Aerohive Private PSK

Table of Contents

Introduction

Wireless networking has gone through several evolutionary steps to equal – and in some cases, exceed – the security found in wired networks. The first step in this evolution was the development of preshared keys, or PSK. Each device in a network uses a preshared key to encrypt traffic, thus providing additional security. The disadvantages of classic PSK include the fact that it is impossible revoke the network-wide key should an individual leave the organization, as well as the fact that it is relatively easy to crack. Today, the clear choice in authentication for enterprises that are deploying or upgrading wireless networks is 802.1X. However, moving from PSK to 802.1X can prove to be challenging, as some devices do not support 802.1X or are cumbersome to set up. This can lead to the choice between the purchase of new equipment or a compromise in security. 802.1X also faces challenges when used to secure devices not owned by the enterprise, such as those of guests, students, subcontractors or the like. Because 802.1X requires the installation of a software client, it is difficult or impossible to use on such unmanaged devices.

Aerohive's patent-pending Private PSK provides the ease of PSK with many of the advantages of 802.1X solutions. The IT manager can provide unique passphrases to each user on a single SSID, which creates a one-to-one relationship between the key and user instead of the one-to-many paradigm of classic PSK, thus providing the ability to truly authenticate each individual. This enables 802.1X-like capabilities even though it appears like only a PSK is required on the laptop or Wi-Fi device. While classic PSK does not allow the revocation of a single user's credentials since all users share the same passphrase, Private PSK offers a unique PSK per individual and therefore enables the administrator to revoke a single set of credentials. Furthermore, since Private PSK, like 802.1X, allows a means to identify individual, users on a single SSID, each can be granted different user profiles. This allows all users to connect to the same network, but get unique levels of service based on their roles.

Benefits
- Simple key creation, distribution and revocation saves administrator time and reduces the cost and complexity of using a single PSK or trying to get hard-to-configure devices online using 802.1X
- Guests can be given unique keys, thereby eliminating the risk of one guest eavesdropping on another. In addition, entering a PSK is often simpler than loading up a captive web-portal and entering a username and password
- If a person leaves the company, classic PSK requires that the key be reset for all users, which can be an IT support burden. With Private PSK, just that one user's key can be revoked
- Many clients do not support 802.1X or the latest WPA2 standard with opportunistic key caching required for fast roaming between APs. With Private PSK, those clients can see significant performance increases with roaming
- Many legacy clients don't support 802.1X but most will support WPA-PSK. Those clients can be made secure without a costly client and application upgrade

Overview of Common Methods for Wi-Fi Access

When implementing a wireless LAN, organizations must chose a means by which users prove that they are who they say that they are. This choice often involves a compromise between complexity and security. The three most common methods for new deployments are:

- Open Authentication – No Wi-Fi security
    - All traffic is sent in the clear
    - May use captive web portal for self registration or authenticated access
    - May segment traffic to specific VLAN or network

- Preshared Key – IEEE 802.11i WPA or WPA2 Personal
    - Uses a single secret key that is shared among all clients and APs for an SSID
    - The shared key is used for encrypting traffic between the clients and APs with TKIP or AES-CCMP

- IEEE 802.1X (EAPOL) – IEEE 802.11i WPA or WPA2 Enterprise
    - Authenticates users and, optionally, their client devices, based on user credentials and machine certificates.
    - The keys used by client and AP are securely and dynamically negotiated with the RADIUS server using 802.1X (EAPOL)
    - The APs and clients use the key to generate secure temporary keys for each session with RADIUS.
    - Traffic is encrypted with TKIP or AES-CCMP.

SSIDs with open authentication are the easiest to configure, and as a result, many enterprise guest networks are set up using this method. There are significant problems with this configuration, however, especially with security. All traffic to and from clients is sent in the clear, and there is no control as to who associates with the open SSID. Many Wi-Fi capable devices may even connect automatically, without a user even being aware of it. This leaves the wireless device open for attack, and can place an extra burden on the Wi-Fi infrastructure.

