VOSS-4-UC
Upgrade Notes for VOSS-4-UC 21.1

Release 21.1

Sep 10, 2021

Contents

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.

Note: For Release 21.1, there is no upgrade procedure with a Delta bundle.

Follow the upgrade procedure in the *Upgrade Guide with ISO*.

Important:

- Customers who operate certain End-of-Support versions of VOSS-4-UC may be required to upgrade to newer versions of the software prior to upgrading to VOSS-4-UC 21.1.

  These versions include VOSS-4-UC 18.1, 18.1-PB3, 19.1.1, 19.1.2

  Upgrade Paths:

  - CUCDM 11.5.3 (Patch Bundle 4b) > ISO upgrade to 19.2.1 > 21.1
  - 18.1 (Patch Bundle 3/3b) > ISO upgrade to 19.2.1 > 21.1
  - 19.1.1 > Delta Bundle upgrade to 19.2.1 > 21.1
  - 19.1.2 > Delta Bundle upgrade to 19.2.1 > 21.1
- For VOSS-4-UC release 21.1, refer to the VOSS-4-UC 21.1 Release Changes and Impact document for details on model and workflow changes. Customizations related to these changes may be affected. Note that this impact document is not applicable when upgrading from 20.1.1.
- VOSS-4-UC will not support API Backward Compatibility from 21.1 and future releases. Documentation is available to highlight API differences” in order for integrators to apply the necessary changes.
- VOSS-4-UC User Management transactions have undergone major changes in order to rationalize entities and more easily incorporate different UC vendors in future. These changes have the side effect of more transactions being executed during User and Subscriber creation and updates. The increase in transactions leads to longer running UC Application Data Sync operations. The number of transactions will be optimized in future releases in order to speed up Data Sync operations.
- User Management migration updates default authentication types on SSO Identity Providers when upgrading from 19.3.4 to 21.1 (not applicable when upgrading from 20.1.1). If an SSO Identity Provider exists at the provider hierarchy level, the default authentication settings:

  - Authentication Scope: Current hierarchy level and below
  - User Sync Type: All users

  will not allow any non-SSO user logins (typically local administrators). The solution is to log in as higher level administrator account (full access) and set the SSO Identity Provider:

  - Authentication Scope: Current hierarchy level only
  - User Sync Type: LDAP synced users only

  Please refer to the *SSO Identity Provider: Field Reference* topic in the Core Feature Guide under *Configure Single Sign-On for VOSS-4-UC*.

- If any Microsoft integrations exist in VOSS-4-UC pre-upgrade, then the existing device connections configured for Azure AD Online will be migrated to MS Graph. The MS Graph connection configuration requires additional details, which must be obtained prior to upgrade.

  Please see the *VOSS-4-UC Configuration and Sync* and *Microsoft Configuration Setup* topics in the Core Feature Guide. The connection configuration must be added to the migrated connection details after upgrade to ensure continued serviceability.

  After the upgrade, the `MsolAccountSku` instances must be imported again from `MSGraph` by utilizing a Model Type List that specifies the `device/msgraph/MsolAccountSku` model and associating the Model Type List to a Data Sync before executing.

  Using a full access account, ensure that the related MicrosoftTenant, MSTeamsOnline and MSGraph instances have the same name by renaming instances. This will allow for the successful management of the instances by the exposed MicrosoftTenant.

- Any customer using the Microsoft / Cisco Hybrid (Direct Routing) adaptation will not be able to upgrade to the 21.1 release. This adaptation is only supported on release 19.3.4 and has not been made compatible with some of the core functionality in the new release.

- **EKB-9885 Privacy field does not update when modifying Cisco Unified Client Services Framework devices**

  After upgrade, import the `device/cucm/PhoneType` model for all Unified CM Clusters in order for this change to work.

- When upgrading to 21.1, the **app template** install step may not succeed if:

  - attempting to upgrade a LandingPage without any “Sections” defined
  - attempting to upgrade a MenuLayout without any “Menu Items” defined

  If the installation is not successful, for the duration of the upgrade:

  - Add any arbitrary entry in Sections to a LandingPage without any Sections
  - Add any arbitrary entry in Menu Items to a MenuLayout without any Menu Items

  or

  - remove any MenuLayout and LandingPage instances by first unlinking from any Roles and then deleting if this is acceptable

  then

  - rerun the template install step

VOSS-847: Support for Microsoft O365 and MS Teams Management

2.1 Introduction

This feature introduces many new features to support the management of Microsoft O365 and Teams users and configurations.

