

Aerohive PPSK Guide



This guide explains the difference between PPSK (Private Pre-Shared Key) user types, their creation, and the distribution of PPSK passwords. Aerohive provides two types of PPSK users: cloud and local. Cloud PPSK users are stored in one central location in the cloud while local PPSK users are stored locally on all APs serving SSIDs that use PPSKs for user authentication.

The creation of PPSK users can vary widely depending upon who creates them: HiveManager NG administrators, guest management administrators, and company employees. They can create PPSK users either through the PPSK user creation tool in the HiveManager NG GUI or through a separate web app. Finally, network users can self-register and obtain PPSK passwords for themselves through a captive web portal, the iPad Kiosk App (a free app available for download from the Apple App Store), or the Guest Management Web Application in kiosk mode.

In addition to multiple methods for creating PPSK users, there are multiple methods for distributing PPSK passwords. They can be sent by email or SMS text message, or they can be printed and handed out.

Document Revision History

Revision	Date	Notes
01	1/18/2017	Initial version
02	1/26/2017	Added notes about cloud PPSK user group settings and revised contact instructions for those interested in the Guest Management reference app
03	2/3/2017	Revised the introduction to the device PPSK section
04	3/3/2018	Updated content to reflect changes in the HiveManager NG GUI

Contents

Introduction.....	3
Cloud PPSK.....	3
Creating a Cloud PPSK SSID	6
Creating a Cloud PPSK User Group	7
Creating Cloud PPSK Users	10
HiveManager NG Administrators.....	10
Guest Management Administrators.....	13
Employees or Guests (Guest Management Web Application).....	16
Self-Registering through a Captive Web Portal	20
Self-Registering with the iPad Kiosk App	24
Defending against DoS Attacks.....	25
Deleting Cloud PPSK Users	25
Local PPSK.....	26
Creating a Local PPSK SSID	27

Introduction

For an SSID using standard PSK, all users and devices share the same key (password or passphrase). If a user leaves or a device is lost or compromised, you must change the shared key for security reasons and reconfigure every AP and client device with the new key. In addition, all users and devices must share the same user profile, which assigns them to the same VLAN and applies the same firewall policy, QoS policy, schedule, and SLA. In contrast, for an SSID using PPSK, every user and device has a unique key. If a user leaves or a device is lost or compromised, you only need to delete or change the key for that user or device. Additionally, you can assign multiple user profiles to different PPSK user groups within the same SSID. The advantages of PPSK can be achieved through 802.1X/EAP authentication. However, PPSKs do not need PKI, certificates, or RADIUS servers, making them simpler to deploy.

Aerohive provides a choice of two types of PPSK (Private Pre-Shared Key) users: cloud PPSK users and local PPSK users. The key difference between the two types is where they are stored. Cloud PPSK users are stored in Aerohive-hosted servers within the HiveManager NG cloud platform or—for an on-premises solution—within the HiveManager NG virtual appliance. Local PPSK users are stored locally on Aerohive APs.

Each PPSK user type serves a purpose and offers different benefits. This guide examines each type and explains how they work and how to use them.

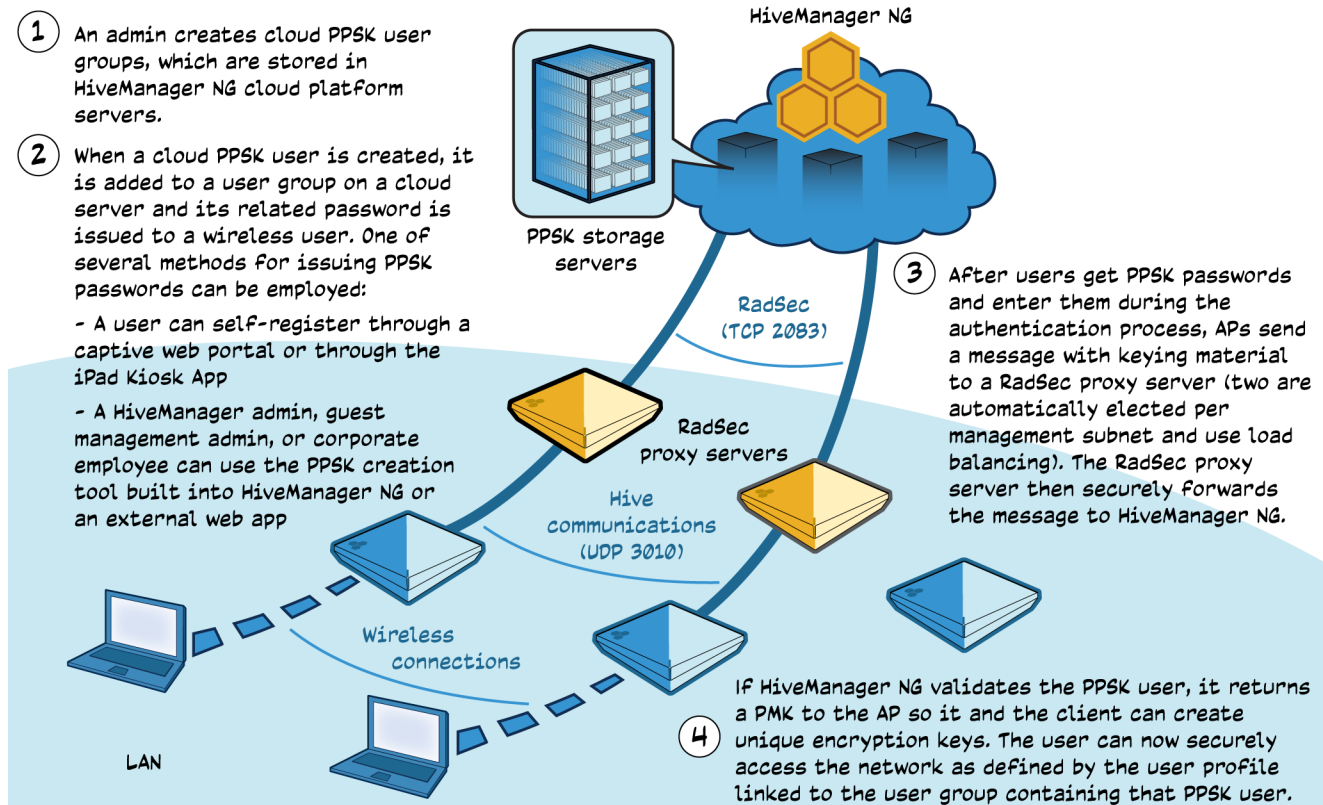
Cloud PPSK

Key Points: This section explains what cloud PPSK users are, who can create them, and how.

Cloud PPSK provides a flexible and scalable approach to PPSK user management. An admin creates PPSK user groups that are stored in the cloud. Then HiveManager NG administrators, guest management administrators, employees, and even network users themselves create PPSK users that HiveManager NG adds to those groups and maintains within PPSK-to-MAC address binding tables. Each HiveManager NG account can hold up to approximately 20,000 cloud PPSK users.

Storing PPSK users in a central repository in the cloud instead of on APs themselves provide numerous advantages:

- Because of increased computational resources on HiveManager NG cloud servers, the Aerohive Cloud Services platform can support many more PPSK users than an AP can.
- People can use PPSKs at multiple sites that advertise the same SSID. To accomplish this with local PPSKs, every AP at each site would need to store the same set. However, because cloud PPSK users are stored in a central location and can be accessed from anywhere that permits outbound traffic on TCP port 2083 to the Internet, people can use them anywhere that links an SSID to the same PPSK user group.
- People can self-register for their own PPSK through a captive web portal, the iPad Kiosk app, and the Guest Management Web Application (in kiosk mode). Captive web portals and the Guest Management Web Application can additionally require employee or manager approval before HiveManager NG sends PPSK passwords to self-registered users.
- Creating, modifying, and deleting cloud PPSK users and user groups do not require any AP updates.



RadSec Proxy Server Election Process

RadSec is a protocol that provides a means to secure RADIUS communications over untrusted networks, and a RadSec proxy server is an AP that relays RADIUS communications from hive members in the same management subnet to HiveManager NG over RadSec on TCP port 2083. Each management subnet has two RadSec proxy servers, which use load balancing to distribute work between themselves. To determine which two APs will be RadSec proxy servers, the DA (designated AP)—a sort of information hub and decision-maker for all hive members on the same management subnet—adds up the following scores and chooses the two with the best total:

- The hive member can make a RadSec connection to HiveManager NG on TCP port 2083: +51 points
- The hive member is a portal: +25 points
- The current CPU on the hive member is the lowest of all candidates: +8 points
- The hive member has the greatest percent of free memory in relation to total memory: +10 points
- The hive member is not a DA: +6 points

Note: If a hive member is a BR100, it is excluded from selection.

