Mitel 5634 VoWiFi Migration Guide

58016278

October 2020

Mitel®

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

TRADEMARKS

Parameter Migration and Device Management

To make the upgrade from Mitel 5624 (WH1) to Mitel 5634 (WH2) easier, WH2 supports parameter migration allowing to create user parameter templates from all variants of WH1 and WH2 handsets.

Parameter migration requires the use of the compatible Device Manager. For information about the latest released product version, refer to the Mitel Software Download Center. Read the Release Notes before applying any changes in order to get up-to-date information about the product release.

In most cases, it is possible to replace an WH1 handset with an WH2 of the same variant by creating such a template and applying it to the new handset. This document aims to describe all deviations from this rule.

A few parameters are not suitable to migrate directly from WH1. When non-default values are set for these parameters in WH1, it might be necessary to evaluate how to adapt these changes to WH2. This includes the following:

- **Network** > **General** > **Auto switch network timeout**

Wi-Fi

The Wi-Fi chipset used in WH2 is different from the one used in WH1.

Differences can be visible when a walk-through of the site is done with a connected phone call between the two handsets. Reading the RSSI values at the same spot may show differences and the handover location may be different for the two handsets.

Typically, there are four things that should be evaluated using the tools in the handset:

- Coverage area co-channel interference
- Roaming candidates
- Roaming performance (where and when roaming occurs)
- Voice quality in walk and talk test

This can be done by measurement only and by listening to real calls.

Some older Wi-Fi features that are supported by WH1 are no longer supported by WH2. The following paragraphs describe the most important differences between the Wi-Fi implementations.

802.11ac

WH2 supports 802.11ac and uses it whenever supported by the infrastructure. WH1 does not support 802.11ac but does not have any problems coexisting with 802.11ac devices. It is therefore recommended to enable 802.11ac for SSID used by WH2 for both pure WH2 installations and mixed WH1/WH2 installations.

802.11n

During the early years of WH1, it was possible to disable 802.11n due to compatibility issues by setting the parameter **802.11 Protocol** to either **802.11b/g** or **802.11a**. WH2 has not similar compatibility issues with modern infrastructures so the parameter has been removed and now it is possible to select which frequency band should be used (2.4GHz or 5 GHz). The handset uses 802.11ac or 802.11n if available in the infrastructure.

Transmission Power

It is not possible to set a fixed transmission power in WH2. Transmission power is controlled by the infrastructure using 802.11d and 802.11h.

WEP

WEP is perceived deprecated due to security weaknesses and is therefore not recommended to be used in any installation. WEP encryption has been replaced by WPA and WPA2, where the latter is preferred due to its stronger encryption, authentication, and key management strategies for wireless data and system security.

WPA is now deprecated and not allowed to be used in any new products as a stand-alone encryption. For older devices that do not support WPA2, it is recommended to use WPA Mixed Mode (WPA + WPA2). This mode allows newer devices to use stronger WPA2 AES-based CCMP encryption, while still allowing older devices to connect with older WPA TKIP secure protocol.

A-MPDU Packet Aggregation

During interoperability testing there has been issues with the Aruba controllers when the A-MPDU aggregation was enabled in the handset. Therefore, it is recommended to set this parameter to **Off** when connecting to Aruba Wi-Fi and **On** when connecting to other networks.

EAP-FAST

The EAP-FAST method is not supported in WH2.

To deploy WH2 to an existing WH1 installation, at least one of the security methods supported by WH2 must be configured. That is, for installations where only EAP-FAST is enabled, a new method needs to be configured on the existing SSID, or a new separate SSID for WH2 needs to be created.

Advanced Authentication Options

The **Advanced** option for Wi-Fi authentication is no longer available in WH2. Any supported authentication methods should be possible to be configured without the **Advanced** option, which was needlessly adding complexity to the configuration process.

802.11w

Protected management frames (802.11w) are supported and are enabled whenever supported by the infrastructure.

Since WH1 does not support but can coexist with 802.11w clients, it is possible to enable optional 802.11w support in mixed WH1/WH2 installations.

Roaming and Scanning

In WH1, the **Roaming methodology** parameter can be set to **System aided roaming** for infrastructures such as Extricom, which aim to control the roaming process. In WH2, this parameter has been removed since the normal roaming method can be used for all types of infrastructures.

Number of Enabled Channels and 802.11k

When many channels are enabled and have to be scanned before each roam, there is always a risk that the audio quality is affected. This is especially true if many DFS channels are enabled. The longer the handset is scanning each channel, the greater the likelihood that an AP is found, but this also affects sound quality negatively.

A new option, **802.11k** has been added to the available options in the **5 GHz channels** parameter. When it is selected, the handset uses the 802.11k neighbor lists received from the AP to choose which channels to scan during the roaming process. It allows AP deployments where more channels are used without decreasing the roaming performance. The handset roaming performance of course is highly dependent on receiving correct neighbor information from the infrastructure. If the handset fails to find a suitable roaming candidate in the neighbor list, it might

perform a scan of all channels (that is, all 5 GHz channels allowed in the current regulatory domain).

Fast Roaming Methods

The preferred fast roaming method in WH2 is 802.11r Fast Transition.

Opportunistic key caching (OKC, also known as Proactive key caching) is still supported and is used when 802.11r is disabled either in the system or the handset.

PMKSA-Caching is supported in WH2. When this option is selected, OKC is automatically disabled.

For existing WH1 installations where both OKC and PMKSA caching are used, it is recommended to use 802.11r Fast Transition from WH2 and create a single mobility domain for all the controllers.

In case 802.11r is not supported by the infrastructure, the best alternative is to enable PMKSA caching in the WH2 handsets if roaming between controllers is more frequent than roaming within a controller. If intra controller roaming is the most common case, OKC should be configured.

