Customizations

Common Tasks

The user interface allows for a number of common procedures across all interfaces. This includes item single- and multi-selection, actions on items and ordering or moving items.

- Menu Paths

All tasks in this document are described as if you are logged in as a Cisco user administrator.

Clone

An item instance can be cloned. Cloning provides a quick way to create items or instances that have very similar data.

On the GUI, a clone button is available to carry out the task. This button is available on the specific item page and not on the list of items view.

The cloned item is created in the system only after the user clicks **Create** on the button bar.

If an item refers to other items, only the current item instance is cloned, and not the referenced items. For example, if a Phone on the system is cloned, the device models (Phone and Remote Destination) that are referred to in this item are not cloned.

The cloned key field(s), for example Name, must be edited with new values to ensure creation of a new item in the system. An error message, "Error, Duplicate Resource Found." is displayed if a key field is not changed.

Create a Clone

Procedure

Step 1 Choose the hierarchy level of the item or item instance to be cloned.

Step 2 Choose the required item or instance that you want to clone.

Step 3 Click **Clone** on the button bar.

Step 4 The page refreshes and the form displays the cloned item.

Step 5 Edit the required details, and click **Create** on the button bar when complete to create the new instance from the clone.

Selecting Items

Items that have already been created can be modified or deleted as required. This can be performed either on single items or multiple items.

Procedure

Step 1 For a single item in the list view, click the required single item that you want to edit or delete.

Step 2 For multiple items in the list view, select the check box for each item that you want to edit or delete. If the list view of items spans more than one page, items can be selected on each page as required.

Step 3 Click **Delete** or **Modify** in the button bar to delete or modify the selected items.

Ordering Lists

The list view of items allows for basic ordering by column.

The ordering of a column is shown by the up/down arrow.

Procedure

Step 1 Click in the column header of a list. String columns are sorted alphabetically and numeric columns are sorted numerically.

Step 2 Click the column header name or up/down arrow to change the direction or the sort order of the column.

Filtering Lists

Cisco Unified Communications Domain Manager 10.6(1) allows you to filter lists in order to view only data based on specific criteria. This includes Transactions and their Sub Transaction and Log lists.

A **Filter** button is available next to the navigation controls at the bottom of a list. Select the button to open the multi-filter dialog.

A filter instance consists of a selected column, a matching filter type and a value. Values are case insensitive. Filter instance rows can be added or removed on the dialog to create a filter. The combination of instances create a single filter where all instance rows are applied.

To apply the filter, press Enter or select the **Apply** button. This will hide the active filter dialog and show the filtered list.

For model lists, actions can then for example be carried out on a selection of items from the filtered list. The filter remains active until it is removed or until the user session on the GUI ends.

The **Filter** button funnel icon is black when a filter is active, and white when no filter is present. A funnel icon also shows in the list header to indicate that a filter is active and that the list is currently filtered.

If a filter is active on a list, select the **Filter** button to display the multi filter dialog again.

Close an unapplied filter dialog by clicking outside it. Unapplied filters are lost when the dialog is closed.

A filter remains active even when navigating away from the list. More than one filter can be therefore be active on lists available in a session on the GUI.

Remove an active filter by selecting the **Remove** button on the multi filter dialog or by selecting the **X** button next to the active **Filter** button.

Navigating Lists

If a list contains multiple items, page navigation controls at the bottom, center of the screen allow you to:

- scroll to the next/previous page using the right/left arrow respectively.

- scroll to the first or last page of the list as required.

- Go to a specific page by entering the required page number and clicking **Go** (or pressing **Enter**).

• Specify the number of items to display on a page, 25 to 200 (in increments of 25).

• If you are unsure of the total number of items in a particular list view, click on the [get total] link.

Updating on Pop-up Screens

User interface forms that open pop-up screens to add or delete instances carry out the Add or Delete task when the **OK** button is clicked on the pop-up screen. In these instances, it is not necessary to click the **Modify** button on the parent user interface form to complete the task.