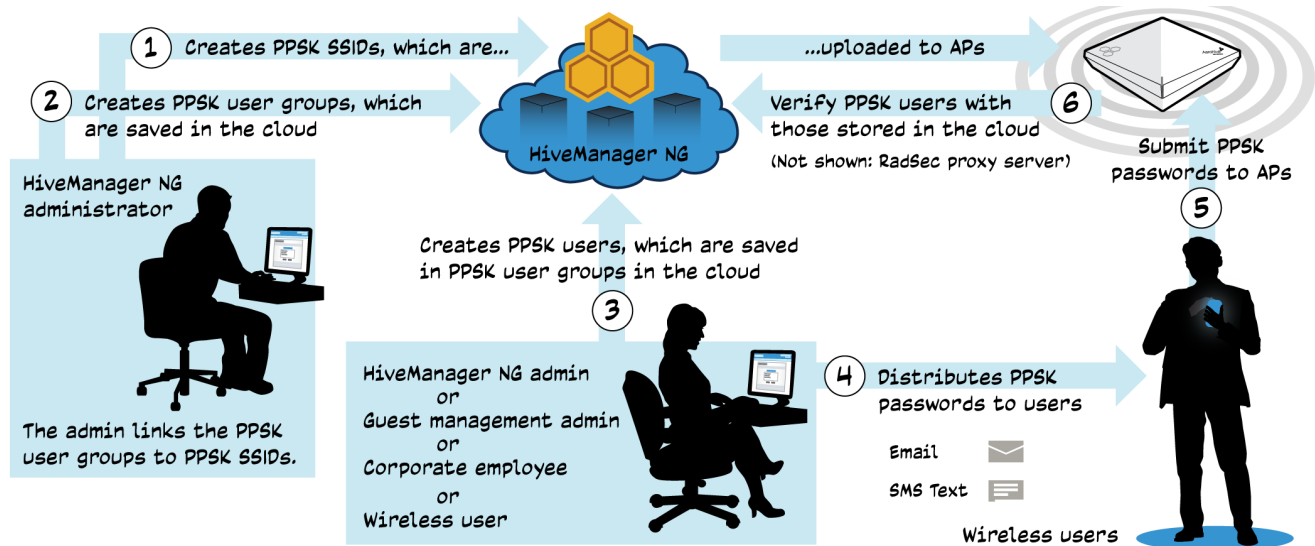
After the DA selects two RadSec proxy servers, it waits 30 minutes and calculates their scores again. If another AP has a score that is more than 15 points higher than one of the current RadSec proxy servers, it takes its place. For example, if the scores for two RadSec proxy servers are 80 and 81 and another AP gets a score of 96, then this AP will take the place of the AP with a score of 80 ($96 - 80 > 15$). If an AP gets a score that is more than 15 points higher than those of both current RadSec proxy servers, it takes the place of the one with the lower score.

Setup and Authentication Process

Setting up user authentication with cloud PPSKs involves four steps:

1. Creating a PPSK SSID
2. Creating one or more PPSK user groups
3. Creating and adding PPSK users to a group
4. Distributing PPSK passwords to individual users

A HiveManager NG admin must create PPSK SSIDs and user groups. The HiveManager NG admin can also add users to groups and distribute PPSK passwords. Additionally, to ease the administrative burden on HiveManager NG administrators, guest management administrators, employees, and users themselves (self-registration) can create PPSK users, add them to a group, and distribute their passwords.



After users have their own PPSK passwords, they use them when associating and authenticating with an AP. APs send keying material to a RadSec proxy server that in turn sends it to HiveManager NG. Once HiveManager NG validates a PPSK user, it sends the AP with which that client is associated a PMK (pairwise master key). Using the PMK, the AP derives a unique PTK (pairwise transient key) for encrypting/decrypting unicast data traffic. The client derives the same PMK and PTK. The AP keeps the PMK in its roaming cache and shares it with nearby APs in case the client roams to them.

The AP with which the client is associated and each hive neighbor with which that AP shares its roaming cache entries immediately start a timer that counts down in 60-second intervals. If the client is still associated at the end of an interval, the AP restarts its timer and informs its neighbors that the client is still connected in its next roaming cache update, which occurs every 60 seconds by default. The neighbors then restart their timers too. If the client session ends, they all keep the PMK in their caches in case it returns, and they continue counting down for sixty 60-second intervals. If the client returns within the hour, the client and any of the APs can use their cached PMK. If the client does not return, they remove the PMK from their caches. The next time the client connects, the AP to which it associates must repeat the process, contacting HiveManager NG again to get a new PMK.

The interval and timeout are configurable: `roaming cache update-interval <number1> ageout <number2>`, where `<number1>` can be from 10 to 36000 seconds (default: 60) and `<number2>` can be 1-1000 (default: 60). Multiplying them together determines when a PMK expires. By default: 60 seconds x 60 = 3600 seconds or 1 hour.

Creating a Cloud PPSK SSID

Key Points: A HiveManager admin creates SSIDs requiring users to submit unique PPSK passwords.

You can create a single SSID that requires users to submit PPSK passwords created by someone else and delivered to them separately, or you can create a pair of SSIDs: an open self-registration SSID through which users acquire a PPSK password, and an access SSID through which they submit it to access the network securely. The following instructions explain how to create the former. For instructions on the latter, see "Self-Registering through a Captive Web Portal" on p. 20.

1. Log in to HiveManager NG as an admin with read/write privileges, click **CONFIGURE**, select an existing network policy or create a new one that supports wireless, and then click **Wireless Networks > Add > All other Networks (standard)**.

Wireless Network

2. Enter the following to define an SSID using service PPSKs for user authentication and leave any unspecified settings at their default values:

Name (SSID): Cloud-PPSK

Note: This is the name for how the object is stored in the HiveManager and HiveOS. You cannot use spaces in this name.

Broadcast Name: Cloud-PPSK

Note: This is wireless network that the AP advertises over the air. Its name can include spaces.

SSID Usage: SSID Authentication

Private Pre-Shared Key: (select)

Key Management: WPA2-(WPA2 Personal)-PSK

Encryption Method: CCMP (AES)

Set the maximum number of clients per private

PSK: By default, APs do not impose a maximum number of concurrent clients per PPSK user. This is a simple way of providing PPSK users for variously sized groups of visitors, each group getting its own unique PPSK password. A maximum of one restricts a PPSK to one client device at a time. You can use the same PPSK on more than one device but not at the same time. Increasing it to two or three clients per PPSK user is convenient for people with multiple active wireless devices because they can use the same PPSK password on all of them at the same time.

Clear the check box to leave the maximum number of concurrent clients per PPSK user as 0 (unrestricted), or select it and enter a number from 1 to 15 to impose a maximum.

Controlling the Number of Clients per PPSK

The maximum number of clients per PPSK user is restricted per SSID and controlled by looking at the roaming cache of neighboring hive members. A maximum number of clients per PPSK user is enforced only on an AP and its first-hop neighbors. It is not enforceable on non-neighboring hive members. For example, on a school campus with several buildings, the PPSK user-per-client maximum would be enforced on all the APs in the building where a student was using his key (assuming that all the APs in that building were first-hop neighbors). However, if that student shared his PPSK password with other students in various buildings across campus, the friends could all connect to the same SSID in their different locations even if doing so exceeded the PPSK user-per-client maximum. Users can use the same PPSK password in different buildings because the control appears only in neighbors' roaming cache lists.

Enable Captive Web Portal: Leave it toggled **OFF** to allow authenticated PPSK users onto the network directly after submitting a valid key. Toggle it **ON** to require authenticated PPSK users to accept a network use policy agreement displayed on a captive web portal before APs allow them onto the rest of the network.

Wireless Network

Name (SSID) *
Broadcast Name *

Broadcast SSID Using
☒ WiFi0 Radio (2.4 GHz or 5 GHz)
☒ WiFi1 Radio (5 GHz only)

SSID Usage

SSID Authentication

MAC Authentication

Enterprise
WPA / WPA2 802.1X

Personal
WPA / WPA2 PSK

Private Pre-Shared Key

WEP

Open Unsecured

Key Management

Encryption Method

☒ Set the maximum number of clients per private PSK
Range : 0-15, 0=no limit

☐ Set the MAC binding numbers per private PSK
Range : 1-5

Enable Captive Web Portal

The next step is to create one or more PPSK user groups as explained in the next section. Then, after creating user groups, return to the SSID and either assign a default user profile for all user groups or assign a different user profile to each user group based on user group membership. By linking multiple user groups to a single SSID, you can assign each group with a different user profile to provide unique traffic settings such as user VLAN and firewall policies. In addition, reducing the number of SSIDs that each AP broadcasts conserves airtime that management frames from the additional SSIDs would otherwise have consumed. For instructions, see "Creating a Device PPSK SSID" on p. 27.

