SmartPTT 9.14.5

Customer Release Notes

December 2024

Elcomplus Inc.

MOTOTRBO Updates

Compliance with the new firmware and software releases.

M2024.02 SUPPORT

SmartPTT supports MOTOTRBO release M2024.02 released in Summer 2024.

M2024.01 SUPPORT

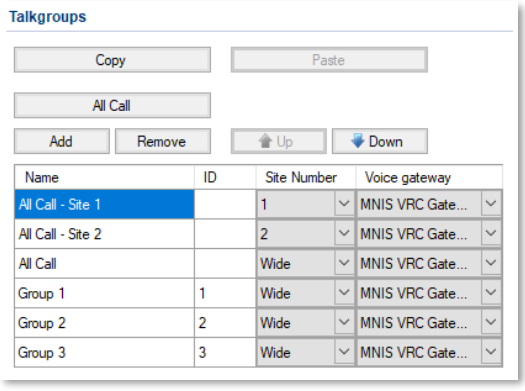
SmartPTT supports MOTOTRBO release M2024.01 released in February 2024.

CAPACITY MAX 750 SITES

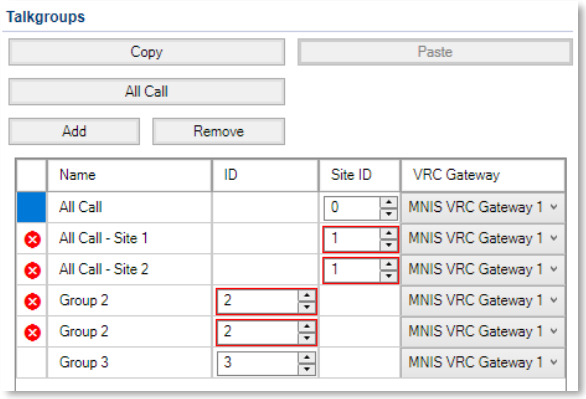
SmartPTT supports an increased range of Site IDs in Capacity Max. Previously they ranged from 1 to 255. Now they range from 1 to 900.

Additionally, SmartPTT enhances the view and setup of talkgroup, single-site, multisite, and system-wide call destinations. Please find those changes illustrated below.

Before:



After:



CONNECT PLUS SUPPORT

SmartPTT keeps supporting MOTOTRBO Connect Plus systems. The only supported MOTOTRBO release for that kind of system is R2.10.5.

Authentication Upgrades

Giant leap to industry-standard authentication solutions.

SmartPTT switches to the industry-standard authentication solutions. Being a Windows-only application, it now supports authentication mechanisms available in that operating system.

With the upgrades, SmartPTT users and distributors gain the following benefits:

- Greater compliance with corporate cyber security requirements. This includes at least password and account policy updates, centralized user account suspension, and password security.
- Reduces SmartPTT user setup expenses.

Please find the upgrades description below.

ACTIVE DIRECTORY SUPPORT

SmartPTT introduces authentication of Active Directory users a.k.a. “domain users”. For authentication, the product uses Windows-specific Lightweight Directory Access Protocol (LDAP). Authenticated users are automatically added to the list of user accounts.

⚠ Authentication is performed using login and password. No Kerberos or other advanced authentication solutions are implemented.

For authentication, users require to be included in specific user groups. Domain name and user groups are configured during the product installation and upgrade. Setup modification is available only by re-installing the product.

All users and user groups must belong to the same domain. All users must be direct members of the configured user groups. No users from other domains are authenticated. No user group nesting is supported.

LOCAL USERS AND GROUPS

SmartPTT introduces authentication of local Windows users created on the SmartPTT server host computer. Authenticated users are automatically added to the list of user accounts.

⚠ Authentication is performed using login and password. No Kerberos or other advanced authentication solutions are implemented.

For authentication, users require to be included in specific user groups. User groups are configured during the product installation and upgrade. Setup modification is available only by re-installing the product.

SERVER-ONLY AUTHORIZATION MODE

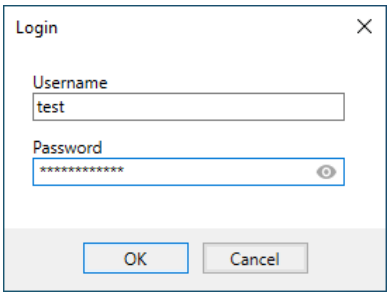
SmartPTT provides the ability to set up server-only (centralized) authentication. In this mode, SmartPTT does **not** authenticate users in the Dispatcher App (as it did before), and requests server to confirm/reject user authentication.

The mode is optional in SmartPTT. It is configured during the product installation/upgrade and can be changed only by the modification of the installed product.

As a result, customers get an **increased cyber security compliance** if they choose SmartPTT.

