


[Home](#) → [TechLibrary](#) → [Network Director](#) → [Network Director User Guide](#) →

Understanding PSK Authentication

 8-Jan-19

Pre-Shared Key (PSK) is a client authentication method that uses a string of 64 hexadecimal digits, or as a passphrase of 8 to 63 printable ASCII characters, to generate unique encryption keys for each wireless client. PSK is one of two available authentication methods used for WPA and WPA2 encryption on Juniper Networks wireless networks. PSK is not the default authentication method when creating a WLAN Service profile because the other choice, 802.1X authentication, is the standard and is stronger.

 **NOTE** 802.1X and PSK authentication types can be applied simultaneously—clients will use the most secure option that they are capable of using. For more information about 802.1X authentication, see [Understanding the IEEE 802.11 Standard for Wireless Networks](#).

This topic describes:

What Is PSK?

There are two WPA forms of encryption available with Network Director: Wi-Fi Protected Access (WPA) and the newer WPA2. Pre-shared key (PSK), a shared secret method, can be added to either encryption method:

- WPA/WPA2 Enterprise (requires a RADIUS server) and provides coverage for large entities.
- WPA/WPA2 Personal (also known as WPA-PSK) is appropriate for use in most residential and small business settings.

How Does PSK Work?

With PSK, you configure each WLAN node (access points, wireless routers, client adapters, bridges) not with an encryption key, but rather with a string of 64 hexadecimal digits, or as a passphrase of 8 to 63 printable ASCII characters. Using a technology called TKIP (Temporal Key Integrity Protocol), that passphrase, along with the network SSID, is used to generate unique encryption keys for each wireless client. Those encryption keys are constantly changed. When clients connect, the PSK authentication users provide the password to verify whether to allow

them access to a network. As long as the passwords match, a client is granted access to the WLAN.



NOTE You have the option to encrypt the PSK plain-English passphrase.

When Would I Use PSK Authentication?

PSK was designed for home and small office networks that do not require the complexity of an 802.1X authentication server. Some reasons to use PSK authentication are:

- PSK is simple to implement, as opposed to 802.1X authentication, which requires a RADIUS server.
- Your legacy clients might not support 802.1X or the latest WPA2 standard. You can use both WPA/WPA2 and PSK simultaneously to accommodate all clients.

Why Would I not Use PSK Authentication?

Even if you have a small company, there are drawbacks to using PSK authentication. For example:

- If an administrator leaves the company, you should reset the PSK key. This can become tiresome and be skipped.
- If one user is compromised, then all users can be hacked.
- PSK cannot perform machine authentication the way that IEEE 802.1X authentication can.
- Keys tend to become old because they are not dynamically created for users upon login, nor are the keys rotated frequently. You must remember to change the keys and create keys long enough to be a challenge to hackers. PSK is subject to brute force key space search attacks and to dictionary attacks.
- Because WPA2-Personal uses a more advanced encryption type, additional processing power is required to keep the network functioning at full speed. Wireless networks that use legacy hardware for access points and routers can suffer speed reductions when WPA2-Personal is used instead of WPA, especially when several users are connected or a large amount of data is moving through the network. Because WPA2-Personal is a newer standard, firmware upgrades can also be required for some hardware that previously used WPA exclusively.

How Is WPA Encryption Different from WPA-PSK Encryption?

The primary difference between WPA and WPA2-Personal are the encryption ciphers used to secure the network. WPA can use only the encryption cipher Temporal Key Integrity Protocol (TKIP). WPA2-Personal can use TKIP, but because TKIP security keys are less secure, the WPA2 protocol usually uses the Advanced Encryption Standard. AES uses a much more advanced encryption algorithm that cannot be defeated by the tools that overcome TKIP security, making it a much more secure encryption method.

RELATED DOCUMENTATION

- [Understanding the IEEE 802.11 Standard for Wireless Networks](#)
- [Understanding WLAN Service Profiles](#)
- [Creating and Managing a WLAN Service Profile](#)
- [Network Director Documentation home page](#)

[← Previous Page](#)

[Next Page →](#)