2.2 Access Profiles

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

- *relation/MicrosoftTenant*
- *view/MicrosoftSubscriberQos*
- *data/MicrosoftSubscriberQasStaging*
- *view/MicrosoftSubscriberQas*
- *relation/MicrosoftSubscriber*
- *device/msteamsonline/**
- *device/msgraph/**
- *data/FlowThroughProvisioningCriteria*
- *data/ModelFilterCriteria*

2.3 Menu Layout

Review the default Provider Menu for configuration examples for the following items.

- **Apps Management > Microsoft Tenant**
- **MS Teams Dial Plan Management**
- **MS Teams Policies**
- **MS Subscriber Management**
- **Customizations > Model Filter Criteria**
- **Customizations > Flow Through Provisioning Criteria**

2.4 Field Display Policy (FDP)

A number of default FDPs have been added or modified. Please review the FDPs for changes which 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 Menu item as per the Menu Layout section.

- *AzureAD_MsolUser_FDP*
- *MSTeamsOnline_CsolUser_FDP*

VOSS-842: Customer and App onboarding automation between V4UC and Assurance

3.1 Introduction

This feature introduces new tools to automate the provisioning of asset and related configuration on VOSS Assurance arbitrator servers.

3.2 Access Profiles

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

- *view/OnboardAssuranceAssets*
- *view/OnboardAssuranceAssetCUCMCluster*
- *view/OnboardAssuranceAssetCUCMServer*
- *view/OnboardAssuranceAssetCUCCluster*
- *view/OnboardAssuranceAssetCUCServer*
- *view/OffboardAssuranceAssets*
- *view/OffboardOneAssuranceAsset*
- *relation/AssuranceArbitratorServer*

3.3 Menu Layout

Review the default Provider Menu for configuration examples for the following items:

- Device Management
  - VOSS Assurance
    - Arbitrators
    - Onboard Assets
    - Offboard Assets

VOSS-835: Extended Webex Teams User and Workplace Management

4.1 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.

4.2 New Default Settings

There are a number of new Global Settings added to control the behavior of the Webex Teams feature.

There are also a number of new default settings to review on the Webex Teams Customer Access page for each managed Webex Teams organization. This can be found under **Services** > **Webex Teams** > **Customer Access** in the default menus.

4.3 Access Profiles

Review custom Access Profiles and ensure the following permissions are included to enable the new Webex Teams functionality:

- *device/spark/Device*
- *relation/WebexTeamsPlace*
- *data/WebexTeamsManualSteps*
- *view/GenerateWebexTeamsUserCsvPerCustomer*
- *view/BulkUpdateWebexTeamsUser*

4.4 Menu Layout

Review the default Provider Menu for configuration examples for the following items.

- Subscriber Management
  - Webex Teams
    - Users
    - Generate User CSV Import File
    - Bulk Update Webex Teams Users
    - Workspaces
    - Devices
    - Licenses
    - Roles
    - Manual Steps

4.5 Field Display Policy (FDP)

A number of default FDPs have been modified. Please review the FDPs for changes which 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 Menu item as per the Menu Layout section.

- *SparkCustomerFDP*
- *SparkUserFDP*
- *SubscriberAdvanced-SiteFDP*

- *SubscriberAdvancedDefault*
- *default (data/QuickAddGroups)*
- *default (view/GlobalSettings)*

VOSS-795: Multi-vendor Subscriber List and Dashboard

5.1 Introduction

This feature introduces a new way to view and manage Subscribers that are multi-vendor e.g. Cisco and Microsoft, compared to the existing Subscriber management that is Cisco only. To enable this new management there are some configuration changes required as detailed below.

5.2 Access Profiles

Review the default ProviderAdmin AP for permission examples for the following model types:

- *relation/MultiVendorSubscribers*
- *relation/MultiVendorSubscriber*

5.3 Menu Layout

Review the default Provider Menu for configuration examples for the following items.