Role Management

Provider administrators can manage the roles that are available for administrators, operators, and users at lower levels in the hierarchy.

Procedure

Step 1   Log in as a provider admin.

Step 2   Select **Role Management** > **Roles**

Step 3   To add a new role click the **Add** button.

a) Enter or select the following role settings:

Table 1: Role settings

Setting	Description
Name	Name of the role. This field is mandatory.
Description	Description of the role.
Hierarchy Type	The type of hierarchy nodes applicable at the selected hierarchy level. For example, at Provider level, the following values are allowed: Provider, Reseller, Customer, and Site. While at the Reseller level, the following values are allowed: Reseller, Customer, Site. Controls which roles are available at which levels in the hierarchy. Also used with Hcs Component Access and Service Assurance Role Type when mapping roles to HCM-F. This field is mandatory.
Hcs Component Access	Controls what HCM-F components (FF and/or SA) that users with this role have access to. Used with Hierarchy Type and Service Assurance Role Type when mapping roles to HCM-F. This field is mandatory.
Access Profiles	Permissions for resources are defined in Access Profiles. This field is mandatory.
Service Assurance Role Type	Controls read/write access to HCM-F components. Used with Hierarchy Type and Hcs Component Access when mapping roles to HCM-F. This field is mandatory.

Setting	Description
Menu Layout	The menu layout assigned to the role. Controls what menu options are available to users assigned to the role.
Landing Page	The home page assigned with the role. Controls what the home page looks like for users assigned to the role.
Theme	The name of the theme assigned to the role. The theme controls the overall look and feel of the GUI.

    b) Click **Save** to save the role.

Step 4   To modify an existing role, click the role.
Change the role settings as needed and click the **Save** button.

Clone a Role

Use this procedure to clone an existing role for a specific hierarchy node (provider, reseller, customer, or site).

Procedure

Step 1   Log in as the hcsadmin or provider administrator.
Note   Administrators can clone roles associated with, or below, their level in the navigation hierarchy.

Step 2   Select **Role Management** > **Roles**.

Step 3   Select a role to be cloned by clicking on its box in the leftmost column.

Step 4   Select **Action** > **Clone**.

Step 5   Enter a unique name for the role in the Role field. Make the name as descriptive as possible using up to 50 alphanumeric characters, including spaces, period(s), hyphens (-), and underscore characters (_).

Step 6   (Optional) Add a description for the role in the Description field.

Step 7   Click **Save** to save the role to the hierarchy that appears in the breadcrumb.

Create a Service Assurance Only Role

To restrict an administrator to performing only service assurance tasks, you need to create the appropriate service assurance only role.

Procedure

Step 1	Login as a Provider or hcsadmin administrator.
Step 2	Select **Role Management** > **Roles**.
Step 3	Click **Add**.
Step 4	Enter a name, and optionally a description, for the role.
Step 5	Select the hierarchy type for the role. Controls the hierarchy level that the role is available at.
Step 6	For Hcs Component Access, select **Service Assurance Only**. The privileges, menu layout, and landing page values are automatically set to the appropriate values for a service assurance only role and cannot be overridden.
Step 7	Optionally, select a theme for the role.
Step 8	Click **Save**.

Create a Fulfillment Only Role

To restrict an administrator to performing only fulfillment tasks, you need to create the appropriate fulfillment only role.

Procedure

Step 1	Login as a Provider or hcsadmin administrator.
Step 2	Select **Role Management** > **Roles**.
Step 3	Click **Add**.
Step 4	Enter a name, and optionally a description, for the role.
Step 5	Select the hierarchy type for the role. Controls the hierarchy level that the role is available at.
Step 6	For Hcs Component Access, select **Fulfillment Only**.
Step 7	Select the privileges for the role.
Step 8	Optionally, select a menu layout, landing page, and theme for the role.
Step 9	Click **Save**.

Deploy a Customized Credential Policy

A default credential policy called HcsCredentialPolicy is shipped with Cisco Unified Communications Domain Manager 10.6(1). However, a customized credential policy can be deployed at a Provider, Reseller, or Customer hierarchy node.