SSIDs with preshared keys have several advantages over open authentication. In addition to being more secure, they are easy to set up, are widely supported by clients, and do not require authentication servers, certificates, or extra configurations on the clients. Despite these benefits, however, the fact that all users on the same SSID must use the same key creates a number of problems. If one user leaves the organization or loses their wireless client, the preshared keys on the access points and all clients must be changed to protect the wireless LAN from unauthorized access. Also, all users on the SSID must belong to the same user profile and, therefore, share the same QoS rate control and queuing policy, VLAN, tunnel policy, firewall policies, and schedules. It is not possible to provide different network policies to different users on the same SSID when applying PSK-based authentication.

SSIDs that use IEEE 802.1X authentication solve the shortcomings of PSKs by providing a unique key to each individual user. After a user authenticates against a RADIUS server, the server sends the access point and client a unique PMK (pairwise master key) from

which they generate PTKs (pairwise transient keys) to use during their session. The RADIUS server can also return attributes to identify different user profiles. With this approach, 802.1X authentication overcomes problems inherent in the classic PSK solution by allowing multiple user profiles per SSID based on individual authentication. This also provides the ability to invalidate users or machines when a user leaves or their machine has been lost, stolen, or compromised. However, 802.1X requires a more involved setup, including a RADIUS server, server certificates, and a user database stored either on the RADIUS server or on an Active Directory or LDAP server with which the RADIUS server communicates. In addition, the clients, or RADIUS supplicants, require additional configuration to support 802.1X.

Wi-Fi Access using Aerohive Private PSK

Though using IEEE 802.1X is the most secure approach to Wi-Fi authentication, this method is typically only implemented for devices managed by IT staffs, where they have control over the domain infrastructure, user accounts, and wireless clients being used. For temporary users such as contractors, students, or guests, the IT staff may not have the access rights required, the knowledge to configure 802.1X clients for all the different wireless devices involved, or even the time to perform such tasks. Even more difficult is the fact that many legacy wireless devices do not support 802.1X or the latest WPA2 standard with opportunistic key caching required for fast roaming between APs. The next best option has traditionally been to use a preshared key for these devices. As we've discussed earlier, however, classic PSK trades off many of the advantages of 802.1X such as the ability to revoke keys for wireless devices if they are lost, stolen or compromised, and the extra security of having unique keys per user or client device.

To draw on the strengths of both preshared key and IEEE 802.1X mechanisms without incurring the significant shortcomings of either, Aerohive has introduced a new approach to WLAN authentication: Private PSKs. Private PSKs are unique preshared keys created for individual users on the same SSID. They offer the key uniqueness and policy flexibility that 802.1X provides with the simplicity of preshared keys.

The following diagram is a simple example showing a WLAN with traditional preshared keys versus that of a WLAN using Aerohive's Private PSK functionality. With the traditional approach, all the client devices use the same preshared key, and all recieve the same access rights because the clients cannot be distinguished from one another.

Figure 1: SSID with Preshared Key vs. SSID with Private PSK
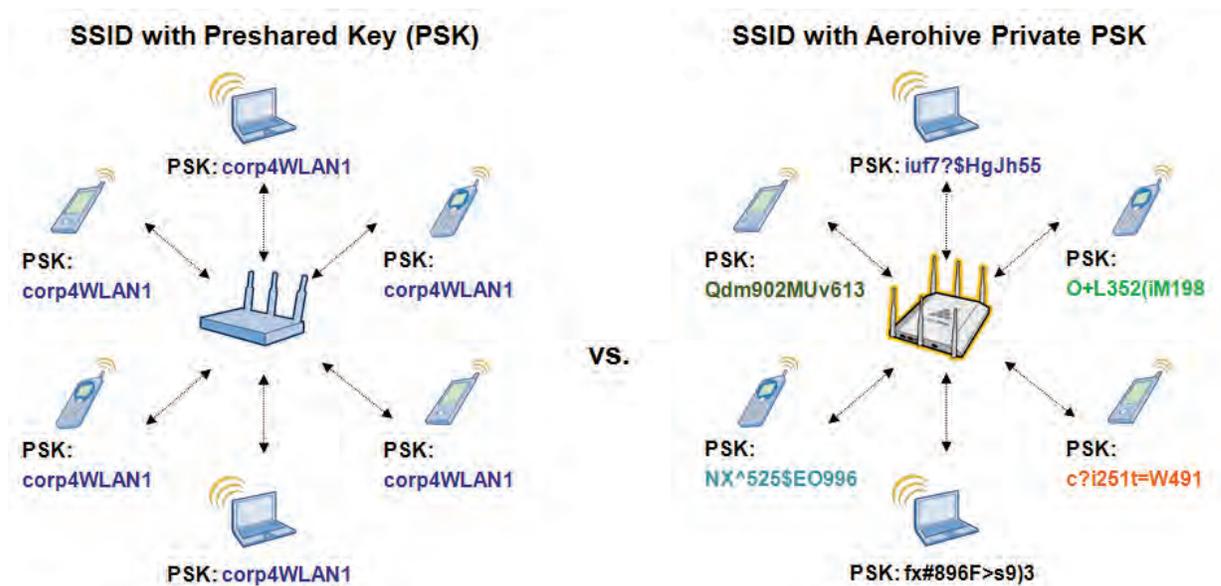
On the other hand, with private PSK, as shown on the right, every user is assigned their own unique or "private" PSK which can be manually created or automatically generated by HiveManager and then sent to the user via email, printout, or SMS. Every