- ***Multi Vendor Subscribers***

  -Model Type: relation/MultiVendorSubscribers -Custom Component: Multi-Vendor Subscribers List (/subscribers/list-mv-subscribers)

5.4 Business Admin Portal Profile

A new checkbox is present on the Subscribers tab of the BAP profile to enable the new Multi-Vendor Subscriber in BAP When this is enabled, you no longer select specific features to allow for Subscribers, but instead select a Field Display Policy which configures the behaviour on the Subscriber edit page in Business Admin Portal. (Note: For Multi Vendor Subscriber to display correctly in the Admin Portal this checkbox must be enabled)

5.5 Field Display Policy (FDP)

When Multi-Vendor is enabled in a BAP profile, a Field Fisplay Policy controls the fields and actions available to the BAP Admin User. A default BAP specific FDP has been added.

- *MultiVendorFDP*

VOSS-794: Improve transaction log management

6.1 Introduction

This feature introduces a new view that is used to modify the transaction log level at Provider hierarchy or above. In addition, a new field has been added to data sync in order to enable configuration of the transaction log level per data sync.

6.2 Access Profiles

Review the default Provider Admin AP for permission examples for the following model type:

- *view/DataSettings*

6.3 Menu Layout

Review the default Provider Menu for a configuration example for the following item.

- *System Settings*

6.4 Field Display Policy (FDP)

There are no new or updated default FDPs. However, data sync includes a new "Transaction Log Level" field that can be hidden or displayed as necessary.

6.5 Important Note on Transaction Log Levels

The feature introduces two new severity levels for transaction logs, namely `Verbose` and `Debug`. `Verbose` and `Debug` log levels are lower severity than the system default (`Info`) severity. It should be noted that some transaction logs have been downgraded `Verbose` severity. Therefore, some transaction logs will no longer be displayed for new transactions upon upgrade.

It should also be noted that the effective log level for data sync transactions is now derived from the new data-sync-specific "Transaction Log Level" field. When the "Transaction Log Level" field is not set, only Warning or higher severity transaction logs are displayed for executed data syncs.

VOSS-790: Pexip Support

7.1 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.

7.2 Access Profiles

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

- *device/pexip/Conference*
- *relation/PexipConference*
- *relation/PexipServer*
- *relation/Subscriber*
  - *AddPexipConference*
  - *DelPexipConference*

7.3 Menu Layout

Review the default Provider Menu for configuration examples for the following items.

- Device Management
  - Pexip Conferencing
- Subscriber Management
  - Pexip Conference Users

VOSS-722: Productize Voss Phone Server

8.1 Introduction

This feature provides the ability to manage VOSS Phone Server. VOSS Phone Server is a standalone SIP based Phone registration server which can be used to register Cisco SIP Phones or 3rd Party SIP Phones. The Dial Plan required to route calls between Cisco Unified CM and VOSS Phone Server is automatically provisioned when moving Phones from Unified CM to VOSS Phone Server.

8.2 Access Profiles

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

- *relation/PRSSwitchREL*
- *relation/GS_SMEInstanceDataPRS_REL*
- *view/VOSSCallControlAuditPhones_VIEW*
- *view/VOSSCallControlConversion_VIEW*
- *relation/PRS_MultiVendorPhone_REL*

8.3 Menu Layout

Review the default Provider Menu for configuration examples for the following items:

- *VOSS Phone Server*
- *VOSS Phone Adaptive Dial Plan*
- *VOSS Phone Audit*
- *VOSS Phone Conversion*
- *VOSS Phones*

VOSS-692: Reset/restart all phones in a Site

9.1 Introduction

This feature provides the ability to perform a Reset or Restart of all registered Cisco phones at a Site.

9.2 Access Profiles

Review the default Provider Admin AP for permission examples for the following model type:

- *view/Site_Phones_Reset*

9.3 Menu Layout

Review the default Provider Menu for configuration examples for the following item.

- Reset-Restart Site Phones

VOSS-689: Improve usability of Media Termination Point, Transcoder and Conference resources

10.1 Introduction

This feature provides the ability to manage Media Termination Points, Transcoders and Conference Bridge resources, for Cisco Unified CM.

10.2 Access Profiles

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

- *relation/MediaResource_MTP_REL*

- *relation/MediaResource_Transcoder_REL*
- *relation/MediaResource_CFB_REL*

10.3 Menu Layout

Review the default Provider Menu for configuration examples for the following items:

- Media Resource MTP
- Media Resource Transcoder
- Media Resource CFB

VOSS-667: Clusterwide Call Park and Directed Call Park

11.1 Introduction

Provides two new capabilities related to managing Cisco Unified CM Call Parks and Directed Call Parks.