Creating a Cloud PPSK User Group

Key Points: A HiveManager admin creates PPSK user groups and links them to PPSK SSIDs.

Service PPSK user groups are like containers into which PPSK users can be added. Only HiveManager NG administrators can create users groups, but then HiveManager NG administrators, guest management administrators, employees, and even users themselves can add PPSK users to them.

To create a service PPSK user group within the context of the SSID you defined in the previous section, click **Add** in the *Authentication Settings: User Groups* section.

Optionally, you can create a service PPSK user group by logging in to HiveManager NG as an admin with read/write privileges and then clicking **CONFIGURE > Users > User Groups > Add**. If you create PPSK user groups outside the context of an SSID, you must reference them from within one or PPSK SSIDs later.

Enter the following, leave other settings at their default values, and then click **Save**:

User Group Name: Enter a name for the PPSK user group. It can be up to 32 characters long without spaces.

Password DB Location: **CLOUD** (This stores the PPSKs in the cloud rather than on local Aerohive APs.)

Password Type: **PPSK**

Enable CWP Register: Select this check box for the user group to be eligible for use in a captive web portal that includes PPSK self-registration. If this check box is cleared, the user group will not appear in the User Groups drop-down list in the New Guest Access SSID dialog box when **Guests can self-register, then sign in** is selected.

Note: For information about the other settings for a service PPSK user group, see the [Configuring a User Group](#) Help topic.

Delivery Settings

Text Messages (SMS): To send PPSK passwords to users by SMS, select the check box and then choose **Default PPSK SMS Template** from the drop-down list.

Email: To send PPSK passwords to users by email, select the check box and then choose **Default PPSK Email Template** from the drop-down list.

Note: If you want to make different templates and use those instead the predefined ones, navigate to Configure > Common Objects > Basic > Notification Templates, define the templates you want, and then choose them from the drop-down lists. For information about creating custom SMS and email templates, see the [Configuring a Notification Template](#) Help topic.

New User Group

User Group Name *

Password DB Location

Password Type

Description

Enable CWP Register ☒ Enable CWP Register

Password Settings

Generate Password Using * ☒ Letters ☐ Numbers ☐ Special Characters

Enforce the use of

PSK Generation Method

Generate Password Length

Maximum Password Length is 63

Expiration Settings

☒ Require Authentication After minutes

Account Expiration

Delivery Settings

Deliver Access Key by * ☒ Text Messages(SMS)

☐ Email

HiveManager NG only applies expiration settings to device RADIUS users and ignores them when the user group is any other type.

Creating Cloud PPSK Users

Key Points: Depending on how you set up administrative privileges, HiveManager NG administrators, guest management administrators, employees, and wireless users can all create cloud PPSK users.

There are several ways to create cloud PPSK users, depending on the role of the person creating them. However, in all cases, a HiveManager NG administrator must first create one or more PPSK SSIDs and cloud PPSK user groups and link the user groups to the SSIDs as described above. The SSIDs can include a captive web portal through which users self-register and obtain PPSK passwords on their own, or they can simply require users to submit passwords obtained by email, SMS, or printout. An admin might create PPSK users and distribute their passwords to users, or users can use the iPad Kiosk App to do that for themselves.

HiveManager NG Administrators

A common use of PPSKs is to secure wireless access for a permanent group of users, such as employees. In this case, a HiveManager admin creates a PPSK SSID and one or more cloud PPSK user groups as described in the previous sections. He then adds users to the groups and distributes the PPSK passwords to users to submit when authenticating themselves as follows:

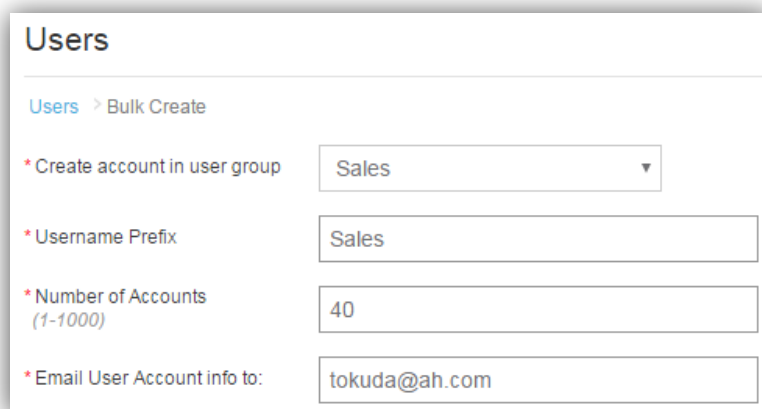
1. Log in to HiveManager NG as an admin with read/write privileges.
2. To add users in bulk, click **CONFIGURE > Users > Users > Bulk Create**, enter the following and then click **Save**:

Create account in user group: Choose a previously defined cloud PPSK user group from the drop-down list.

User name Prefix: Add a prefix such as something that indicates the user group to all users created in bulk.

Number of Accounts: Enter the number of cloud PPSK users you want to create up to 1000 maximum.

Email User Account info to: Enter the email address of the person to whom you want to send PPSK users.



The screenshot shows the 'Users' section of the HiveManager NG interface, specifically the 'Bulk Create' page. The breadcrumb trail is 'Users > Bulk Create'. There are four required fields, each marked with a red asterisk: 1. 'Create account in user group' is a dropdown menu currently set to 'Sales'. 2. 'Username Prefix' is a text input field containing 'Sales'. 3. 'Number of Accounts (1-1000)' is a text input field containing '40'. 4. 'Email User Account info to:' is a text input field containing 'tokuda@ah.com'.

As soon as you click **Save**, HiveManager NG sends a .csv file with a list of all the PPSK users you created.

3. To add users individually, click **CONFIGURE > Users > Users > Add**, enter the following—only the user name and password are required—and then click **Save**:

Create account in user group: Choose one of the PPSK user groups you created previously.

Name: Enter a name for the PPSK user. This name appears in any messages sent to the email address in the *Deliver Password* section. The email messages, which contain login credentials and wireless connection instructions, begins with "Welcome <this_name>". When you choose **Name** in the User Name drop-down list, this field is required. Otherwise, it is optional and if left empty, whatever you define as the user name—email address, phone number, or other—is used in the email message. The name can be up to 32 characters including spaces.

Organization: (optional) For permanent users, leave this empty.

Purpose of visit: (optional) For permanent users, leave this empty.

Email Address: Leave this empty or enter the user's email address. This is only required if you choose **Email Address** in the User Name drop-down list.

Phone Number: Leave this empty or enter the user's mobile phone number, including country code. This is only required if you choose **Phone Number** from the User Name drop-down list.


Note: HiveManager NG does not necessarily deliver the PPSK password to the email address or phone number (as a text message) defined here. These are primarily for tracking purposes. See Deliver Password below.


User Name: Choose one of four identifiers from the drop-down list: **Email Address** (default), **Name**, **Phone Number**, or **Other**. If you select **Other**, you must enter another type of user identifier, such as Jane's iPhone, Guest, or <organization_name> in the additional field that appears.

Password: Enter a text string that will be the PPSK or click **Generate** to have HiveManager NG generate one automatically.

Description: (optional) Enter any notes about the user for future reference.

Deliver Password

Email Address: Enter the email to which HiveManager NG sends the PPSK password when you click the envelope icon () on the *Users* page. It does not have to be the same as that for the user. For example, this might be the address of someone in the HR department or that of someone else who will distribute it. This field is auto-populated if you have already entered an email address above. This option only appears if you previously selected **Email** in the *Delivery Settings* section in the user group configuration.

Text Message: Enter the phone number to which HiveManager NG sends the PPSK password when you click the text message icon () on the *Users* page. Be sure to include the country code. This option only appears if you previously selected **Text Messages (SMS)** in the *Delivery Settings* section in the user group configuration.

Users

[Users](#) > New User

Create account in user group * Sales

Name John Kenyon

Organization

Purpose of Visit

Email Address jkenyon@ah.com

Phone Number +1 4085106100

User Name Name

Password * NgREjNvngT GENERATE

☒ Show Password

Description

Deliver Password

☒ Email Address jkenyon@ah.com

☒ Text Message 1-4085106100

Guest Management Administrators

Guest management administrators are people who can only create PPSK users and distribute PPSK passwords through limited administrative access to the HiveManager NG GUI or through the Guest Check-in Web App. Both options are described below.

Note: Guest management administrators can also log in to HiveManager NG through the iPad Kiosk App to allow wireless users to create their own PPSK users as described in "Self-Registering with the iPad Kiosk App" on p. 24.