When a customized credential policy is set as the default credential policy at a hierarchy node, all users and admins at or below that hierarchy node will be subject to the customized credential policy, except for any users or admins that have explicitly been assigned a different credential policy.

Credential Policy Inheritance

Unless explicitly assigned a credential policy, users and admins are subject to the default credential policy set at a hierarchy node at or above their location. The default credential policy for the hierarchy node closest to the user or admin location is used. If no customized credential policies have been deployed all users and admins are subject to the HcsCredentialPolicy credential policy which is the default credential policy at the sys.hcs level.

Procedure

Step 1 Log in as the provider, reseller, or customer administrator.

Step 2 Set the hierarchy path to the node where you want to deploy a customized credential policy.

Step 3 Select **Role Management** > **Credential Policy**.

Step 4 Either clone the HcsCredentialPolicy credential policy, or add a new credential policy:

- To clone the HcsCredentialPolicy policy, click HcsCredentialPolicy, then in the Action pulldown, select **Clone**.

- To add a new credential policy, click **Add**. The credential policy settings default to the settings for HcsCredentialPolicy.

Step 5 Provide a name for the credential policy.

Step 6 Modify the credential policy settings as needed.

Field	Description
Idle Session Timeout	The number of minutes a user session can be idle before being automatically logged off. The minimum setting is 1 minute and the maximum is 525600 minutes (365 days). The default is 20 minutes.
Absolute Session Timeout	The number of consecutive minutes a user can be logged in, regardless of session activity, before being automatically logged off. A value of 0 disables absolute session timeout. The maximum is 525600 minutes (365 days). The default is 1440 minutes (24 hours).
Password Expires	The number of months that can elapse between password resets. The default is 6 months.
User Must Change Password on First Login	Check this to force users to change password on initial login. The default is disabled.
Lock Duration	The number of minutes a lock will be held when user is locked out. The default is 30 minutes.
Disable Failed Login Limiting per User	Check this to not limit the number of times a user can fail to login before the account is locked. The default is to enable the limit.

Field	Description
Failed Login Count per User	The number of times a user can fail to login before the account will be locked. The default is 20 times.
Reset Failed Login Count per User	After this number of minutes from last login attempt, the failed login count will be reset to 0. The default is 5 minutes.
Disable Failed Login Limiting per Source	Uncheck this to limit the number of times any user from the same IP address can fail to login before the account is locked. The default is to disable the limit. **Note** Do not enable source login rate limiting for a credential policy that will apply to Self Service users. A separate credential policy is recommended for administrators and users that do not use Self Service if source login rate limiting is required.
Failed Login Count per Source	If source login rate limiting is enabled, enter the number of times any user from the same IP address can fail to login before the IP address will be blocked. The default is 10 times.
Reset Failed Login Count per Source	If source login rate limiting is enabled, this value is the number of minutes from last login attempt from the IP address after which the failed login count will be reset to 0. The default is 10 minutes.
Number of Questions Asked During Password Reset	Enter the number of security questions a user or admin must answer when resetting their own password via the Forgot Password link. The default is 3.
Password Reset Question Pool	Contains a list of possible security questions that a user or admin will answer when resetting their own password via the Forgot Password link.

Note It is recommended to make credential policy only more restrictive than HcsCredentialPolicy to not invalidate the Cisco Product Security Baseline.

Step 7 Click **Save**.

Note If a user is already logged in when the credential policy is changed, changes do not take effect until the user logs out and logs in again.

Step 8 Select **Role Management** > **Default Credential Policy**.

Step 9 Provide a name for the Default Credential Policy at this hierarchy node.

Step 10 In the Credential Policy field, select the credential policy you just cloned or added.

Step 11 Click **Save**.

All users and administrators at or below the hierarchy node will now be subject to the default credential policy, unless the user or admin has been explicitly assigned a credential policy.

Session Timeout Rules

The following rules apply to the idle session timeout and absolute session timeout values that can be applied to users via a credential policy:

- Setting the absolute session timeout to 0 disables it.