PASSWORD-PROTECTED CONFIGURATOR

SmartPTT introduces password protection for the Server Configurator. Protection is available only if domain or local authentication is configured. Only System Admins can log on to it.



AUTHENTICATION SETUP SIMPLIFICATIONS

With local/domain authentication configured, SmartPTT eliminates the need to set up “associations” of user accounts in Dispatcher App an on the Server. Instead, SmartPTT users the same credentials to authenticate in the Dispatcher App and on the Server.

Authorization Upgrades

Significant ease of permissions and restrictions management.

SmartPTT introduces significant upgrades related to user authorization, i.e. permissions grant/revoke. Powered with authentication upgrades, they significantly enhance setup experience.

With the upgrades, SmartPTT users and distributors gain the following benefits:

- Significantly reduced user setup and first start expenses.
- Greater flexibility for operators working in different locations/sites.

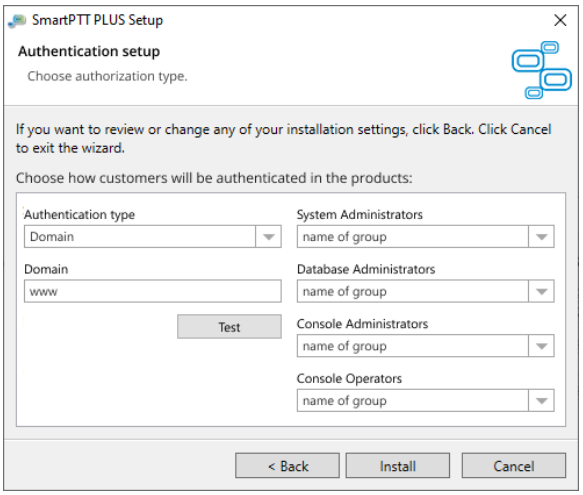
Please find the upgrades description below.

USER ROLES

SmartPTT introduces role-based access to the product. It is available if domain or local user authentication is configured. Currently, SmartPTT supports four user roles:

- System Admins can log on to the Configurator for system setup purposes.
- Console Admins can log on to the Dispatcher App for administration procedures.
- Console Operators can log on to the Dispatcher App for permitted user operations.
- Database Admins, a subset of System Admins, can log on to the Configurator to create and upgrade the product databases.

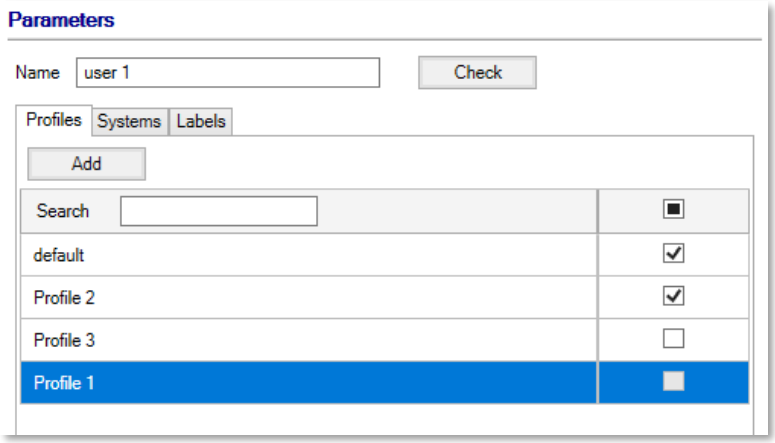
Every user role is related to a local/domain user group.



Additionally, you can add the same user to multiple user groups. At this, SmartPTT grants such users with privileges of all those roles.

PROFILE SELECT

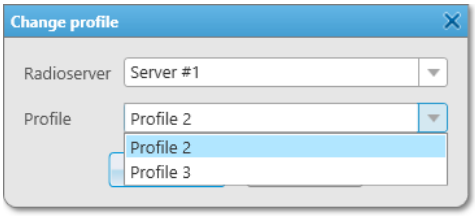
SmartPTT re-introduces the profile selection capability. Previous implementation was removed in 9.7 due to security concerns. No alternative was available in the product until the current release.



List of allowed profiles is configured using the Configurator and on a per-user basis. After that, logged on users will have one of the following profiles assigned:

- Random profile if logged on for the first time,
- Profile used during the last session.