private PSK can also be used to identify the user's access policy including their VLAN, firewall policy, QoS policy, tunnel policy, access schedule and key validity period. Because the keys are unique, no key from one user can be used to derive keys for other users. Furthermore, if a device is lost, stolen, or compromised, the individual user's key can be revoked from the network, preventing unauthorized access from any wireless device using that key. As for the client users, the configuration is the same as using a standard preshared key.

Wireless LAN Requirements & Features	PSK - WPA/WPA2 Personal	Private PSK - WPA/WPA2 Personal	IEEE802.1X - WPA/WPA2 Enterprise
No complex configuration required for clients	✓	✓	✗
Unique Keys Per User On Single SSID	✗	✓	✓
Can revoke an individual user's key or credentials when they leave the company or their wireless device is compromised, lost or stolen	✗	✓	✓
Supports different VLAN, QoS, Firewall or Tunnel policy for different users on same SSID	✗	✓	✓
Does not require clients to support opportunistic key caching for fast roaming	✓	✓	✗
Does not require certificates to be installed on clients	✓	✓	**Depends on Client**
Uses 802.11i standard mechanisms for securing the SSID	✓	✓	✓
Keys are dynamically created for users upon login to the network and are rotated frequently	✗	✗	✓
Can be used to perform machine authentication	✗	✗	✓
If one user is compromised, no other users keys can be compromised	✗	✓	✓

Private PSK Deployments Using HiveManager

Whether or not devices are managed by the corporate infrastructure, the configuration of Private PSK can be greatly simplified using HiveManager. HiveManager is used to configure the WLAN policy, which defines the configuration for HiveAPs including the SSIDs. Diagram 2 shows a WLAN policy that is used to establish a Private PSK - SSID on HiveAPs. In this case, HiveManager is then used to automatically generate a Private PSK user database for corporate devices that are unmanaged, such as smart phones, and a set of Private PSK users for guests. Each Private PSK user has its own preshared key and is assigned to a group from which its policy is inherited.

In **step 1**, the administrator configures the Private PSK SSID and creates the user database which is pushed to the HiveAPs. These users can be manually configured, automatically generated or loaded into the HiveManager using a .csv file, such as an export file from Active Directory.