This feature was available as two separate add-on Adaptations for previous releases called GS Call Park, and Directed Call Park. These Adaptations must not be installed from version 20.1.1 or above.

11.2 Relation

Two new Relations have been added:

- *relation/ClusterwideCallPark_REL*
- *relation/ClusterwideDirectedCallPark_REL*

11.3 Access Profiles

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

- *relation/ClusterwideCallPark_REL*
- *relation/ClusterwideDirectedCallPark_REL*

11.4 Menu Layout

Review the default Provider Menu for configuration examples for the following items.

- *Clusterwide Call Park*
- *Clusterwide Directed Call Park*

VOSS-661: Upgrade platform OS to Ubuntu 18.04

12.1 Introduction

The operating system has been upgraded to Ubuntu 18.04. VOSS-4-UC now supports TLS 1.3, although disabled by default.

12.2 Enabling TLS 1.3

TLS 1.3 is disabled by default in order to provide a seamless upgrade experience for customers using browsers that are incompatible with the stricter security requirements of TLS 1.3. In order to enable TLS 1.3, run:

cluster run all web ssl enable TLSv1.3

Note: TLS 1.1 and TLS 1.2 are both automatically disabled upon enabling TLS 1.3. Conversely, TLS 1.3 is automatically disabled when either TLS 1.1 or TLS 1.2 (or both) are enabled.

VOSS-660: Productize Add Device to User Adaptation

13.1 Introduction

Provides two new capabilities related to adding and removing Device association to and from Subscribers.

Add Device to User: Provides the ability to associate an unassigned Phone or Device Profile to a User.

Remove Device from User: Provides the ability to disassociate a Phone from a User.

This feature was available as an add-on Adaptation for previous releases called GS_AddDeviceToUser. This Adaptation must not be installed from version 20.1.1 or above.

13.2 View

Two new Views have been added:

- *view/GS_AddDeviceToUser_VIEW*
- *view/GS_removeDeviceFromUser_VIEW*

13.3 Access Profiles

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

- *view/GS_AddDeviceToUser_VIEW*
- *view/GS_removeDeviceFromUser_VIEW*

13.4 Menu Layout

Review the default Provider Menu for configuration examples for the following items:

- *Add Device to User*
- *Remove Device from User*

VOSS-651: Number Inventory Overhaul

14.1 Introduction

Enhances Number Inventory management by adding a new Status and Usage field to Directory Numbers, which replaces the previous “Available” and “Used” fields. Status will now be shown as either Available, Used, Used-Utility, Cooling or Reserved.

Realtime usage of each DN is also shown by selecting the new “Usage” tab which returns a pattern match for Phones, Device Profiles, Remote Destination Profiles, Hunt Pilot, Line Groups, Pickup Group Pilot, Voicemail Pilot, MeetMe, CTI Route Point, Call Park, Directed Call Park, System Call Handler and VOSS Phone instances. Usage field will be updated to show service assignment when services are added, updated or removed for corresponding Directory Numbers.

Number Inventory now uses a new Relation, relation/NumberInventoryREL, this replaces the previous use of the data model data/InternalNumberInventory.

Cooling & Reservation menu has been updated to include a new Status of Reserved, the View and Access Profile remain the same as the previous Number Cooling feature, view/IniCoolingMgmtVIEW

14.2 Relation

A new Relation has been added for managing the Number Inventory. This replaces data/InternalNumberInventory:

- *relation/NumberInventoryREL*

14.3 Access Profiles

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

- *relation/NumberInventoryREL*

14.4 Menu Layout

Review the default Provider Menu for configuration examples for the following items:

- *Number Inventory*

14.5 Migration

All Directory Number instances will be migrated to reflect the new Status value, the previous “Available” and “Used” boolean fields will be automatically deprecated.

Menu entries and Access Profiles entries of data/InternalNumberInventory will be automatically replaced with relation/NumberInventoryREL.