- The absolute session timeout takes priority over the idle session timeout. Therefore, setting the absolute session timeout to a value less than the idle session timeout effectively disables the idle session timeout.

- Credential policy session timeouts do not apply to SSO authenticated users. For SSO authenticated users, Cisco Unified Communications Domain Manager honors the SessionNotOnOrAfter SAML 2.0 attribute, which is equivalent to an absolute session timeout, although controlled by the IDP.

GUI Customization

The system allows for the user interface to be customized by a provider administrator (or higher) as required.

This customization includes:

- Theme selection

- Menu Layout customization and associated Field Display Policies

- Landing Page customization

Themes

Themes control the look and feel of the entire GUI interface. This contains all aspects of the presentation including the images, logos, colors, fonts, sizing and positioning.

New themes can be added and existing themes can be edited. These are associated with a user's role. There is no limit to the number of themes that can be added and applied. It is a common practice to have a theme associated with a specific customer (company).

The default theme that applies to the GUI when the system is initially built, is available on the system and can be used as the baseline template. The theme is in the form of a Cascading Style Sheet (CSS) to be exported, edited and re-imported as required.

While all aspects of the exported CSS can be modified, we recommend that the default theme is used as a template in terms of basic design in order to prevent usability or functional issues.

The CSS file itself is simple to export and edit. Clear headers in the CSS file indicate which area of the GUI the design applies to. The headers include the following components:

- Navbar

- Shortcut menu

- Hierarchy breadcrumbs

- Quick search

- Tree menu

- Toolbar

- List

- Form

Images can be stored with the theme or referenced with the use of relative path names.

The theme feature also includes a Use this Theme to style Login page checkbox, which when selected applies the chosen look and feel to the login page across the system. Currently, the system allows only a single theme to be applied to the Login page.

Download, Edit and Update a Theme

Procedure

Step 1 Choose the hierarchy level at which the theme will be applied. Note that themes can only be customized by a Provider Administrator (or higher).

Step 2 Choose **Role Management > Themes** to open the Themes list view.

Step 3 Click the theme that you want to download.

Step 4 Click **Download** on the button bar to download the theme. The exported file is a .zip archive with the name of the theme. The archive contains a folder with the theme name and files called skin.css and skin.less in it.

Step 5 Refer to the recommended practice to edit the Less file at the end of this topic, otherwise save the file and open the CSS file in a text editor.

- Headers are clearly marked and apply to design areas within the GUI.

- Colors, sizes, fonts, images, and so on, can all be overwritten with the required formats.

- Images must be identified with the correct file path name. Preferably, do not use '/' preceding the path name; rather use relative paths, i.e., a path relative to the CSS file location. For example, if you created an image sub-folder called 'img', use 'img/myimage.png'. After upload, the image should be viewable when opening the URL: *http://<hostname>/www/themes/mytheme/img/myimage.png*.

Step 6 When editing is complete, compress the folder and save the file with the `.zip` file extension. Note that any files or folders inside the zip file archive that start with a '.' character will be silently discarded when unzipping the theme. For example, if the zip archive contains any files named `._.DS_Store` or `.directory`, they will be ignored.

Step 7 Return to **Role Management > Themes**:

a) For an update, select the theme name and click **Browse** adjacent to Import File and then open the same theme name. Optionally check the **Backup Enabled** check box to create a backup of the current theme on the server. Click **Modify** to complete the import process.

b) For a new theme, enter a theme name that is the same as the new .zip archive filename. Click **Modify** to complete the import process.

c) To delete a theme, select it from the list and click **Delete**.

The preferred way to edit a theme is to edit and compile the Less files. * In addition to the Less files downloaded in the zipped theme, you will need the Cisco Unified Communications Domain Manager 10.6(1) minimal

theme (that can be provided at request) to compile the Less file. It will be included in the downloaded zipped theme automatically in future releases.

- All changes that made directly in the CSS files will have to be manually carried over after each changes in the Less files.

