SmartPTT PLUS 9.14

Customer Release Notes

MOTOTRBO

Use the newest MOTOTRBO release with the newest SmartPTT.

New release of SmartPTT is available together with the new MOTOTRBO release. New supported version in M2024.01.

INCREASED SITE ID RANGE

M2024.01 introduces an increased range of Site IDs supported in Capacity Max. Now, Site ID ranges from 1 to 900.

In addition to the range increase, SmartPTT introduces usability enhancements for that configuration:

- **Numeric fields**. Now you know what kind of input is required in the Site ID and Talkgroup ID. Moreover, numeric fields are easier to specify.

- **Error indication**. Now you can easily detect invalid values. You have red (error) outline for the invalid value and error icon (❌) on the left of the invalid entry. Moreover, if you point to the icon, you will see what fields contain errors.

- **Sortable table**. Now you can sort table entries by any column. This includes a column with error.

CONNECT PLUS PRESERVATION

SmartPTT keeps providing the support of the wireline interface to Connect Plus systems.

It supports only the latest available MOTOTRBO firmware for Connect Plus (R2.10.5).

Windows Users and Groups

Use Active Directory or local computer accounts in SmartPTT.

SmartPTT introduces the ability to use Windows users accounts and user groups instead of its own accounts. It supports the following user types:

- Domain users and groups, created in the corporate Active Directory.

- Local users and groups, created on the server computer.

SmartPTT uses Lightweight Directory Access Protocol (LDAP) to access Active Directory users and groups.
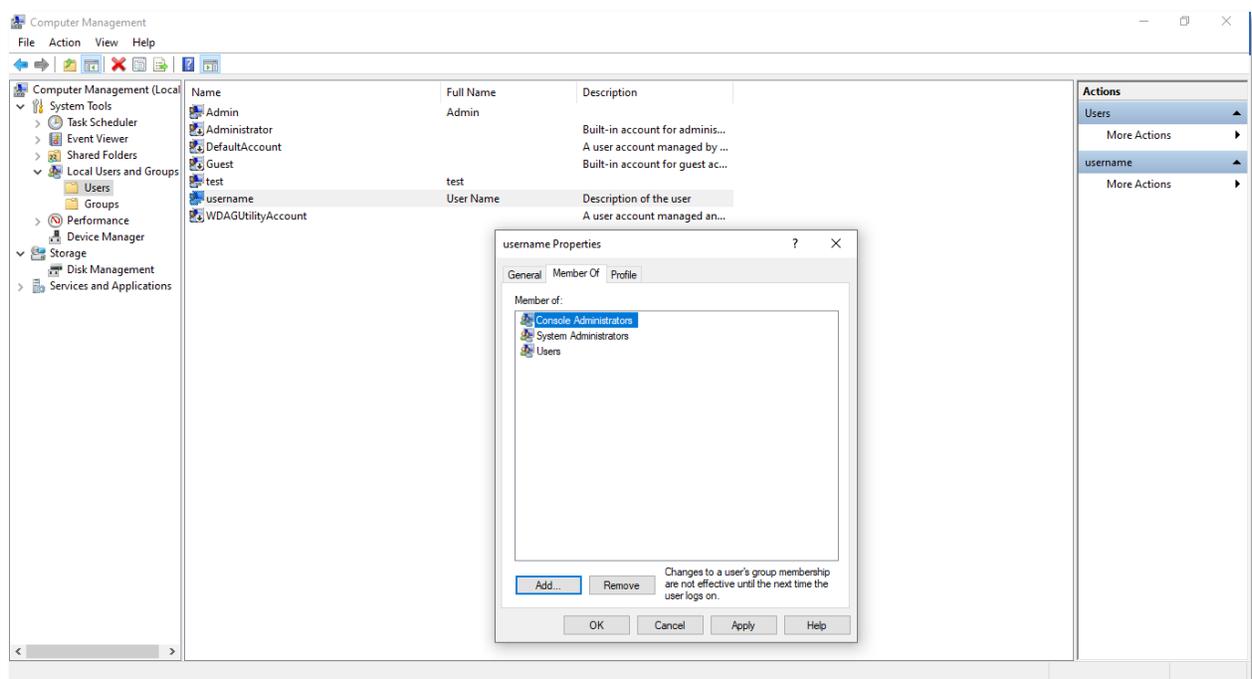
Transition to Windows users and groups opens the following opportunities:

- Users apply the same login and password for all tools in the company, including SmartPTT.

