VOSS Automate

Upgrade Notes for VOSS Automate 21.4 Patch Bundle 2

Release 21.4-PB2

Nov 29, 2023

Contents

Upgrade Overview

There are a number of changes in a new release 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-PB2,

Refer to the detailed steps in the *Method of Procedure (MOP) for 21.4 Patch Bundle 2 Installation*.

VOSS-1138: Webex Teams Calling Management - Initial Phase

2.1 Introduction

The information provided here is to assist in planning for configuration changes as part of the upgrades. This setup could vary depending on the functionality you wish to expose and the different roles in the system.

2.2 Webex Customer Account Token

You will need to obtain a new access token for every Webex Customer Account in Automate after upgrading to this release.

2.3 Network Device List

To support some of the new Webex functionality with this release, it is required to have at least one Network Device List created for every Customer that has a Webex Account configured in Automate.

2.4   Data Sync

After upgrading, the following data syncs should be run for all Webex accounts configured in Automate:

- `SyncSparkRolesLicences<CUSTOMER_NAME>`
- `SyncSpark<CUSTOMER_NAME>`

2.5   Access Profiles

A new tool is being introduced, *Webex User Quick Add*. This tool requires permission to the following model:

- `view/WebexTeamsSubscriberQas`

The following model types have been deprecated and should be removed:

- `view/GenerateWebexTeamsUserCsvPerCustomer`
- `data/WebexTeamsManualSteps`

2.6   Menu Layout

The following model types have been deprecated and should be removed:

- `view/GenerateWebexTeamsUserCsvPerCustomer`
- `data/WebexTeamsManualSteps`

The *Webex App* menu group under the *Cisco Subscriber Management* menu has been moved to the top level as *Cisco Webex App*.

A new tool is being introduced, *Webex User Quick Add*, and is located under the *Cisco Webex App* menu.

2.7   Field Display Policy (FDP)

A number of default FDPs have been added or modified. Please review the FDPs for changes that may need to be incorporated into the customized versions if the default versions have been cloned down and modified. The FDPs may need to be applied to the menu item as per the Menu Layout section.

- `SubscriberAdvanced-SiteFDP`
- `SubscriberAdvancedDefault`
- `SubscriberAdvancedDefault-Restricted`
- `BusinessAdminWebexTeamsUserFDP`
- `SparkCustomerFDP`
- `SparkUserFDP`

VOSS-1144: Webex endpoint scheduled configuration reset to baseline

3.1 Introduction

Adds the ability to initiate a reset of registered Webex RoomOS devices to a predefined baseline configuration state, using a template. This feature also includes a workflow, which can then be added to a schedule to initiate the reset on a timed basis, for example, daily.

3.2 Access Profiles

Review the default ProviderAdminAP for permission examples for the following model types:

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

3.3 Menu Layout

Review the default ProviderMenu for configuration examples for the following items.

- Reset Devices to Baseline
- Device Configuration Profiles
- Test Device Configuration Profile Rendering

3.4 Provisioning Workflow

A new workflow has been added that can be used in a schedule to initiate the reset of devices.

- `WebexDeviceRefreshSchedule`

3.5 Configuration Template

A new configuration template has been added that is used by the workflow, `WebexDeviceRefreshSchedule`, when the schedule has been configured.

This new configuration template must be cloned down and customized as it contains the Reset options as well as the credentials for accessing the Webex RoomOS devices.

- `WebexDeviceRefreshSchedule`

VOSS-1150: Support Operator Connect for Providers

4.1 Introduction

Adds the ability to manage a Microsoft Operator Connect Tenant and import Customer Consents, Numbers, Number Order History, and provides the ability to Order and Release Number ranges. The imported Numbers and Number history models will be moved down to Customer level automatically during the data import if the Tenant ID value matches an existing Microsoft Tenant ID added at Customer level. A Number Inventory entry will also be added at Customer level for each Operator Connect number imported when the data is moved to Customer level. Number Inventory entries will also be added at Customer level when ordering a new Number range.

4.2 Access Profiles

Review the default ProviderAdminAP for permission examples for the following model types:

- `relation/MicrosoftOperatorConnectTenant`
- `device/msoperatorconnect/PartnerOperatorConsents`
- `device/msoperatorconnect/Numbers`
- `view/MicrosoftOperatorConnectUploadNumberRange`
- `view/MicrosoftOperatorConnectReleaseNumberRange`
- `device/msoperatorconnect/TnUploadToAccountV2`
- `device/msoperatorconnect/TnReleaseOrderV2`
- `device/msoperatorconnect/CallingProfilesV2`
- `device/msoperatorconnect/TnUploadToAccountUsages`

4.3 Menu Layout

Review the default ProviderMenu for configuration examples for the following items, under the MS Operator Connect Management folder:

- Operator Connect Tenant
- Partner Operator Consent
- Numbers
- Upload Number Range
- Release Number Range
- Number Order History
- Calling Profiles
- Number User Capabilities

4.4   Data Sync

After adding the Operator Connect Tenant details (`relation/OperatorConnectTenant`), the following new data syncs will be added:

- `SyncMSOperatorConnect__<Name>`

- `SyncMSOperatorConnectNumber__<Name>`

- `SyncPartnerOperatorConsents__<Name>`

- `PurgeMSOperatorConnect__<Name>`

VOSS-1167: Disaster recovery call routing on Oracle SBCs when using Microsoft Teams

5.1   Introduction

Adds the ability to define a Disaster Recovery routing plan to redirect individual Number Inventory entries to alternate numbers. When the routing plan is activated the Local Routing Config entries will be provisioned on an Oracle SBC to redirect the calls. When the routing plan is de-activated the Local Routing Config entries will be removed from the Oracle SBC.