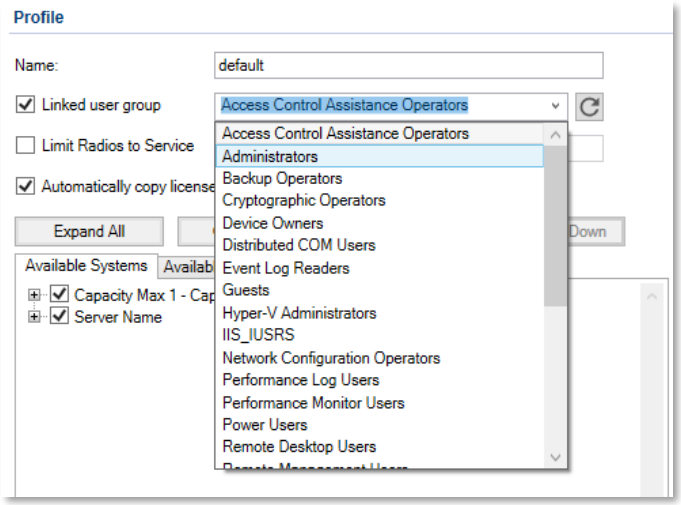
Users can change their profile at any time during their work. If they log on to the system with multiple servers, they will be able to change their profiles individually on every server.



If users have no available profiles, they will have no access to system resources and features. This is a significant difference from the previous releases. To preserve the previous behavior, SmartPTT created a default profile with all the permissions enabled. If undesired, the profile can be removed.

AUTOMATIC PROFILE ASSIGNMENT

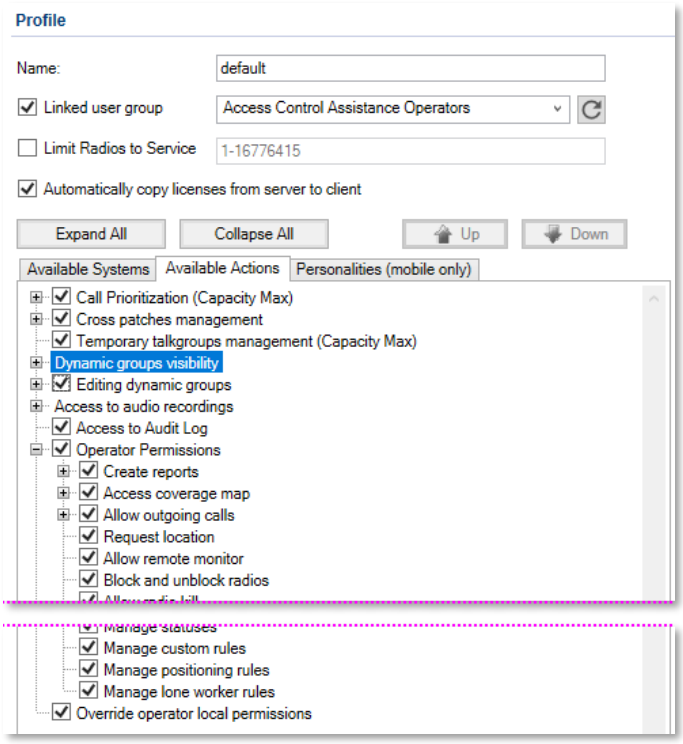
SmartPTT introduces the ability to assign profiles automatically to logged on users. It is available only if domain or local user authentication is configured.



To enable the feature, additional user groups must be created in the Active Directory (or locally). Those user groups must be linked to SmartPTT profiles, and then users must be added to those groups. Upon the logon, SmartPTT will check user membership in those groups and, if confirmed, it will mark the profile as available to be selected by user.

OPERATOR RIGHTS IN PROFILES

SmartPTT introduces new user permissions in profiles. They are the same as permissions collectively known as “Operator Rights”. Previously, they were available only in Dispatcher Apps. Now, all of them can be configured in Profiles, on the Server.



The permissions include fine access to user features like GPS triggers, geofencing, reports, conference calls etc. Additionally, SmartPTT provides the ability to set priority between profile permissions and Operator Rights if they are different.

Audio System Upgrades

Notable changes towards better audio quality.

ENHANCED ACCESSORY SUPPORT

SmartPTT provides better support for audio and dispatch accessories. This includes desktop microphones, speakers, headsets, footswitches etc.

Enhancements are as follows:

- Correct device recognition upon the USB port change. You can re-plug your accessory if your current USP port is malfunctioning or broken.
- Correct device recognition upon Windows updates. You can plan your Windows updates without worrying about SmartPTT re-configuration.

⚠ SmartPTT team recommends disabling automatic OS updates to avoid unexpected and undesired downtime of the product.

As a result, SmartPTT users and distributors **reduce their maintenance expenses** if choose to work with SmartPTT.

SPEAKER ROLE UPDATES

SmartPTT introduces the revised role model for audio outputs (speakers). This includes Select Speaker, Unselect Speaker, Emergency Speaker, and System Speaker.

Moreover, SmartPTT makes Main Audio Device[1] optional. Now you can transform it from stereo speaker to mono speaker or remove it at all.