Limited HiveManager NG GUI Access for Creating PPSK Users

First, a HiveManager NG admin creates an employee group and adds the email addresses of employees whom the admin wants to grant guest management permissions. Then the admin creates guest management accounts for these employees. The employees receive an email from HiveManager NG with a link to create a password. After that, they can log in and create PPSK users.

1. Log in to HiveManager NG as an admin with read/write privileges, click *admin_name* > **Global Settings** > **Credential Distribution Groups** > **Add**, enter the following, and then click **Save**:

Group Name: Enter a descriptive name such as **Guest-PPSK-Creators**.

Admin Account: **Guest Management Role User**

Guest Management User:

Enter the email addresses of one or more people whom you want to create and distribute PPSK users.

Credential Restriction

Restrict the number of credentials per employee to: (select) Enter a number from 1 to 99999 depending on how many PPSK users you want each guest management admin to be able to create. This limit is applied to the number of concurrently active PPSK users. When a user expires, it no longer counts toward this maximum. (When using the Aerohive iPad Kiosk app, everyone who self-registers does so under the login of the guest management admin who launches the app on the iPad. Therefore, make sure that he or she can create plenty of PPSK users.)

Credential Distribution Groups

Group Name *

Admin Account *

Guest Management User *

Type to create a value

Credential Restriction ☒ Restrict the number of credentials per employee to

Registration Operation ☐ Email Approval

Enable User Groups ☐ Select All

☒ 1Day
☒ 7Days

Registration Operation

Email Approval: (clear)

*Note: Currently only the Guest Management Web Application supports email approval. If you select **Email Approval** and a guest management admin belonging to this employee group enters an email address in the "Here to Visit" field in the Register a Guest form, HiveManager NG sends an email requesting approval to that address. Once the recipient clicks **Approve** in the email, HiveManager NG activates the PPSK user.*

Enable User Groups: Select all the PPSK user groups for which the administrators specified in the Guest Management User field can create users.

- Click **Account Management > Add** and create guest management accounts for the people whose email addresses you put in the employee group.

After you create each account, HiveManager NG automatically sends a message to the email address associated with it, prompting the recipient to set up a password and access the Configure > Users page to create PPSK user accounts for visitors.

User Name	User Group	Approval	Delivery	Expiration
guest1	1Day			2018-03-08T20:12:02.733+0000
guest2	1Day			2018-03-08T20:12:02.734+0000
guest3	1Day			2018-03-08T20:12:02.734+0000
guest4	1Day			2018-03-08T20:12:02.734+0000
guest5	1Day			2018-03-08T20:12:02.734+0000
guest6	1Day			2018-03-08T20:12:02.734+0000
guest7	1Day			2018-03-08T20:12:02.734+0000
guest8	1Day			2018-03-08T20:12:02.734+0000
guest9	1Day			2018-03-08T20:12:02.734+0000
guest10	1Day			2018-03-08T20:12:02.734+0000

Guest Check-in Web App

In addition to the built-in PPSK user creation interface, guest management administrators can create PPSK users through the Guest Check-in Web App. This web app is intended for use by lobby or front desk personnel to check in visitors individually and in bulk and deliver PPSK user credentials to them.

For bulk creation, you can import a .CSV file with PPSK user creation details. It also supports various PPSK delivery methods: email, SMS, and print.

The Guest Check-in Web App is available at <https://guest-checkin.aerohive.com>. Guest management administrators log in with their HiveManager NG admin name and password. They are then prompted to choose which VHM to authorize, which is important for people with access to multiple VHMs.

Note: VHM stands for virtual HiveManager and refers to a HiveManager NG account.

After logging in to the web app, click **New Visitor**, enter the following information for the visitor, and then click **Enter**:

Visitor Info

1 Peter Piesque
FULL NAME*

ppiesque@gac.com
EMAIL*

+1415-555-1212
PHONE

7Days
1Day

[Add Visitor](#)

What company are they from?

Enter company name

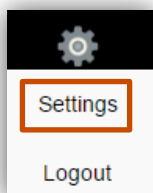
Who are they here to see?

Enter contact name

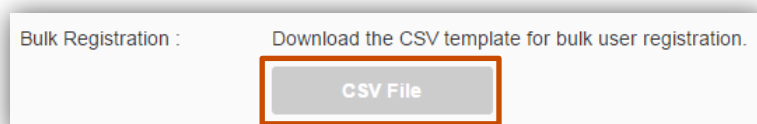
☒ ENTER CANCEL

The title of this field is *Type*. When you click it, a drop-down list appears with the PPSK user groups that you assigned to the guest management admin group to which the current admin belongs.

To import users in bulk, click the gear icon and then choose **Settings**.



Click **CSV File** and save it to your system.



Add entries with information in the provided columns: CompanyName, WhomToSee, Name, Email, Phone, Type. (Remember to include the country code at the start of each phone number.)

Click **Import CSV** on the web app dashboard, navigate to the file you saved, and select it.

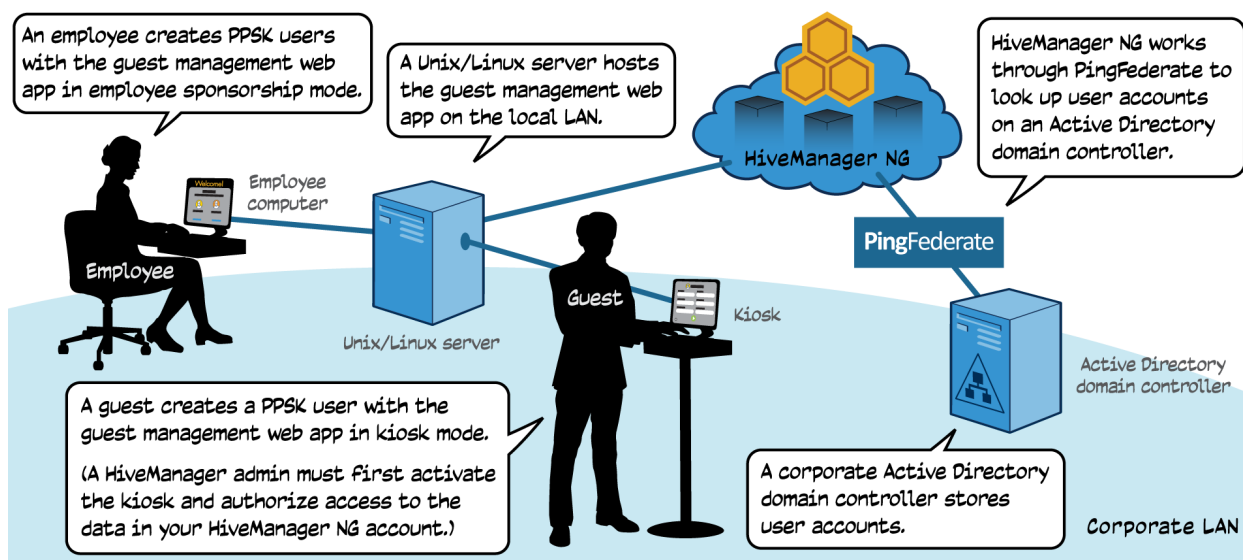


Employees or Guests (Guest Management Web Application)

HiveManager NG can integrate with a guest management web application—a reference app available from Aerohive—that validates employee credentials on a corporate Active Directory server and then allows them to create PPSK users for guests and their own personal wireless devices. The web application can function in two modes: employee sponsorship and kiosk. In employee sponsorship mode, employees interact with a Web UI to create PPSK users. In kiosk mode, employees (or HiveManager NG administrators) can activate a kiosk on a web browser running on a dedicated computer so that guests can create their own PPSK users.

The setup for allowing validated employees to create PPSK users involves two steps: (1) installing an application on a web server and (2) integrating HiveManager NG through PingFederation with an Active Directory domain controller. The major steps are described below.

Note: The setup requires the participation of Aerohive Engineering, especially for the integration of HiveManager NG with Active Directory. If you are interested in this, contact your Aerohive account representative.



Installing the Web App

You must install the web application on a Tomcat web server running on a Unix/Linux server at your own site. You can then customize the web pages with which employees interact so they match your corporate brand. The web server will forward employee login requests and PPSK user definitions over HTTPS to HiveManager NG.

The Linux/Unix server must be running CentOS v5.8 with Tomcat v7 and Nginx v0.8.55 or later web servers installed. If necessary, you can download the required software from the following sites:

CentOS: <https://wiki.centos.org/Download>

Nginx: <http://nginx.org/en/download.html>

Tomcat: http://www.davidghedini.com/pg/entry/install_tomcat_7_on_centos

In addition to the software listed above, the server also requires Java 7 and Maven v3.0.3 or later to compile and deploy the web application.