An email alert can also be sent on plan activate and deactivate to individual configured email addresses and/or email groups. An Oracle SBC must have been added and added to a Network Device List before configuring the routing plan.

5.2   Access Profiles

Review the default ProviderAdminAP for permission examples for the following model types:

- `relation/dr_routing_plan_rel`

- `view/dr_routing_plan_view`

5.3   Menu Layout

Review the default ProviderMenu for configuration examples for the following items:

- Define Call Routing Plan
- Activate/DeActivate Call Routing Plan

5.4   Email Template

A new email template instance (`data/EmailHtmlTemplate`) has been added and can be cloned down and customized. This email template will be used when activating or deactivating the routing plan.

- DR Activation

5.5   Macros

The following macros will need to be cloned down and customized to match the required configuration of the Local Routing Config entries on the Oracle SBC:

- `dr_routing_OracleSBC_NewLine`

- `dr_routing_OracleSBC_country_code`

- `dr_routing_OracleSBC_replace_country_code`

- `CustomerBuild_OracleSBC_TitleCFWD`

VOSS-1214: Support Microsoft Teams and Teams Phone licensing via group membership

6.1   Introduction

From release 21.4-PB2 onwards, License Management has been removed and is no longer used to control the logic with managing licenses. VOSS Automate will honor any license-related configuration in the configuration templates and related workflows. This includes Quick Subscriber, Quick Offboard Subscriber, associated Quick Add Groups, and general Subscriber Management.

It is advised that administrators evaluate their current configuration templates and ensure that if any licensing logic exists in the templates, that this is correct, as it will be applied when invoked and not controlled by the redundant **Manage Licenses** checkbox on Site Defaults Doc.

Also see the *Licensing Users for MS Teams and Teams Phone by Group Membership* topic in the Core Feature Guide.

Group Management is a great way to scale the level of users who are licensed. Instead of individually licensing a user, all users who require Microsoft Office 365 licenses can just be added to a group that is properly licensed and they will inherit it.

VOSS Automate now allows for the control of adding or removing Microsoft users to groups. This can be achieved on an adhoc basis or via a workflow when executed through Quick Subscriber, Subscriber from Profile, Flow Through Provisioning, or Quick Offboard Subscriber.

6.2   Access Profiles

Review the default ProviderAdminAP for permission examples for the following model type:

- `view/MsGraphManageGroup`

In order for the Group Management Quick Action on the MultiVendorSubscriber to appear, the access profile must have the *Read* and *Create* actions for this model.

6.3   Menu Layout

Review the default ProviderMenu for configuration examples for the following new entry:

- Manage Group Membership

This can be found as a sub-menu under Microsoft Subscriber Management. It allows for the adhoc adding and/or removing of a user's group membership.

VOSS-1234: Utilize AudioCodes ARM registration data to reconcile the number inventory

7.1   Introduction

Adds the ability to connect to AudioCodes ARM server and import the RegisteredUsers for the purpose of aligning the Directory Number status with devices that are registered directly to the Audio Codes ARM.

When a `RegisteredUser` is imported that matches a directory number in *Available* state, the number will be automatically updated to *Used*. When the devices become unregistered on the Audio Codes ARM, the `RegisteredUsers` model is removed on the next import and the *Used* directory number will be put into *Cooling* status automatically for two days and then automatically moved back to *Available* status if a device has not re-registered again with that same matching number for two days. If the device registers again at any point, the number will be moved back to *Used* state.

7.2   Access Profiles

Review the default ProviderAdminAP for permission examples for the following model types:

- `relation/AudioCodesConnection`
- `device/audiocodes/RegisteredUsers`

7.3   Menu Layout

Review the default ProviderMenu for configuration examples for the following items:

- Audio Codes ARM Connection
- Audio Codes ARM Registered Users

EKB-14895: Add tool to merge two users into a single user for multi vendor subscribers

8.1   Introduction

Adds a tool for merging two different users, which have been imported from different vendors, eg: Cisco and Microsoft, where the usernames do not match.

A primary user can be elected and the services from the secondary user will be merged into the primary user. The remaining `data/User` instance from the secondary user will be removed.

8.2   Access Profiles

Review the default ProviderAdminAP for permission examples for the following model types:

- `view/ConsolidateUsers`

8.3   Menu Layout

This tool has not been exposed in the default ProviderAdmin menu but can be added by adding an entry with the following model type:

- `view/ConsolidateUsers`

EKB-15513: Add "allowlist' capability to Global Settings to prevent unwanted Update workflows from triggering

9.1   Introduction

Adds a new "allowlist" capability to the system Global Settings that allows fields to be defined for model types that allow the *Update* workflows for the specified models to be triggered during a data sync. Any fields that have not been specifically set in the allowlist will not trigger the *Update* workflows if the field changes.

This can provide a more efficient mechanism for specifying fields over the existing denylist functionality, which has been in use in all prior versions. The denylist relies on specifying all fields that should not trigger the *Update* workflows. Any fields not specified would still trigger the *Update* workflows. This can lead to the denylist requiring constant maintenance if new fields are introduced, or if previously unidentified fields start triggering updates.

Either the allowlist method or the denylist method should be selected. If fields exist in both lists, the allowlist takes precedence over the denylist, and *Update* workflows will be triggered if the specified field changes on a data sync.

Add and *Delete* workflows are still triggered, regardless of allowlists and denylists.

9.2   Menu Layout

Review the system Global Settings menu, which is exposed in the sysadmin and tdkadmin user menus, by default.

- `data/Settings`