VOSS-612: Audit log filtering

15.1 Introduction

This feature introduces a fixed set of audit log filters (called rulesets) in order to control the verbosity of audit log messages that are streamed to remote syslog servers. Prior to this upgrade all operating system audit event information (including a subset of CLI commands) was streamed to remote syslog servers when the audit log feature was enabled.

15.2 Ruleset Configuration

Eight rulesets have been created, namely:

- Default Rules
- CLI Commands
- User and Group
- Network Events
- Security
- Software Management
- Root Commands
- File Access

Refer to the Platform Guide for details of what each ruleset includes. By default, the following rulesets are enabled on upgrade:

- Default Rules
- CLI Commands

In order to enable all rulesets (behaviour prior to upgrade) on all the nodes in a cluster, the following command must be run:

cluster run all log audit ruleset enable all

VOSS-604: Internal Number Inventory Audit Tool Replacement

16.1 Introduction

Provides a new tool for Auditing Number Inventory which caters for the new Status and Usage fields. All the following services are now Audited: Phones, Device Profiles, Remote Destination Profiles, Hunt Pilot, Line Groups, Pickup Group Pilot, Voicemail Pilot, MeetMe, CTI Route Point, Call Park, Directed Call Park, System Call Handler and VOSS Phone instances. Directory Numbers are now also set back to

Available state when not assigned to services. A new View, view/NumberInventoryAudit has been added, this replaces the previous version of the Directory Number Inventory Audit Tool view/HcsDNInventoryMgmtView.

This tool was available as an add-on Adaptation in previous releases called Number Inventory Audit. This Adaptation must not be installed from version 20.1.1 or above.

16.2 View

A single new View has been added:

- *view/NumberInventoryAudit*

16.3 Access Profiles

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

- *view/NumberInventoryAudit*

16.4 Menu Layout

Review the default Provider Menu for configuration examples for the following items:

- *Audit Number Inventory*

16.5 Migration

Menu entries and Access Profiles entries of the previous tool view/HcsDNInventoryMgmtView will be automatically replaced with view/NumberInventoryAudit.

VOSS-592: Productize Multi-cluster FAC Adaptation

17.1 Introduction

This feature provides the ability to manage Forced Authorization Codes in a multi Unified CM Cluster environment, but can also be used when only a single Unified CM Cluster exists. In a multi-cluster setup Forced Authorization Codes will be added to all Unified CM Clusters, can be synced to all Clusters and can be Deleted from a single or all Clusters.

This feature was available as an add-on Adaptation for previous releases called GS_FAC. This Adaptation must not be installed from versions 20.1.1 or above.

17.2 Access Profiles

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

- *relation/GS_FAC_REL*
- *view/GS_FACSync_VIEW*
- *data/GS_FACAuthLevels_DAT*
- *data/GS_FAC_Help_DAT*

17.3 Menu Layout

Review the default Provider Menu for configuration examples for the following items:

- Forced Authorization Codes
- Sync FAC Codes Cross Clusters
- Customize Authorization Levels
- Customize Help

VOSS-568: Implement customer-specific SSO URLs

18.1 Introduction

This feature adds the ability to configure a domain name that users use to access VOSS-4-UC during SSO authentication. Once authenticated by the SSO Identify Provider, users will be redirected to VOSS-4-UC using the initial domain.

18.2 Field Display Policy (FDP)

One default FDP has been modified. Please review the FDP for changes which may need to be incorporated into the customized versions if the default version has been cloned down and modified.

- *HcsSsoIdpRelFDP*

VOSS-556: Number Range Management Tool

19.1 Introduction

Provides a common tool, for Provider and Enterprise deployment types, for managing Number Inventory entries, Add, Modify and Delete in ranges.

This new tool replaces the previous “Add Directory Number Inventory” (view/HcsDNMgmtVIEW) for Provider deployment types as well the previous “Maintain Internal Number Inventory Range” (view/UcsMaintainMultiInternalNumberInventoryVIEW) for Enterprise deployment types.

19.2 View

A single new View has been added

- *view/NumberInventoryRangeMgmtVIEW*

19.3 Access Profiles

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

- *view/NumberInventoryRangeMgmtVIEW*

19.4 Menu Layout

Review the default Provider Menu for configuration examples for the following items.

- Number Range Management

19.5 Field Display Policy (FDP)

A single new FDP has been added.