1. After the environment is set up, contact your Aerohive account representative to obtain the web application source code and download it to a directory on your local computer.
2. Change your current directory to `.../hive-ref/guest-mgmt-ref-app/`

3. To build the project, run **mvn clean install**

The built web app is now located in `.../hive-ref/guestmgmt-ref-app/target/guestmgmt-ref.war`

4. Copy the war file from `target/guestmgmt-ref.war` on your computer to the `webapps` directory on the Tomcat server; for example, `/opt/tomcat_instance1/webapps`
5. Define the following configuration file and save it on your Tomcat server. Its default location is `/Aerohive_app/etc/guestmgmt-ref-application.properties`

```
guestmgmt-ref-application.properties

#####
# Guest Management Reference Application      #
#                                           #
# Version: 1.0                             #
#####

#-----
# Deployment mode
#-----
# Enable kiosk mode or use employee-sponsored registration
app.kiosk.enable=<true|false>
# Specify the passcode to launch the kiosk. (Only required for kiosk mode.)
app.kiosk.password=<passcode>
# Three login types are supported: 1. VHM 2. PINGFED 3. LDAP
# 2 & 3 are connected to Active Directory.
oauth.login.type=VHM
#-----
# Customer's API account information
# Contact Aerohive to create API account (required).
#-----
app.apollo.clientId=<ClientId>
app.apollo.clientSecret=<ClientSecret>
app.apollo.clientRedirectUri=<RedirectUrl>
# API URL prefix (don't change)
app.request.forward.xapi.url.prefix=xapi/v1/
#-----
# HiveManager NG server information (required)
# Check with your HiveManager NG administrator.
#-----
# Specify the HiveManager NG global server.
# For cloud services, it is https://cloud.aerohive.com
# For on-premises, it is https://<HMNG-server-address>
app.apollo.url.base=https://cloud.aerohive.com
# Specify the customer's regional server.
# For cloud services, it is https://<regional-dc>.aerohive.com
# For on-premises, it is https://<HMNG-regional-server-address>
app.apollo.vpc.url=https://<regional-dc>.aerohive.com
```

```
# Specify the customer's ownerId.
app.apollo.ownerId=<customer-ownerId>
#-----
# Active Directory and PingFederate information
#
# This is required for enabling Active Directory login.
# The customer needs to preconfigure the customer's ADFS with
# Aerohive's PingFederate service before this.
#
# Check with Aerohive Support and your HiveManager NG administrator.
#-----
# Specify the customer's PingFederate/ADFS URL.
# PingFederate URL example: https://<ping-federate-service>?PartnerIdpId=http://<customer-idp-
service>&TargetResource=https://<hmng-account-service-idfederate-for-ping>
oauth.login.pingfed.ad.url=https://<ping-federate-service>?PartnerIdpId=http://<customer-idp-
service>&TargetResource=https://<hmng-account-service-idfederate-for-ping>
# Specify the customer's LDAP/ADFS URL.
# LDAP ULR example:
https://<apollo.url.base>/services/acct/login/ad?client_id=<ClientId>&redirect_url=<RedirectUrl>
>
oauth.login.ldap.ad.url=https://<apollo.url.base>/services/acct/login/ad?client_id=<ClientId>&r
edirect_url=<RedirectUrl>
#-----
# Application web server attributes (required)
#-----
# Enable to accept a self-signed certificate for SSL. Default is true.
app.disable.ssl.verification=true
# Specify the application server address.
app.server.address=<server-address>
# Specify the application URL prefix.
# Only modify this when choosing a different URL for the application.
app.service.path=/guestmgmt-ref
# Specify the application's cookie expiration time (in milliseconds).
app.cookie.expire=43200
#-----
# System Internal attributes
# Do not modify the section below.
#-----
# API Request Headers
app.apollo.clientId.header=X-AH-API-CLIENT-ID
app.apollo.clientSecret.header=X-AH-API-CLIENT-SECRET
app.apollo.clientRedirectUri.header=X-AH-API-CLIENT-REDIRECT-URI
# API HMNG Account Login
app.apollo.url.thirdpartylogin=/thirdpartylogin
# OAuth Token Exchange
app.apollo.url.accesstoken=/services/acct/thirdparty/accesstoken
```

6. Start or restart your Tomcat server by running **service tomcat7 restart**

The following is the source code directory structure:

Under root /guestmgmt-ref-app/

- /pom.xml The Maven file for compilation and deployment
- /src/ All Java and Web UI source files
- /target/ Target files from running the Maven command

Under /src/main/

- /java Java source code
- /java/com/aerohive/partner/rest/ Aerohive REST API objects
- /java/com/aerohive/partner/web/ Defines the app workflow following the Spring MVC framework
- /java/com/aerohive/partner/web/ApolloApiProxyController.java Aerohive API proxier
- /java/com/aerohive/partner/web/ViewController.java Controls the web page view and flow
- /java/com/aerohive/partner/web/auth/ Implements OAuth token exchanges and logout logic
- /java/com/aerohive/partner/web/util Implements utilities
- /resource Configuration and log properties
- /webapp/ Web app sources based on the JavaScript Dojo framework
- /webapp/resources/ All Web UI source code
- /webapp/resources/images/ Image files shown in the Web UI; you can change the logo and other images by replacing files with same file names
- /webapp/resources/css/ Style files, where you can customize colors, fonts, and so on
- /webapp/resources/i18n/ Internationalization and localization messages; support for more languages is possible by adding localized JavaScript files by language code
- /webapp/WEB-INF/web.xml Defines servlet attributes and application servlet mapping
- /webapp/WEB-INF/views/ JavaScript files for launching the web page
- /webapp/WEB-INF/config/ Spring Bean configuration files

Linking HiveManager NG with Active Directory

The second part of the setup is to define a relationship through PingFederation between HiveManager NG and the Active Directory database where you store employee user accounts to validate login credentials. To complete this step, you must work closely with Aerohive Engineering.

After a user is authenticated, the web app on the Tomcat server displays a page for creating a PPSK user. The employee can create and delete users and the web app relays the information over HTTPS to HiveManager NG. For a large organization that already has Active Directory user accounts in place, it is convenient to use PingFederation to have HiveManager NG communicate with Active Directory. This way, if new people join the company and existing employees leave, you only need to update the Active Directory database to control their ability to create PPSK users.

Note: A HiveManager NG admin who logs in through the app is directed directly to HiveManager NG, not to Active Directory through PingFederation. HiveManager NG admin accounts are stored on HiveManager NG, not on the Active Directory server. Only employee accounts are stored there.

Self-Registering through a Captive Web Portal

Key Points: Wireless users can self-register and obtain PPSK passwords through a captive web portal.

Network users can create their own PPSK users. When they first associate with an AP and open a web browser, the AP directs them to a captive web portal that it is hosting on a built-in web server. The captive web portal prompts them to register and then provides them with PPSK passwords.

1. As a HiveManager NG admin, log in to HiveManager NG, create a cloud PPSK user group as described previously in this guide, and select **Enable CWP Register**.
2. Within a network policy, click **Wireless Networks > Add > Guest Access Network**, enter the following, and then click **Save**:

SSID Name: Enter the name of the SSID configuration object used within HiveManager and HiveOS. It can be the same as the one advertised for users or it can be different.

SSID Broadcast Name: HiveManager automatically fills in this field with the same name as that entered in the SSID Name field above. This is the name of the SSID that guests access after they self-register.

Secured Network: (expand section)

Guests can self-register and then sign in. As an option an employee can approve: (select)

Add employee approval: If you do not want employees to approve guest registration requests, leave it as is. On the other hand, if you want employees to approve them, click and add one or more domain names to the list. Employees belonging to a listed domain can then approve guest self-registrations.

Guest Self-Registration SSID: Enter the name of the SSID that guests first use to self-register for a PPSK.

*Note: If you want to customize the colors, fonts, and some of the content on the captive web portal landing, success, and error pages, click **Customize Captive Web Portal**.*

Set the maximum number of clients per private PSK: Restrict the number of client devices that can use the same PPSK. By default, no limit is imposed.

Pre-Defined Settings

Pre-Defined Settings: If you want to use the default user profile for guest access, do not click this button. If you want to create and apply a new user profile, click it, enter a new name in the Name field, choose a different VLAN, and then click **Save**.

Authentication DB

Cloud: (leave selected; it is the only available choice)

User Groups

Choose a previously defined service PPSK user group. If you do not see a group that you want in the drop-down list, click **User Group Settings** and define a new one.