As a result, SmartPTT users and distributors get a **greater audio quality** in the product, with less amount of “parasite” audio and a smaller number of audio routing issues.

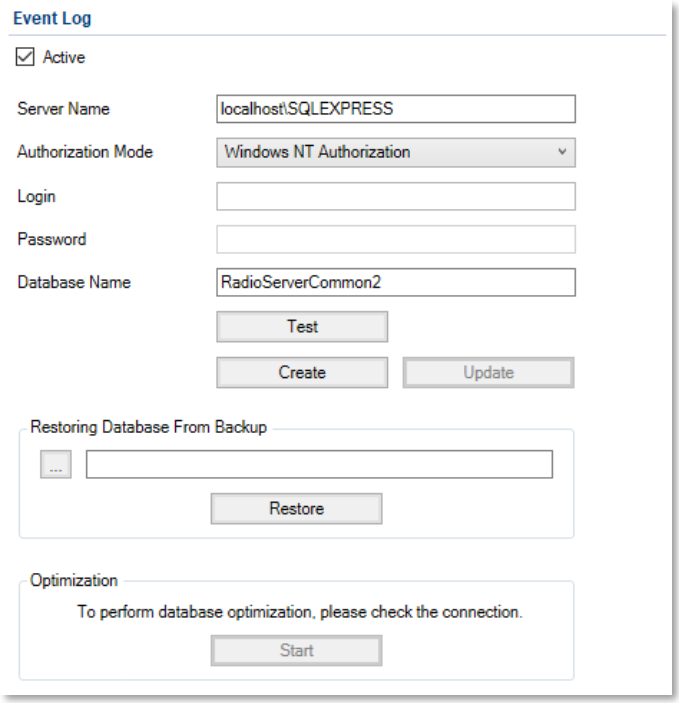
[1] Main Audio Device was a non-removable set of audio outputs which configuration repeats default audio device in the operating system. Having that device created complications in planning and implementing straightforward audio logic for SmartPTT users.

Other Upgrades

Right decisions on the way to quality, security, and usability.

MANUAL-ONLY DATABASE UPGRADES

SmartPTT introduces manual-only database creation and upgrade. It is available only if domain or local user authentication is configured.



Previously, database management activity did not require extra privileges in SmartPTT. This resulted in complications with end-user IT departments. Currently, only users with the Database Admin role can do create new and upgrade existing databases. The upgrade implies creating new tables, modifying their existing structure, adding indexes.

SILENT INSTALL COMMANDS

SmartPTT provides the ability to install SmartPTT using a command-line interface. For that, customers should call the SmartPTT distribution package (executable file) with specific attributes.

Using that approach, customers may implement controllable product upgrades using Task Schedulers or corporate package managers.

As a result, customers get significant **maintenance expenses reductions** if they choose SmartPTT.

AUDIT LOG

⚠ SmartPTT team is not responsible for regional and other limitations of the functionality in SmartPTT PLUS (if any). If you have such limitations, please contain Motorola representatives in your region.

SmartPTT introduces Audit Log. It is a centralized (managed by server) storage of dispatcher logon and logoff attempts. Additionally, the Profile Select events are logged there.

Audit Log is available only in the SmartPTT API. The data are provided upon the HTTP request using the session token received upon the successful authorization via API. The response is provided in the JSON file. For the API description, submit a request to your SmartPTT sales manager.

CHANNEL (FREQUENCY) SELECT LOGGING

Starting the release, SmartPTT logs the Channel/Frequency Select event into the server and dispatcher event logs. With that, users will be able to correlate their voice calls with channels on which this was made.

MISCELLANEOUS

- Enhanced behavior of the Event Log. Now, available entries do **not** depend on resources available currently in profiles.
- Renaming is made for the tab previously known as “Network Configuration”. Now, it is named “Monitoring”.
- Profiles get a new parameter named “Use for anonymous connections”. If selected, the profile selection functionality becomes available for the SmartPTT mode of operation when the Server does not require user credentials.

> ⚠ Do not enable the parameter if server authentication is enabled.

Contact Us

SmartPTT is developed and released by Elcomplus Inc., a Florida corporation (US). For more information on the product, visit https://smartptt.com/

For more information about the product setup and use, see https://smartptt.com/wiki/

TECHNICAL SUPPORT

To contact a technical support engineer, use the following information:

- Email: support@smartptt.com
- Web request: https://support.smartptt.com/hc/en-us/requests/new
- Phone: +1-786-362-5525

SALES & MARKETING

If you have any questions related to the product sales, email to sales@smartptt.com

If you have any questions related to the product marketing, email to marketing@smartptt.com

FEEDBACK & PROPOSALS

For any feedback on the product (including feedback on customer documentation), please email to feedback@smartptt.com