VOSS Automate

Upgrade Notes for VOSS Automate 21.4 Patch Bundle 1

Release 21.4-PB1

Mar 26, 2024

Contents

Upgrade Overview 2

VOSS-1100: Webex Room Onboarding 2

VOSS-1122: Write to Active Directory as part of Quick Add/Subscriber from profile onboarding workflow 3

VOSS-1124: Support Microsoft dial plan elements in generic dial plan 4

EKB-5746: Enable MS Proxy to communicate over HTTPS 5

Upgrade Overview

In a new release, there are a number of changes that could relate to exposing new features or capabilities in the system. The default out of the box system would expose these. However, on a system where the configuration around the user experience has been applied, this might mean some changes to configured menus, display policies, and so on to expose the new features in your setup.

Where relevant, we have included this information with the feature information to assist in planning for configuration changes as part of the upgrades. This setup could vary.

Important: When upgrading to release 21.4-PB1,

Refer to the detailed steps in the *Method of Procedure (MOP) for 21.4 Patch Bundle 1 Installation*.

VOSS-1100: Webex Room Onboarding

2.1 Introduction

When adding or updating a Webex Workspace new configuration, options have been added to capture the physical Webex RoomOS device details, namely IP Address, Profile and configuration Username/Password. VOSS Automate will then connect to the physical RoomOS device, apply the settings defined in the configuration Profile and then register/activate the device with the Workspace on the Webex Control Hub using the Device Activation Code generated for the specific Workspace.

A reference Device Configuration Profile called "ActivateWebexRoomOSDevice" has been added; this should be cloned down the required hierarchy and customized as required. An option has also been added to test the XML rendering of the Device Configuration Profile.

2.2 Access Profiles

Review the default Provider admin AP for permission examples for the following model types:

- `data/RoomosDeviceConfigurationProfile`
- `view/RenderRoomosDeviceConfigurationProfile`

2.3 Menu Layout

Review the default Provider menu for configuration examples for the following items under Webex App submenu.

- Device Configuration Profiles
- Test Device Configuration Profile Rendering

VOSS-1122: Write to Active Directory as part of Quick Add/Subscriber from profile onboarding workflow

3.1 Introduction

Adds a new option to enable an imported Active Directory user to be updated, using a specified configuration template, during Cisco Quick Add Subscriber and Microsoft Quick Add Subscriber provisioning.

This enables the chosen/auto-provisioned Line value to be written back to Active Directory to any of the user's Telephone Number fields as an example.

3.2 Macros

Several reference macros have been added/updated which can be used in the new configuration template to define which values from Quick Add Subscriber are written back to the user on Active Directory

- `DISPLAY_GET_FIRST_LINE` - Returns the first selected/auto-selected Line
- `DISPLAY_GET_FIRST_LINE_E164` - Returns the E164 number associated to the first selected/auto-selected Line
- `DISPLAY_NAME_GET_FNAME` - Returns the First/Given name from the Quick Add Subscriber page
- `DISPLAY_NAME_GET_LNAME` - Returns the Last/Surname from the Quick Add Subscriber page
- `DISPLAY_GET_USERNAME` - Returns the Username from the Quick Add Subscriber page

3.3 Configuration Template (CFT)

A new configuration template will be added for each LDAP Server, at the same hierarchy level of the LDAP Server, when the **Enable Write Options** checkbox has been enabled on the LDAP Server (`relation/HcsLdapServerREL`) configuration page.

- This new configuration template should be customized to define which fields should be written back to the Active Directory Server for the User.
- This new configuration template must be selected in the field **LDAP Write Back Template** on the LDAP User Sync (`relation/HcsLdapUserSync`) configuration page in order to trigger the write back step during Quick Add Subscriber.

Note: When writing back to Active Directory for the purpose of syncing to Azure AD for Microsoft Teams provisioning, the LDAP Authentication Attribute on the LDAP user sync configuration must be to `userPrincipalName` and the Username mapping on the User Field Mapping page must also be set to `userPrincipalName` for the specific LDAP Server.

VOSS-1124: Support Microsoft dial plan elements in generic dial plan

4.1 Introduction

Adds the ability to push and remove Microsoft Teams dial plan elements using generic dial plan, and includes the following elements:

- Tenant Dial Plan
- SBC Gateways
- PSTN Usage
- Voice Routes
- Voice Routing Policies
- Translation Rules.

4.2 Access Profiles

Review the default ProviderAdminAP for permission examples for the followingnmodel types:

- `view/DP_MaintenanceVIEW`
- `data/DP_DialPlan`
- `data/DP_msteamsonline_CsTenantDialplan`
- `data/DP_msteamsonline_CsOnlinePstnGateway`
- `data/DP_msteamsonline_CsOnlinePstnUsage`
- `data/DP_msteamsonline_CsOnlineVoiceRoute`
- `data/DP_msteamsonline_CsOnlineVoiceRoutingPolicy`
- `data/DP_msteamsonline_CsTeamsTranslationRule`

4.3 Menu Layout

Review the default ProviderMenu for configuration examples for the following items under the Dial Plan Management Tool submenu:

- Dial Plan Maintenance
- Dial Plans
- Tenant Dialplan
- SBC Gateways
- PSTN Usages
- Voice Routes
- Voice Routing Policies

- Translation Rules

EKB-5746: Enable MS Proxy to communicate over HTTPS

Upon upgrade to release 21.4-PB1, all communication between VOSS Automate and the Windows PowerShell Proxy will default to HTTPS, requiring existing configurations to be updated.

The port used for secure communication is TCP 5986 instead of TCP 5985 which is used for insecure HTTP.

For existing PowerShell configurations with transport over HTTP, the driver parameter `winrm_transport` can be set to `plaintext` and can be manually added to the `data/MSTeamsOnline` instance to ensure backward compatibility temporarily. If integrating with Exchange Online then the same driver parameter can be added to `data/MSExchangeOnline` temporarily.

Reverting back to insecure communication is only recommended as a temporary measure while the PowerShell Proxy is being configured for secure communication.

Contact VOSS support to assist in the reconfiguration of your winrm driver.