Multi-Preshared Key

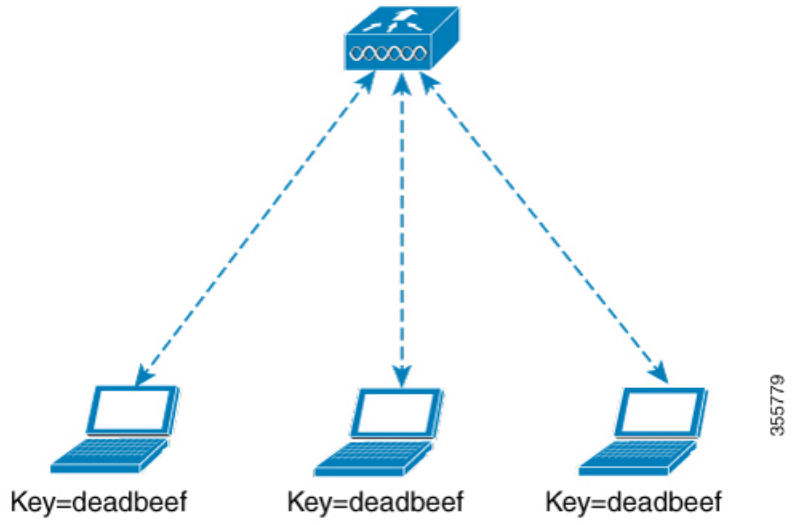
Information About Multi-Preshared Key

Multi-PSK feature supports multiple PSKs simultaneously on a single SSID. You can use any of the configured PSKs to join the network. This is different from the Identity PSK (iPSK), wherein unique PSKs are created for individuals or groups of users on the same SSID.

From 16.10 onwards, each SSID supports five PSKs, which can be extended

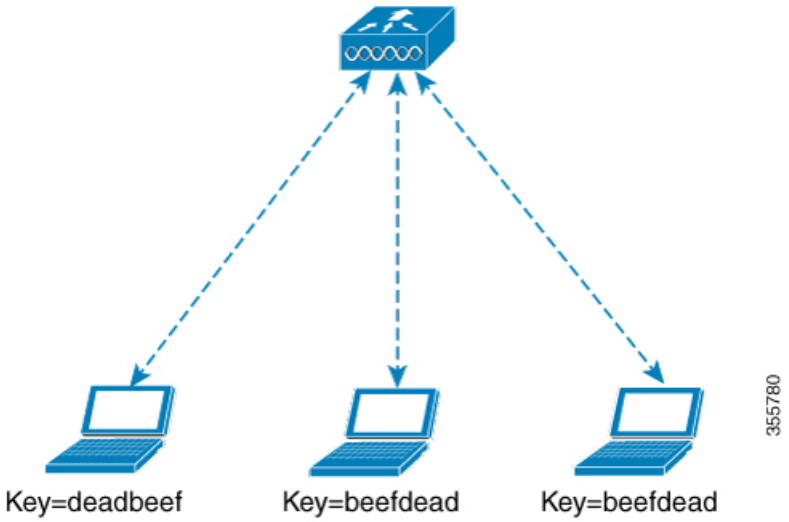
In a traditional PSK, all the clients joining the network use the same password as shown in the below figure.

Figure 1: Traditional PSK



But with multi-PSK, client can use any of the configured pre-shared keys to connect to the network as shown in the below figure.

Figure 2: Multi-PSK



In Multi-PSK, two passwords are configured (deadbeef and beefdead) for the same SSID. In this scenario, clients can connect to the network using either of the passwords.

Restrictions on Multi-PSK

- Central authentication is supported in local, flex, and fabric modes only.
- In central authentication flex mode, the standalone AP allows client join with the highest priority PSK (*priority 0* key). New clients that do not use the highest priority PSK are rejected during the standalone mode.
- Multi-PSK does not support local authentication.
- Multi-PSK is different from iPSK. In iPSK, the PSK password comes from ISE authorization policy, so MAB is required. MPSK uses a pool of passwords locally configured in WLAN, so ISE is not used.

Configuring Multi-Preshared Key (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 On the **Wireless Networks** page, click the name of the WLAN.

Step 3 In the **Edit WLAN** window, click the **Security** tab.