Figure 2: HiveManager Configuration and Private PSK Generation and Distribution
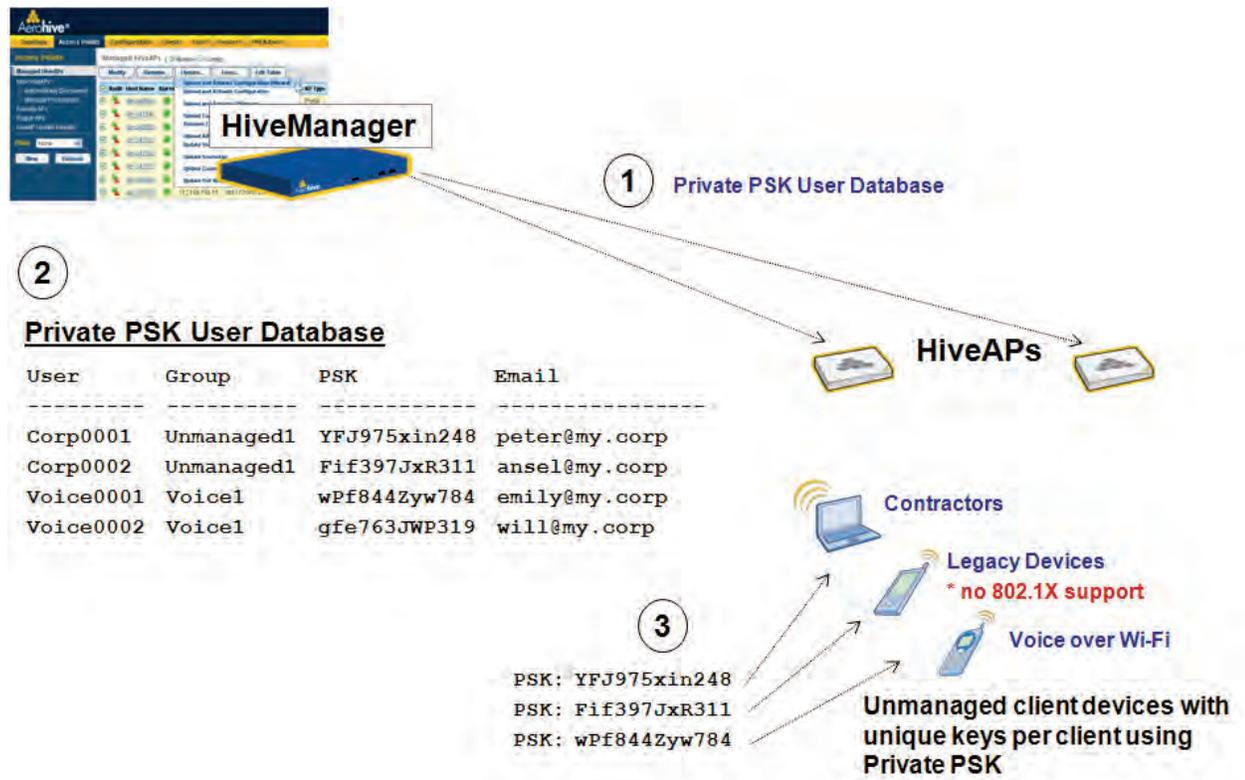
In **step 2**, the administrator can click a button in HiveManager to email the individual private PSKs to selected users. This is demonstrated in Figure 3. When the user receives the email, they can use their unique PSK to connect to the wireless network.

Figure 3: Emailing Private PSKs to Users

In **step 3** the clients, loaded with their unique keys can access the network and be assigned their unique policy.

Figure 4: Revoking Private PSKs

If a person leaves the company or loses their key, the key can be revoked as is shown in **Figure 4**. By simply selecting Private PSK users, clicking remove and updating the user database on HiveAPs, the keys can be removed from wireless LAN preventing access from any device using these keys.

Securing Guest Access with GuestManager and Private PSK

Using GuestManager's Private PSK implementation, a lobby administrator can use a simple web-based interface to allocate guests their own Private PSKs that can be time limited and revoked if necessary. Using GuestManager with Private PSK, you get the additional benefits of a:
- Simplified web interface used to allocate Private PSKs to guests
- Customizable print templates that can be used by lobby administrators to print account keys and logon instructions for guests
- Guest revocation using RADIUS Dynamic Change of Authorization Messages (RFC 3576) that does not require updating the user database on HiveAPs
- RADIUS accounting.

An example of how GuestManager operates with Private PSK is demonstrated in the steps displayed in **figure 5**.