Schedule

To make the SSID available all the time, leave the schedule toggled **OFF**. To limit availability to certain times, toggle the schedule **ON** and set the days and times when it is available.

New Guest Access SSID

*SSID Name

*SSID Broadcast Name

Authentication Type Note: You will not be able to edit the Authentication Type after saving.

> Unsecured (Open) Network

✓ Secured Network

☐ Create credentials for guests to log in to your network.

☒ Guests can self-register, then sign in. As an option, an employee can approve.

☐ Create global password (PSK) credentials for your guests to log in to your network.

[Add employee approval](#)

[CUSTOMIZE CAPTIVE WEB PORTAL >](#)

*Guest Self-Registration SSID

☒ Set the maximum number of clients per private PSK

Range 0-15, 0 = no limit

Pre-Defined Settings

View pre-defined settings for this SSID.

Authentication DB

Select Cloud if you want the password database credentials to be stored on a local AP. **NOTE: V**
opened between the network devices and Hive

User Groups

Here is a list of available user groups to choose from. Or, you can [create one](#).

[USER GROUP SETTINGS >](#)

Schedule

You can designate a schedule for SSID availability.

[SAVE](#) [CANCEL](#)

Guest Access Approver Email Domain List

Allow employees within the following domain to sponsor and approve guests.

Domain Name * [ADD](#)

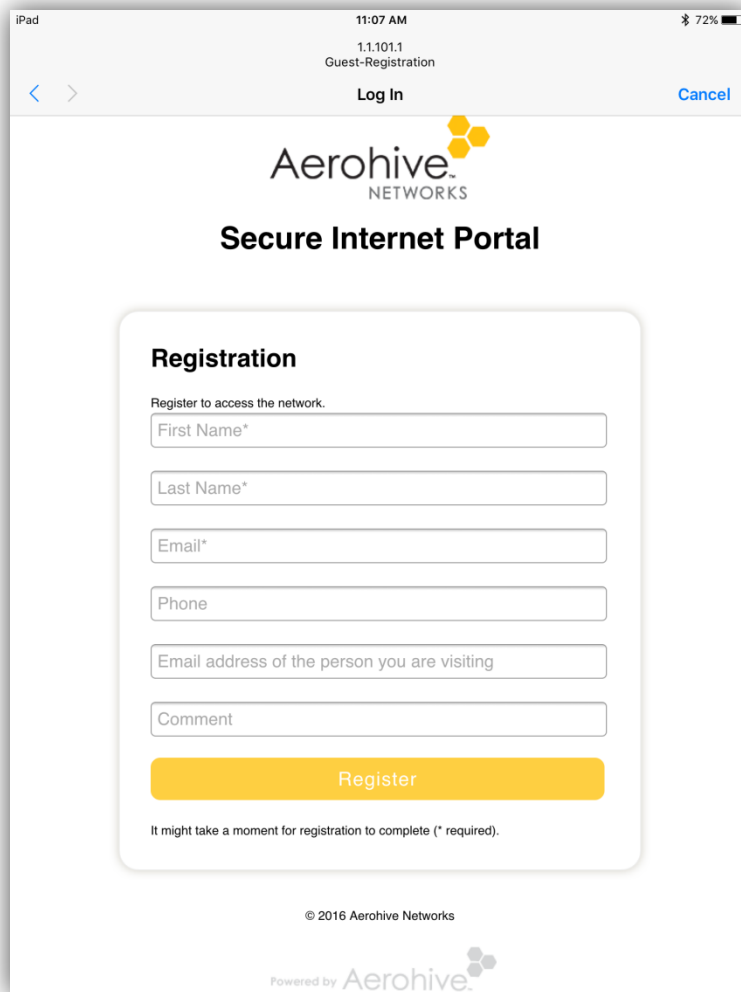
<input type="checkbox"/> DOMAIN NAME	ADDED ON
<input type="checkbox"/> your-domain1.com	2018-03-03 14:32:19
<input type="checkbox"/> your-domain2.com	2018-03-03 14:32:27

This configuration adds two SSIDs to the network policy: an open SSID that users initially access to self-register and obtain a PSK password through a captive web portal (Guest-Registration) and a secure SSID that they subsequently access by submitting their passwords and through which they reach the rest of the network (Guest-Access).

Wireless Networks			
Add			
SSID	Guest Access	Access Security	VLAN
<input type="checkbox"/> Guest-Access	Edit	Private PSK	BYOD-VLANs
<input type="checkbox"/> Guest-Registration	Edit	Unsecured (Open) Network	

3. Upload the configuration to your access points.

When a user connects to the open SSID, a captive web portal appears with a self-registration form. (Note that the phone number must include the country code and omit punctuation such as dashes and parentheses.)



Registration

Register to access the network.

First Name*

Last Name*

Email*

Phone

Email address of the person you are visiting

Comment

Register

It might take a moment for registration to complete (* required).

© 2016 Aerohive Networks

Powered by Aerohive

After the user completes the form and clicks **Register**, the AP sends a PPSK user request to one of the two RadSec proxy servers in its management subnet. The RadSec proxy server forwards it to HiveManager NG, which creates a PPSK user and returns a PMK and password to the AP, which displays the password briefly before quickly reverting to the registration form. If you enabled employee approval (and added the domain name of employees' email addresses to the *Guest Access Approver Email Domain List*), HiveManager NG sends an approval request like the following to the email address entered in the fifth field of the registration.

Hi, <employee_name>:

Click [Approve](#) to activate access for the following user:

User Name: Grace James

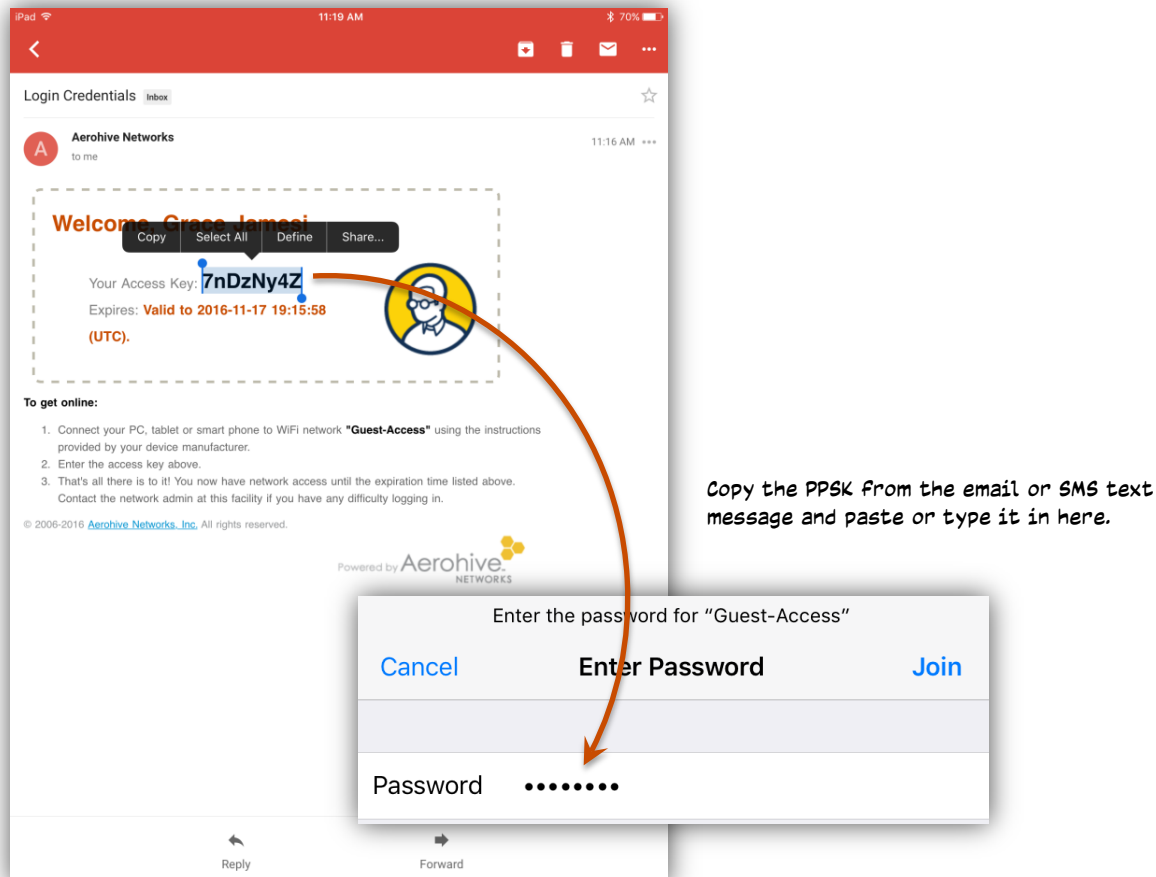
Email Address: grace.james22@gmail.com

Phone Number: 6505676122

Expiration: No limit.