CCKM is not supported in WH2. To deploy the WH2 to an existing WH1 installation where CCKM is used, at least one of the key management methods supported by WH2 must be enabled as well. This can be done either on the existing SSID or on a new separate SSID for WH2.

CCX

Cisco Compatible Extension (CCX) is not supported in WH2. This means that for example, TSPEC setup, TX power, and channel limitations might work differently in WH2 than in WH1 when connected to Cisco Wi-Fi infrastructure.

Power Save Mode

The option to disable U-APSD power save mode and use active mode during calls has been removed from WH2. U-APSD mode is expected to work well with all currently available infrastructures and disabling it would only result in deteriorating call time performance.

TSPEC Behavior

TSPEC configuration mismatches are handled differently in WH1 and WH2. In case of WH2, make sure that the handset parameter **TSPEC Call Admission Control** matches the system configuration.

If the system (AP) side is configured to mandatory TSPEC on AC Voice but TSPEC is set to **Off** in the handset, an WH1 will adapt and send the voice traffic in AC Best effort. Consequently, the configuration mismatch can go undetected and result in degraded voice quality since the voice traffic is sent over the air with lower priority.

In the same scenario, an WH2 refrains from connecting to any call until the configuration mismatch is corrected either by disabling TSPEC on the system side or setting the handset parameter to

Automatic or **Required**. In this case, information about the detected problem can be found in the Admin menu of the handset in **Device info** → **WLAN info**.

An WH2 with a software version earlier than 2.2.8 does not support TSPEC for AC Video, which is used for SIP signalling. To resolve this issue, either upgrade the handset software or disable TSPEC for video in the system.

Aruba 800 Controller Compatibility

WH1 contained a small adjustment for a problem with traffic prioritization in an old Aruba controller. This is no longer available in WH2.

Default Gateway

The WH2 handset requires a default gateway to be configured, either statically or using DHCP. The main reason for this is that the default gateway is used to check for network connectivity issues. Since it is possible to deploy the WH1 without a default gateway, it is important to ensure that this condition is met when introducing the WH2 to an existing WH1 deployment.

Telephony

Voice Codecs

WH2 supports the OPUS wideband codec. In addition, all codecs supported by WH1 are still supported.

Selecting OPUS as the preferred codec for WH2 in a mixed WH1/WH2 environment is acceptable, as a common supported codec is selected for calls between WH1 and WH2.

H.323

WH2 is a SIP device and it does not support H.323.

For existing WH1 H.323 deployments using Innovaphone PBXes, both H.323 and SIP are supported by the PBX and it is possible to use SIP for WH2 and H.323 for WH1.

Location

The handset is compatible with Cisco Mobility Service Engine (MSE) and AiRISTA Flow Real Time Location System (RTLS) which give a more accurate location than AP Location. For details on location services supported on particular handset variants, refer to the product's Data Sheet.

Battery Saving Options

In WH2 the default battery saving setting is **Black also in call**, which is recommended for extending the battery life. By contrast, in WH1 the default setting is **Information**.

If the screen saver is set to **Black also in call**, no information is shown on the screen both when the handset is not in use and during the ongoing call.

Logging and Troubleshooting

The PC side application PDL is no longer required for retrieving logs from WH2. If logs must be collected and sent to R&D for analysis, an appropriate log level can be enabled either in the handset admin GUI or through Device Management.

The handset can be configured to send logs to either an SFTP server or make them available to be retrieved by connecting the handset to a Windows PC as a USB drive using a DP1 desktop programmer. These files are encrypted and can only be decrypted by R&D.

As in WH1, it is possible to configure the handset to send some clear text logs to a remote syslog server.

The web server that was available in WH1 has been removed from WH2. The syslog, SFTP, and USB drive features provide similar functionality.

In contrast with WH1, logging in to the handset via telnet is not possible in WH2 to improve the security of the device.

Software Download

The software image for WH2 is larger than the one for WH1. It means that it takes longer to upload the image to device management and download to the handset.

Software upgrade using TFTP is no longer supported.

Document History

Version	Date	Description
E	08 June 2020	**Update:** General update and editorial changes in the document. Created a note in WEP. Update in Parameter Migration and Device Management. Minor changes in 802.11n. Update in Location.
D	22 May 2020	**Update:** The 2.11 Fast Roaming Methods has been updated with the latest product version information.
C	13 May 2020	**New:** TSPEC Behavior Default Gateway
B	28 February 2020	The Parameter Migration and Device Management section has been updated with the latest product version information.
A	14 December 2019	First revision.

Abbreviations and Glossary

AP	Access Point
CCX	Cisco Compatible Extension
DHCP	Dynamic Host Configuration Protocol A protocol for automating the configuration of computers and handsets that use TCP/IP.
DFS	Dynamic Frequency Selection
EAP-FAST	EAP-Flexible Authentication via Secure Tunneling
OKC	Opportunistic key caching (also known as Proactive key caching)
PBX	Private Branch Exchange A telephone system within an enterprise that switches calls between local lines, and allows all users to share a certain number of external lines. Also referred to as Call Manager.
PMKSA	Pairwise Master Key Security Association
RSSI	Received Signal Strength Indication
TSpec	Traffic Specification
TFTP	Trivial File Transfer Protocol
U-APSD	Unscheduled Automatic Power Save Delivery It is also referred to as WMM-PS.
Wi-Fi	A family of radio technologies that is commonly used for implementing a WLAN. Used generically when referring to any type of IEEE 802.11 network.
WEP	Wired Equivalent Privacy
WPA/WPA2	WPA and WPA2 mixed mode WPA/WPA2 mixed mode operation permits the coexistence of WPA and WPA2 clients on a common SSID.