- *Name: NumberInventoryRangeMgmtViewFDP*
- *Target Model Type: view/NumberInventoryRangeMgmtVIEW*

19.6 Migration

Menu and Access Profiles entries of the previous tools, view/HcsDNMgmtVIEW and view/UcsMaintainMultiInternalNumberInventoryVIEW, will be automatically replaced with view/NumberInventoryRangeMgmtVIEW.

VOSS-551: User Management Overhaul

20.1 Introduction

This is a complete overhaul of User Management with the goal of simplifying the interaction between VOSS-4-UC and other external systems.

The following User related Data Models, Relations and View have been deprecated:

- *data/NormalizedUser*

- *data/HcsUserProvisioningStatusDAT*
- *data/LdapUser*
- *data/SsoUser*
- *data/UserAuthMethod*
- *data/HcsAdminUserDAT*
- *relation/HcsUserREL*
- *relation/HcsAdminUserREL*
- *view/HcsAuditUserSyncToVIEW*

All User related information is now stored in a single data model:

- *data/User*

A number of changes to make Authentication more flexible have also been introduced which affect LDAP and SSO Server configuration and Field Mapping.

20.2 Relation

A new Relation has been added for managing Users and Admin Users. This replaces both relation/HcsUserREL and relation/HcsAdminUserREL

- *relation/User*

20.3 Data Model

A new Data Model has been added for managing Field Mappings for LDAP and Unified CM. Field Mapping is no longer configured on the individual LDAP User Sync or CUCM instances.

- *data/UserFieldMapping*

20.4 Access Profiles

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

- *relation/User*
- *data/UserFieldMapping*

20.5 Menu Layout

Review the default Provider Menu for configuration examples for the following items:

- *Users*
- *Admins*
- *User Field Mapping*

20.6 Migration

All User instances will be migrated to reflect the new changes,the instances of the deprecated user related data models will be removed.

Menu entries and Access Profiles entries of relation/HcsUserREL and relation/HcsAdminUserREL will be automatically replaced with relation/User.

VOSS-519: Productise IOS Gateway Adaptation

21.1 Introduction

This feature adds to new menu items related to Cisco SIP Trunk and IOS Device provisioning.

Quick Add SIP Gateway: Provides the ability to add an IOS Device, SIP Trunk configuration and SIP Gateway/Port configuration in a single step.

SIP Gateway Port: Provides the ability to add, modify and delete Port configuration for an existing SIP Gateway. The relevant IOS Device Commands are generated for both actions and are available under the existing IOS Commands menu (data/HcsCommandDAT)

This feature was available as an add-on Adaptation for previous releases called GS_IOS_Gateways. This Adaptation must not be installed from version 20.1.1 or above.

21.2 View

A single new View has been added:

- *view/GS_IOSGateway_QuickAdd_View*

21.3 Relation

A single new Relation has been added:

- *relation/GS_IOSGateway_PortData_REL*

21.4 Access Profiles

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

- *view/GS_IOSGateway_QuickAdd_View*
- *relation/GS_IOSGateway_PortData_REL*
- *relation/GS_IOSGateway_PortData_REL*

21.5 Menu Layout

Review the default Provider Menu for configuration examples for the following items:

- *Quick Add SIP Gateway*
- *SIP Gateway Port*

21.6 Configuration Template (CFT)

For Quick Add SIP Gateway two sample CFTs have been provided for the SIP Trunk and SIP Port specific configuration. These CFTs appear as selectable choices from the dropdown when adding the Port via the GUI.

In order to appear in the dropdown the target model type in the CFT must be "device/cucm/SipTrunk" for the SIP Trunk and "relation/GS_IOSGateway_PortData_REL" for the SIP Port Configuration.

The CFTs must also have the "Custom feature usage identifier" value of "IOSGateway". See the sample CFTs for configuration examples:

- Name: *GS_IOSGateway_SampleSipTrunk_CFT*
- Target Model Type: *device/cucm/SipTrunk*
- Name: *GS_IOSGateway_SampleE1Port_CFT*
- Target Model Type: *relation/GS_IOSGateway_PortData_REL*
- Custom feature usage identifier: IOSGateway

For SIP Gateway Port a single CFT has been added for use in the Menu configuration:

- Name: *HcsAnalogGateway_Menu_CFT*
- Target Model Type: *relation/GS_IOSGateway_PortData_REL*