The email message comes from Aerohive Networks with the subject *Approve User Credential*. After the employee clicks **Approve**, HiveManager NG sends an email or SMS text message with the PPSK password to the user. The user can then copy the password, connect to the secure access SSID, and paste or type it in when prompted for a password.

If you did not enable employee approval, HiveManager NG sends an email or SMS text message with the PPSK password to the user immediately after a successful registration.




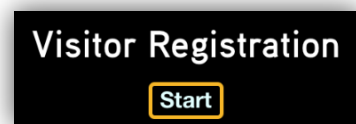
Self-Registering with the iPad Kiosk App

Key Points: The iPad kiosk is a simple way for users to self-register and create their own PPSK users.

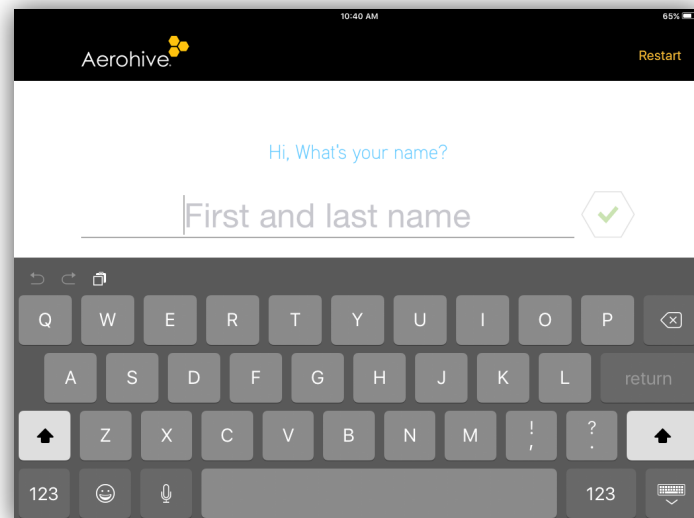
This app is intended for use in unattended lobby areas, or in reception areas where guests register themselves for temporary wireless access at the organization they are visiting.

The guest management administrator who sets up the app on an iPad must log in first, choose his or her HiveManager NG account, and authorize the app to communicate with it. (For security, use a guest management admin account instead of a HiveManager NG admin account with full access rights to HiveManager NG.)

Next, a list of credential types (PPSK user groups) for which the admin can create PPSK users appears. The admin chooses one PPSK user group and then taps the check mark icon  to lock the app to the guest management administrator's account and the selected PPSK user group. Then everyone else who self-registers does so under that administrator's login. Therefore, it is important that he or she can create plenty of PPSK users.



The app supports visitor sign-in using an email or phone number, an optional employee lookup and approval process (using LDAP), and various PPSK password delivery methods: SMS, email, print, and QR code for Androids.



It is possible to exit the app by rebooting the iPad or double-clicking the **Home** button and sliding the app off screen. However, by putting the iPad in Guided Access mode, you can lock the screen so that users cannot switch to another app:

1. Press the **Home** button and then tap **Settings > General > Accessibility**.
2. Enable **Guided Access**, select **Passcode Settings > Set Guided Access Passcode**, and then enter a passcode.
3. Return to the home screen and tap the **Aerohive Kiosk** icon to launch the app.
4. Triple-click the **Home** button. In the Hardware Buttons Options menu, disable **Sleep/Wake Button** so that people cannot turn off the iPad. Also, enable **Keyboards** and **Touch** so they can enter information as they register. Then tap **Start** to enter Guided Access mode.
5. To exit, triple-click the **Home** button, enter the passcode, and then tap **End**.

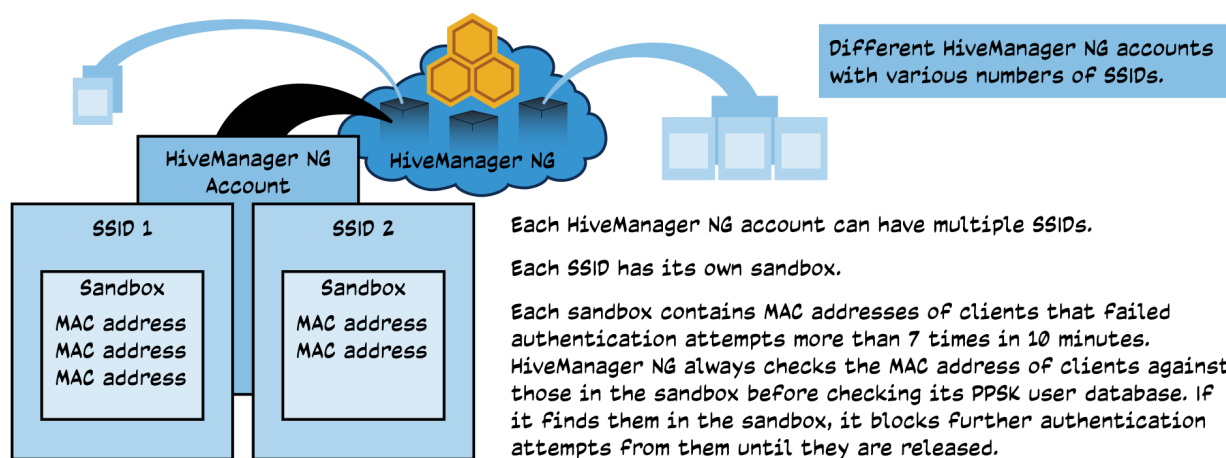
The Aerohive iPad Kiosk app is [available on the app store](#) and works on iPads running iOS 8.0 or later.

Defending against DoS Attacks

Key Points: This section describes the HiveManager NG defense mechanism against DoS attacks.


When HiveManager NG authenticates a PPSK user, it must check a large list to see which PPSK password matches the one that the user submitted. If users repeatedly submit incorrect passwords or those for deleted or expired PPSK users, it could introduce a DoS (denial of service) attack.

To prevent such an attack, HiveManager NG temporarily puts the MAC address of a client device that keeps failing authentication into a sandbox, which is sometimes referred to as *jail* or *black list*. Each HiveManager NG account maintains one sandbox per SSID. By default, a user can fail authentication 10 times in 7 minutes. After that, HiveManager NG puts the MAC address of the client device into the sandbox and blocks any future authentication attempts for 30 minutes. After 30 minutes, it releases the MAC address. For all authentication attempts, HiveManager NG first checks the client MAC address against the list in the sandbox for the corresponding SSID.



Deleting Cloud PPSK Users

Key Points: This section describes the behavior to expect when you delete PPSKs of actively connected clients.

To delete one or more PPSK users, click **Configure > Users > Users**, select the check boxes of the PPSK users you want to delete, and then click the **Delete** icon (). If a user's client is currently associated with an AP in an active session when you delete a PPSK user, the AP will not immediately end the session by deauthenticating the client. HiveManager NG tracks the session of each client in its accounting log (*admin_name* > Global Settings > Logs > Accounting Logs), updating log entries at 10-minute intervals by default. The next time HiveManager NG updates an accounting log entry and discovers that a PPSK user has been deleted for an active session, it sends a request to the AP to deauthenticate the client. As a result, APs deauthenticate clients at 10-minute intervals from the start of their sessions. After an AP deauthenticates a client, the user will have to register again the next time he or she connects.

The following command changes the accounting interval:

```
security-object <name> security aaa radius-server account-interim-interval <number>
```