- Representatives of IT/cybersecurity departments have full control over the user access to all tools in the company, including SmartPTT. Also, they change and apply password policies to them instantly.

- Business gets increased cybersecurity of the solutions. Also, they reduce maintenance expenses on interaction and mutual control between account department and SmartPTT Admins.

If you are not yet ready to switch to the new account type, you can keep using the existing approach. However, please consider other benefits of switching to Windows users and groups.

USER ROLES

SmartPTT introduces four user roles in the SmartPTT product:

- **System Admins**. Group of users who can access the Configurator.

- **Console Admins**. Group of users who can access the Dispatcher App for audio configuration, server connection, and other administrative/supervisory purposes.

- **Console Operators**. Groups of primary Dispatcher application users who receive and transmit calls, tracks subscribers on maps, handle emergency cases, etc.

- **Database Admins**. Subset of Administrators who can create and upgrade databases via the Configurator and Dispatcher App.

Each of those roles is related to a user group in the Active Directory or Server computer.
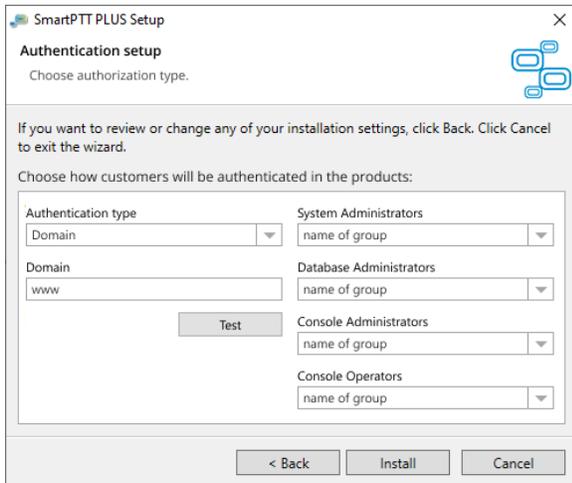
Depending on your policies, you can do this:

- Associate the same user group with multiple roles to eliminate a role that you do not need in the product.

- Add users to multiple groups to assign them with unique roles.

SEAMLESS AUTHENTICATION

With Windows users and groups, SmartPTT eliminates the need to associate Dispatcher App accounts with server accounts. Instead, both Dispatcher App and server will validate the credentials independently.

1. When you log in to the Dispatcher App, it validates your credentials by communicating with the local account storage or active directory.

2. If valid, it forwards the same credentials to all connected SmartPTT servers.

3. If valid, users get access to those servers immediately.

This approach eliminates a great amount of work to be performed in each Dispatcher App. Moreover, it is enhanced with the Automatic Profile Assignment functionality. For details, see Automatic Profile Assignment on page 9.

CONFIGURATOR ACCESS

If Windows users and groups are used, SmartPTT enables password protection for the Configurator, an application with access to the critical parameters (IP addresses, API keys, Secure Keys, etc.).
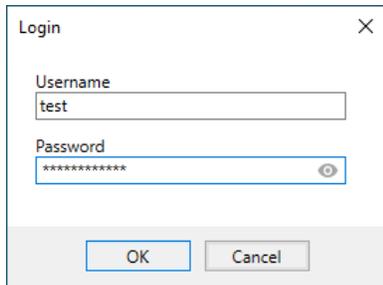
To access it, users must have the role of System Admins and belong to the corresponding user group.

Profile Upgrades

Select the right profile for the right time. Get the right profile at the very first start.

SmartPTT provides significant upgrades of its Profiles system. The upgrade includes Profile Select, Automatic Profile Assignment, and Extended Permissions.

PROFILE SELECT

SmartPTT introduces the ability to select a profile for Dispatcher App users and Web Console operators. Similar functionality was available in SmartPTT 9.5 and earlier. However, the current implementation is more obvious, secure, and flexible.

The functionality opens following opportunities:

- Users select a proper set of resources and capabilities for their current situation. They do not waste their time to mute unnecessary resources and filter out unnecessary log entries.

- SmartPTT Admins save their time on profile change for users. Now, users themselves decide what and where to use.