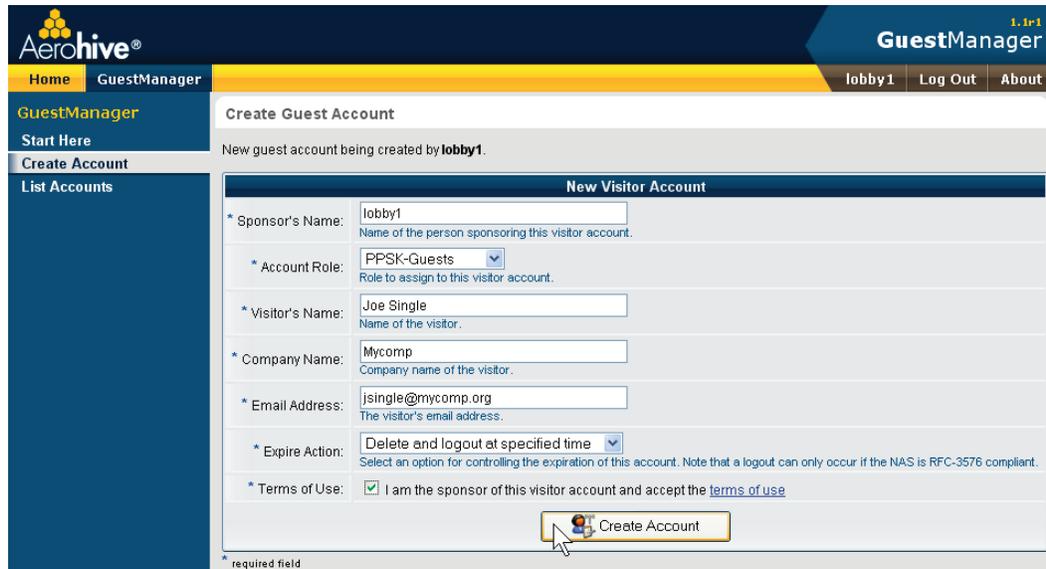**Figure 5: GuestManager Operation with Private PSK**
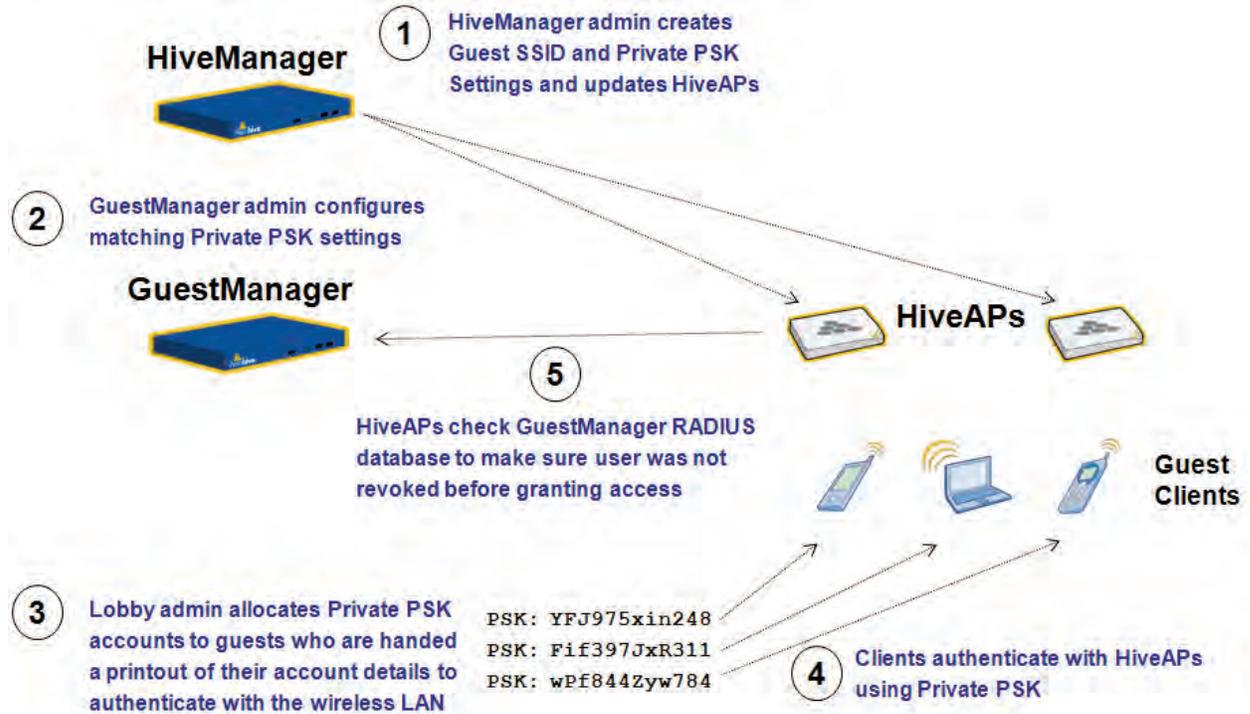
1. The administrator creates the necessary WLAN policy configuration which includes the SSID, user profile, and Private PSK configuration in HiveManager. The Private PSK configuration parameters include a key regeneration timeframe, secret key, location, and an option to validate keys with GuestManager. The administrator can create up to 1000 private PSKs for a location. Once HiveAPs are updated, based on the key regeneration time, the HiveAPs will generate keys for the Private PSKs.