Step 4 In the **Layer2** tab, choose the **Layer2 Security Mode** from the following options:

- None: No Layer 2 security
- 802.1X: WEP 802.1X data encryption type

- WPA + WPA2: Wi-Fi Protected Access
- Static WEP: Static WEP encryption parameters
- Static WEP+802.1X: Both Static WEP and 802.1X parameters

Parameters	Description
802.1X	
WEP Key Size	Choose the key size. The available values are *None*, *40 bits*, and *104 bits*.
WPA + WPA2	
Protected Management Frame	Choose from the following options: • Disabled • Optional • Required
WPA Policy	Check the check box to enable WPA policy.
WPA Encryption	Choose the WPA encryption standard. A WPA encryption standard must be specified if you have enabled WPA policy.
WPA2 Policy	Check the check box to enable WPA2 policy.
WPA2 Encryption	Choose the WPA2 encryption standard. A WPA encryption standard must be specified if you have enabled WPA policy.
Auth Key Mgmt	Choose the rekeying mechanism from the following options: • 802.1X • FT + 802.1X • PSK: You must specify the PSK format and a preshared key • Cisco Centralized Key Management: You must specify a Cisco Centralized Key Management Timestamp Tolerance value • 802.1X + Cisco Centralized Key Management: You must specify a Cisco Centralized Key Management Timestamp Tolerance value • FT + 802.1X + Cisco Centralized Key Management: You must specify a Cisco Centralized Key Management Timestamp Tolerance value

Parameters	Description
Static WEP	
Key Size	Choose the key size from the following options: • 40 bits • 104 bits
Key Index	Choose a key index from 1 to 4. One unique WEP key index can be applied to each WLAN. As there are only four WEP key indexes, only four WLANs can be configured for static WEP Layer2 encryption.
Key Format	Choose the encryption key format as either ASCII or HEX.
Encryption Key	Enter an encryption key that is 13 characters long.
Static WEP + 802.1X	
Key Size	Choose the key size from the following options: • 40 bits • 104 bits
Key Index	Choose a key index from 1 to 4. One unique WEP key index can be applied to each WLAN. As there are only four WEP key indexes, only four WLANs can be configured for static WEP Layer2 encryption.
Key Format	Choose the encryption key format as either ASCII or HEX.
Encryption Key	Enter an encryption key that is 13 characters long.
WEP Key Size	Choose from the following options: • None • 40 bits • 104 bits

Step 5 Click **Save & Apply to Device**.

Configuring Multi-Preshared Key (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id ssid* **Example:** `Device(config)# wlan mywlan 1 SSID_name`	Configures WLAN and SSID.
Step 3	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 4	**security wpa akm psk** **Example:** `Device(config-wlan)# security wpa akm psk`	Configures PSK.
Step 5	**security wpa wpa2 mpsk** **Example:** `Device(config-wlan)# security wpa wpa2 mpsk`	Configures multi-PSK.
Step 6	**priority** *priority_value* **set-key** {**ascii** [**0** | **8**] *pre-shared-key* | **hex** [**0** | **8**] *pre-shared-key*} **Example:** `Device(config-mpsk)# priority 0 set-key ascii 0 deadbeef`	Configures PSK priority and all its related passwords. The *priority_value* ranges from 0 to 4. **Note** You need to configure **priority 0** key for multi-PSK.
Step 7	**no shutdown** **Example:** `Device(config-mpsk)# no shutdown`	Enables WLAN.
Step 8	**exit** **Example:** `Device(config-wlan)# exit`	Exits WLAN configuration mode and returns to configuration mode.

	Command or Action	Purpose
Step 9	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying Multi-PSK Configurations