- Business saves the time on the time operator need to begin the work in the target location.
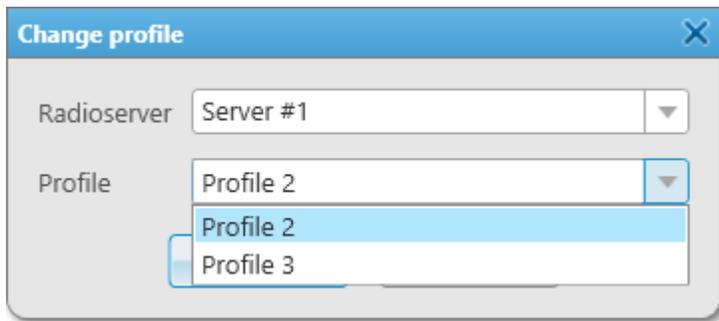
The functionality is **unavailable** for the following user types:

- Mobile App users (use Personalities instead).

- API Applications.

AUTOMATIC PROFILE ASSIGNMENT

If Windows users and groups are used, SmartPTT allows you to link a profile to a user group. This might be an additional user group, not the one related to a user role. If you add SmartPTT user to that group, corresponding profile will become automatically available to it.
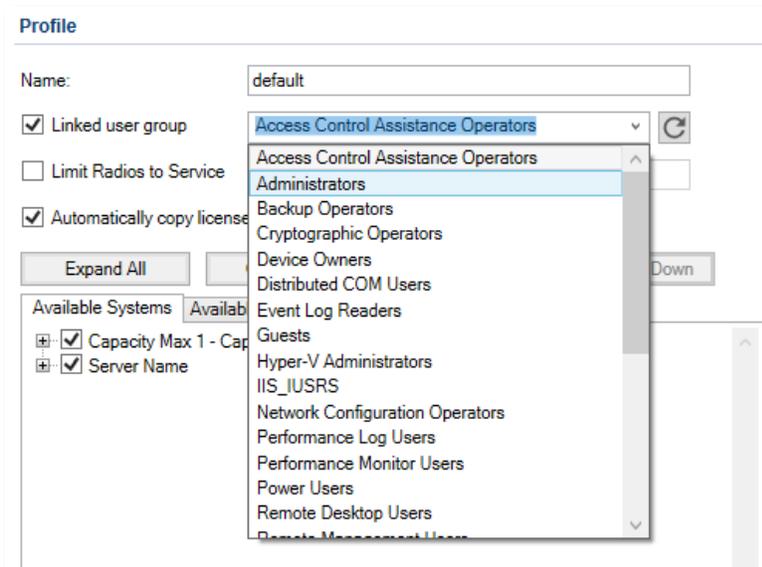
The functionality opens following opportunities:

- SmartPTT Admins do not spend any more time on adding new users. They only inform account managers to which group users must be added.

- Business saves a great amount of time for their SmartPTT Admins and prevents user passwords being exposed to them.

ALL OPERATOR RIGHTS IN PROFILES

SmartPTT introduces a copy of all Operator Rights (permissions configured on per-user basis in individual Dispatcher Apps) in Profiles. All those permissions are grouped under the dedicated node, for easier recognition. And, as always, the functionality is supported on per-server basis (when possible).

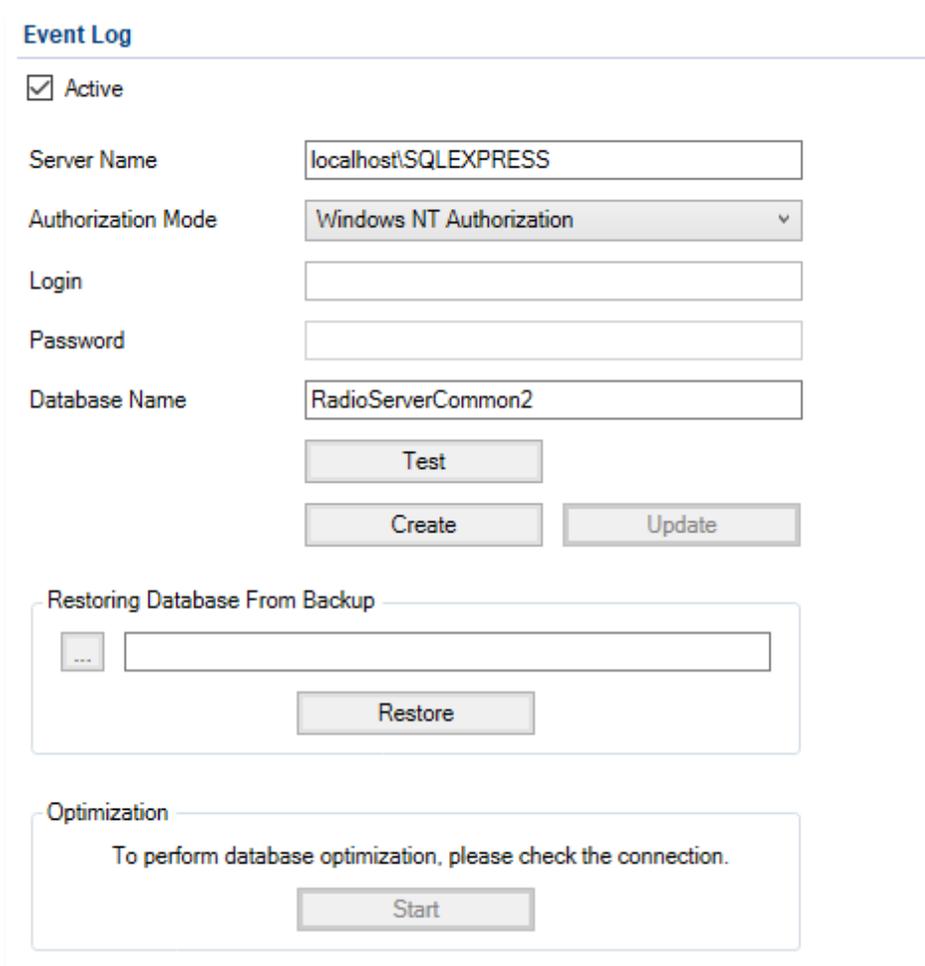The functionality opens following opportunities:

- SmartPTT Admins can manage all the possible user permissions from one place. There is no need to access Dispatcher App remotely or in person. Also, they can manage conflicts between Operator Rights and Profiles by enabling/disabling priority of profile permissions.

- Business saves admin's time on performing their duties.

Permissions are not yet applicable in Web Console.

Manual Database Update

Ensure your data availability when updating your SmartPTT.

Due to data safety concerns, SmartPTT enforces manual upgrades of the database structure and data.

If Windows users and groups are used, the upgrade permission will be available only to the following users:

- Those who combine the roles of System Admins and Database Admins. These users can upgrade Server databases.

- Those who combine the roles of Supervisor and Database Admins. These users can upgrade the Dispatcher App database.

The functionality opens following opportunities:

- Surety that software upgrade will not result in data accessibility failures.

- Control by personnel who are authorized to perform database upgrades and who do not.

Audit Log API

Centralized log of user sessions and selected actions.

SmartPTT introduces a centralized Audit Log. Currently, logged data include this:

- Event types: logons, logoffs, and failed logon attempts.

- Event parameters: timestamp, source IP address, username).

Information is retrievable only with the Audit Log API[1]. The API itself uses REST-like requests with configurable parameters. Responses provided in the form of JSON messages. For API testing, please use Postman or other applications that support WebSocket (authorization) and REST technologies.

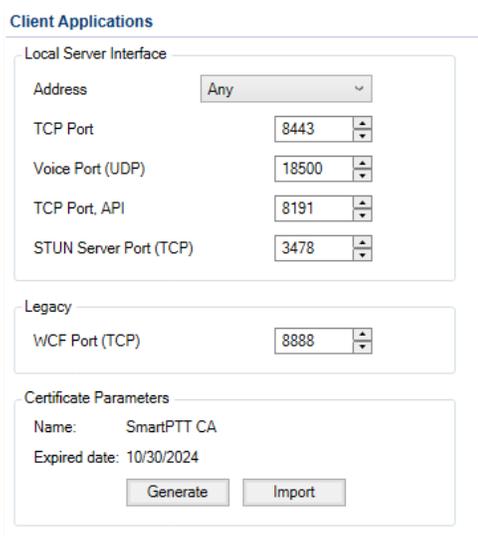To request API docs, submit a request to the SmartPTT Support Center.

⚠   SmartPTT is not responsible for possible regional and other limitations of the SmartPTT API functionality. For such questions, please contact Motorola Solutions in your region.

---

[1] Audit Log API is a part of paid functionality of SmartPTT API.

Miscellaneous

Enhancements available in the Product.

- Enhanced behavior of the Event Log. Now, available entries do **not** depend on resources available currently in profiles.

- Renaming is performed for the section previously known as "Clients Connection". Now, parameter and section names have clearer explanation of their role in the product.

- 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/products/smartptt-plus/

TECHNICAL SUPPORT

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

- Email: support@smartptt.com

- Web form: 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