2. To allow the delegation of control and distribution of Private PSKs, the administrator then configures the same Private PSK parameters into the GuestManager. This enables GuestManager to generate the exact same PSKs that are generated on

HiveAPs, including the same key regeneration times. However, the control as to whom the Private PSKs are given, and when the PSKs are active can now be given to a delegated administrator such as a lobby administrator, without the need for them to touch the configuration of HiveAPs.

3. As guests arrive, the lobby administrator with limited web access can create a guest Private PSK user account (**Figure 6**). Once created, the lobby administrator clicks a button to print login credentials and instructions for the guest.

Figure 6: Lobby Administrator Creates Guest Account

4. Guest users authenticate their client devices to the guest SSID using their unique Private PSK.

5. HiveAPs validate the Private PSK with GuestManager using the Private PSK as a user account to ensure the account is still active. If permitted, GuestManager will send an access accept to the HiveAP to permit the user to login to the wireless LAN. GuestManager can also be configured to return RADIUS attributes to assign the user profile assigned to the user.

By combining the steps of using the Private PSKs for encryption, and for validating the user with RADIUS, this method ensures that only valid guests will be able to securely access the network. If the lobby administrator revokes the guest user from GuestManager, GuestManager will send a RADIUS change of authorization message to the HiveAP which flushes the user's authentication cache from all APs in the Hive, forcing the client to reauthenticate. However, if the user has been revoked, the RADIUS authentication will fail and the user will not be granted access to the wireless LAN.

Summary

Today, 802.1X is regarded as the gold standard for Wi-Fi security and authentication by industry analysts, vendors, and enterprise IT managers. Unfortunately, the wholesale migration to 802.1X is inhibited by the cost of upgrading legacy clients, the deployment complexity of 802.1X, and the inability of guest networks to work with it. Aerohive's Private PSK addresses the security and management challenges of legacy clients, mobile devices, and guests that cannot be moved to 802.1X, allowing enterprises to use 802.1X where they can and Private PSK everywhere else. This dramatically improves Wi-Fi security and manageability while it reduces wireless LAN deployment and operating costs.

About Aerohive

 Aerohive Networks reduces the cost and complexity of today's networks with cloud-enabled, distributed Wi-Fi and routing solutions for enterprises and medium sized companies including branch offices and teleworkers. Aerohive's award-winning cooperative control Wi-Fi architecture, public or private cloud-enabled network management, routing and VPN solutions eliminate costly controllers and single points of failure. This gives its customers mission critical reliability with granular security and policy enforcement and the ability to start small and expand without limitations. Aerohive was founded in 2006 and is headquartered in Sunnyvale, Calif. The company's investors include Kleiner Perkins Caufield & Byers, Lightspeed Venture Partners, Northern Light Venture Capital and New Enterprise Associates, Inc. (NEA).

Corporate Headquarters
Aerohive Networks, Inc.
330 Gibraltar Drive
Sunnyvale, California 94089 USA
Phone: 408.510.6100
Toll Free: 1.866.918.9918
Fax: 408.510.6199
info@aerohive.com
www.aerohive.com

EMEA Headquarters
Aerohive Networks Europe LTD
Sequel House
The Hart
Surrey, UK GU9 7HW
+44 (0)1252 736590
Fax: +44 (0)1252 711901

SB0900506