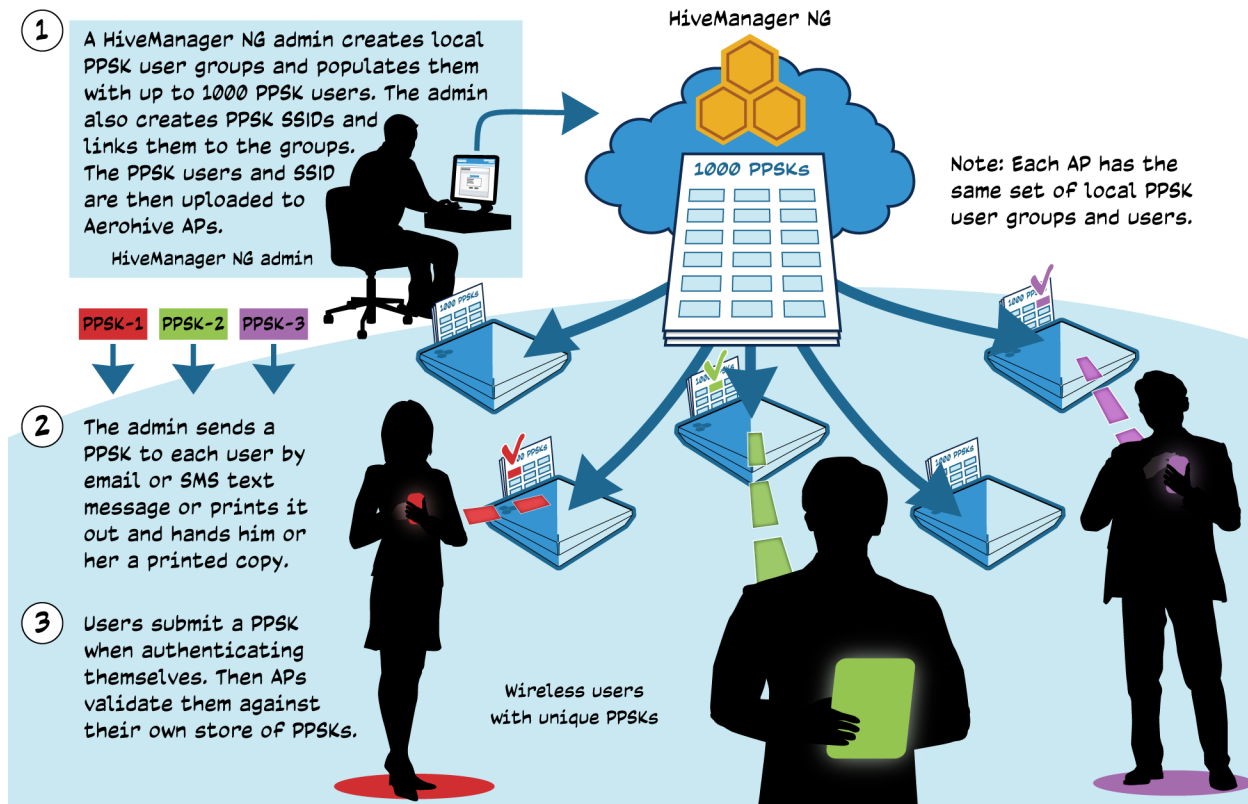
The <number> value can be from 10 to 1,000,000,000 seconds. The default is 600 seconds (10 minutes).

To deauthenticate a client immediately, enter the following set of three commands in which <mac_addr> is the MAC address of the client device:

```
clear auth roaming-cache mac <mac_addr>
clear auth roaming-cache mac <mac_addr> hive-neighbors
clear auth local-cache mac <mac_addr>
```

Local PPSK

Local PPSK authentication works well with a limited number of users. Most APs can store up to 9999 PPSK users with the exception of the AP100 series (AP121, AP122, AP130, AP141), which can store up to 4096. If you need an AP to support more than 4096 or 9999 different PPSK users (across multiple user groups), then you should use cloud PPSK instead. Like cloud PPSK user groups, Aerohive also limits the number of users in a local PPSK user group to 1000.



Setting up local PPSK user authentication involves five components:

- Creating a PPSK SSID
- Creating one or more PPSK user groups
- Adding PPSK users to the groups
- Distributing PPSK users to APs
- Distributing PPSK passwords to individual wireless users

Creating a Local PPSK SSID

The following instructions explain how to create a PPSK SSID and user groups, add users to the groups in bulk, assign user profiles based on the group to which users belong, and upload the configuration to your APs.

1. Log in to HiveManager NG as an admin with read/write privileges, click **CONFIGURE**, select an existing network policy or create a new one that supports wireless, and then click **Wireless Networks > Add > All other Networks (standard)**.

Wireless Network

2. To define an SSID using local PPSKs, enter the following and keep the default values for all other settings:

Name (SSID): Local-PPSK

Note: This is the name for how the object is stored in the system. You cannot use spaces in this name.

Broadcast Name: Local-PPSK

Note: This is wireless network that the AP advertises over the air. Its name can include spaces.

SSID Usage: SSID Authentication

Private Pre-Shared Key: (select)

Key Management: WPA2-(WPA2 Personal)-PSK

Encryption Method: CCMP (AES)

Set the maximum number of clients per private PSK: By default, APs do not impose a maximum number of clients per PPSK. You can keep this setting or limit one or more clients per PPSK based on how many wireless devices individual users typically connect to the network.

Clear the check box to leave the maximum number of clients per PPSK as 0 (unrestricted), or select it and enter a number from 1 to 15 to impose a maximum.

Enable Captive Web Portal: Leave it toggled **OFF** to allow authenticated PPSK users onto the network directly after submitting a valid key. Toggle it **ON** to require authenticated PPSK users to accept a network use policy agreement displayed on a captive web portal before APs allow them onto the rest of the network.

3. In the *Authentication Settings* section, add a device PPSK user group by clicking **Add** under *User Groups*.

New User Group

4. Enter the following and then click **Save**:

User Group Name: Enter a name for the PPSK user group. It can be up to 32 characters long without spaces.

Password DB Location: LOCAL (This stores the PPSKs locally on Aerohive APs rather than in the cloud.)

Password Type: PPSK

Note: For information about the password and expiration settings, see the [Configuring a User Group](#) Help topic.

Delivery Settings

Text Messages (SMS): To enable HiveManager NG to send PPSK passwords to users by SMS, select the check box and then choose **Default PPSK SMS Template** from the drop-down list.

Email: To enable HiveManager NG to send PPSK passwords to users by email, select the check box and then choose **Default PPSK Email Template** from the drop-down list.

*Note: If you want to make different templates and use those instead the predefined ones, navigate to **Configure > Common Objects > Basic > Notification Templates**, define the templates you want, and then choose them from the drop-down lists. For information about creating custom SMS and email templates, see the [Configuring a Notification Template](#) Help topic.*

Wireless Network

5. To add more device PPSK user groups, repeat the previous steps.

6. You can add users to the local PPSK user group you just created one by one or in bulk.

To add users singly, click **Add** in the # of Users column and define each one individually. This approach can work if you only have a few users but is impractical for larger numbers.

To add users in bulk, click **Save** to save your SSID configuration, and then click **Users > Users > Bulk Create**.

Users

7. Enter the following and then click **Save**:

Create account in user group: Choose the name of the PPSK user group you created in the previous section.

User Name Prefix: Enter a prefix to append to all PPSK user names, such as "Guest".

Number of Accounts: Enter the number of device PPSK users to add to the user group. It can be from 1 to 1000.

Email User Account info to: Enter the email address of the person to whom you want to email PPSK user account information.

*Note: As soon as you click **Save**, HiveManager NG sends a .csv in an email attachment to this email address. The recipient can then distribute the PPSK passwords to users out of band.*

8. To return to the PPSK SSID configuration, click **Network Policies > policy_name > Wireless Networks > ssid_name**.

Wireless Network

9. Scroll down to the *User Access Settings* section and then click **+** to create a user profile that APs will apply to users that successfully authenticate with their PPSKs.

Create User Profile

10. Configure the default user profile for the SSID and then click **Save**. For information about the many settings in a user profile, see the *Adding a New User Profile* section in the [Viewing the User Profile List Help topic](#).

Wireless Network


If you assigned multiple PPSK user groups to the SSID, you can assign each one its own user profile that defines a VLAN, firewall and QoS policies, availability schedules, SLA level and actions, and traffic limits based on data or time. Assigning different groups of users to different VLANs offers an added benefit of keeping broadcast domains small to limit broadcast and multicast traffic to reasonable levels so that they do not negatively affect overall network performance.

11. To assign different user profiles to different PPSK user groups, select **Apply a different user profile to various clients and user groups** in the *User Access Settings* section and then click **Add**.

Create User Profile

12. Create a user profile that you want to apply to one of the PPSK user groups and then click **Save**.

Wireless Network

13. Scroll down to the *User Access Settings* section, and then click the **Add a user profile assignment rule** icon () in the Assignment Rules column for the user profile that you want to apply to one of the PPSK user groups.

User Profile Assignment

14. Enter a name and description of the assignment rule and then click **+ > User Group**.

User Group

15. Select the check box of the user group to which PPSK users must belong for the AP to assign the user profile to them and then click **Select**.

User Profile Assignment

16. Make sure that the user profile assignment rule you just defined is listed and then click **Save**.

Wireless Network

17. To assign different user profiles to other user groups, repeat the previous four steps.
18. After you finish assigning user profiles to all the PPSK user groups, save the SSID by clicking **Save**.
19. To upload the network policy and PPSK users to your APs, click **Deploy Policy**.

Deploy Policy

20. Select the check boxes of all the APs to which you want to upload the network policy and PPSK users and then click **Upload**.

Device Update

21. Select **Update Network Policy and Configuration**, select **Delta Configuration Update**, and then click **Perform Update**.