road
Ashburton, United Kingdom,
TQ13 7UP
Tel: +44 1364 655500

San Jose Office
2590 N. 1st Street, Suite 220
San Jose, CA 95131 USA

Cambium Networks Consulting Private Ltd
5th Floor, Quadrant 1, Umiya Business Bay
Tower 2,Outer Ring Road
Kadubisenahalli, Varthur Hobli Road
Bangalore East Taluk, Bangalore- 560037