To verify the configuration of a WLAN and a client, use the following command:

```
Device# show wlan id 8
WLAN Profile Name     : wlan_8
================================================
Identifier                                    : 8
Network Name (SSID)                           : ssid_8
Status                                        : Enabled
Broadcast SSID                                : Enabled
Universal AP Admin                            : Disabled
Max Associated Clients per WLAN               : 0
Max Associated Clients per AP per WLAN        : 0
Max Associated Clients per AP Radio per WLAN  : 200
Number of Active Clients                      : 0
CHD per WLAN                                  : Enabled
Multicast Interface                           : Unconfigured
WMM                                           : Allowed
WifiDirect                                    : Invalid
Channel Scan Defer Priority:
  Priority (default)                          : 5
  Priority (default)                          : 6
Scan Defer Time (msecs)                       : 100
Media Stream Multicast-direct                 : Disabled
CCX - AironetIe Support                       : Enabled
CCX - Diagnostics Channel Capability          : Disabled
Peer-to-Peer Blocking Action                  : Disabled
Radio Policy                                  : All
DTIM period for 802.11a radio                 : 1
DTIM period for 802.11b radio                 : 1
Local EAP Authentication                      : Disabled
Mac Filter Authorization list name            : Disabled
Mac Filter Override Authorization list name   : Disabled
Accounting list name                          :
802.1x authentication list name               : Disabled
802.1x authorization list name                : Disabled
Security
    802.11 Authentication                     : Open System
    Static WEP Keys                           : Disabled
    802.1X                                    : Disabled
    Wi-Fi Protected Access (WPA/WPA2/WPA3)    : Enabled
        WPA (SSN IE)                          : Disabled
        WPA2 (RSN IE)                         : Enabled
            MPSK                              : Enabled
            AES Cipher                        : Enabled
            CCMP256 Cipher                    : Disabled
            GCMP128 Cipher                    : Disabled
            GCMP256 Cipher                    : Disabled
        WPA3 (WPA3 IE)                        : Disabled
        Auth Key Management
            802.1x                            : Disabled
            PSK                               : Enabled
```

```
            CCKM                                    : Disabled
            FT dot1x                                : Disabled
            FT PSK                                  : Disabled
            FT SAE                                  : Disabled
            PMF dot1x                               : Disabled
            PMF PSK                                 : Disabled
            SAE                                     : Disabled
            OWE                                     : Disabled
            SUITEB-1X                               : Disabled
            SUITEB192-1X                            : Disabled
    CCKM TSF Tolerance                              : 1000
    FT Support                                      : Adaptive
        FT Reassociation Timeout                    : 20
        FT Over-The-DS mode                         : Enabled
    PMF Support                                     : Disabled
        PMF Association Comeback Timeout            : 1
        PMF SA Query Time                           : 200
    Web Based Authentication                        : Disabled
    Conditional Web Redirect                        : Disabled
    Splash-Page Web Redirect                        : Disabled
    Webauth On-mac-filter Failure                   : Disabled
    Webauth Authentication List Name                : Disabled
    Webauth Authorization List Name                 : Disabled
    Webauth Parameter Map                           : Disabled
    Tkip MIC Countermeasure Hold-down Timer         : 60
Non Cisco WGB                                       : Disabled
Band Select                                         : Enabled
Load Balancing                                      : Disabled
Multicast Buffer                                    : Disabled
Multicast Buffer Size                               : 0
IP Source Guard                                     : Disabled
Assisted-Roaming
    Neighbor List                                   : Disabled
    Prediction List                                 : Disabled
    Dual Band Support                               : Disabled
IEEE 802.11v parameters
    Directed Multicast Service                      : Disabled
    BSS Max Idle                                    : Disabled
        Protected Mode                              : Disabled
    Traffic Filtering Service                       : Disabled
    BSS Transition                                  : Enabled
        Disassociation Imminent                     : Disabled
            Optimised Roaming Timer                 : 40
            Timer                                   : 200
    WNM Sleep Mode                                  : Disabled
802.11ac MU-MIMO                                    : Disabled
802.11ax paramters
    OFDMA Downlink                                  : unknown
    OFDMA Uplink                                    : unknown
    MU-MIMO Downlink                                : unknown
    MU-MIMO Uplink                                  : unknown
    BSS Color                                       : unknown
    Partial BSS Color                               : unknown
    BSS Color Code                                  :
```

To view the WLAN details, use the following command:

```
Device# show run wlan
wlan wlan_8 8 ssid_8
 security wpa psk set-key ascii 0 deadbeef
 no security wpa akm dot1x
 security wpa akm psk
 security wpa wpa2 mpsk
  priority 0 set-key ascii 0 deadbeef
  priority 1 set-key ascii 0 deaddead
```

```
 priority 2 set-key ascii 0 d123d123
 priority 3 set-key hex 0 02345678901234567890123456789012345678901234567890123456789012345678901234

 priority 4 set-key hex 0 12345678901234567890123456789012345678901234567890123456789012345678901234

no shutdown
```