- Edit the Less files and compile them to get the new CSS files.

- The aim with Less is that a theme can be customized with the minimum of technical knowledge.

To compile the Less theme, a Less compiler is required.

Add a Theme

Procedure

Step 1 Login as **hcsadmin**.

Step 2 Prepare the theme file

a) Create a folder and add a file skin.css with the required name of the theme. The name of the folder must be the same as the intended theme name (only alphanumeric characters can be used, with no spaces or special characters).

b) Add any CSS overrides to the file. Note that only the definitions as shown in the export of a provided CSS file `skin.css` can be modified.

c) Add required image files in this folder (if any).

d) Optionally create a settings.json file in the theme folder. The settings.json has flags that controls overall appearance of elements on pages. Refer to the Theme Settings reference topic.

e) Create a .zip archive file with the same filename as the folder.

Step 3 Add the theme to the system

a) Choose the hierarchy level at which the theme will be created.

b) Choose **Role Management > Themes** to open the Themes list view.

c) Click **Add** on the button bar to open the Themes input form. Note that themes can only be customized by a Provider Administrator (or higher).

d) Enter the Theme Name (same as the file name created above).

e) Click the **Browse** button to import the created theme zip file. Wait until the system displays the file chosen in the **Import File** field.

f) If the theme must also apply to the login page, check the "Use this Theme to style Login page" check box.

g) Click **Save** on the button bar when complete.

Theme Field Reference

Base

Theme Name *	name	The name that is given to the Theme.

Use this Theme to style Login page	is_login_theme	Should Login page use this theme?
Site Title	title	The title for the site
Import File *	import_file	
Backup Enabled	backup	Create backup if existing theme exists

Login Page Details

Title	title	Title displayed at top of login page.
Banner text	banner	Banner text displayed at bottom of login page.

Theme Settings Reference

All the flags are boolean, and can have a value of true or false.

Flag Name	Default	Comment
leftSearch	false	Places search box in the sidebar. When set to true, rightSearch must be false.
rightSearch	true	Places search box in the right navbar. When set to true, leftSearch must be false.
fixedNavbar	true	Make navbar sticky at the top of the screen by adding a 'navbar-fixed-top' as class.
fixedSidebar	true	Make sidebar sticky (always visible).
fixedBreadcrumbs	true	Make context hierarchy path always visible.
enableCustomJS	false	Execute custom Javascript that creates a non-native menu scrollbar. Required by the Futurama2 theme.

The contents of a settings.json file with default values looks like:

```
{
    "leftSearch": false,
    "rightSearch": true,
    "fixedNavbar": true,
    "fixedBreadcrumbs": true,
    "fixedSidebar": true,
    "enableCustomJS": false
}
```

Set the Login Page Theme

Procedure

Step 1 Choose the hierarchy level in which the theme was created or to which the theme belongs.

Step 2 Choose **Role Management > Themes** to open the Themes list view.

Step 3 Click the required Theme Name that you want to use for the Login page.

Step 4 On the **Base** tab, check the Use this Theme to style Login page check box.

Step 5 On the **Login Page Details** tab, enter the required text in the Title field and Banner text field. The text entered in the Title field will be displayed at the top of the Login page, above the logo. The text entered in the Banner Text field will be displayed at the bottom of the Login page, below the **Log In** button.

Step 6 Click **Save** on the button bar when complete to implement the selection.

What to Do Next

The Login page theme can also be applied to the login page during the log in process. Do this by adding the suffix '?theme=<theme_name>' to the login request url, where <theme_name> is an available theme.

Menu Layouts

Menu layouts define the view a user has of the menu content and structure on the GUI. This is fully customizable up to three levels deep and can be created or edited to represent the content any user needs to have access to. The association of the defined view of the menu is made with the user's role and menu layouts can be created directly on the GUI.

To refine a view of model entities for a user, a Field Display Policy (FDP) and Configuration Template (CFT) for a model can be applied. The FDP and CFT for a specific model is applied as part of the menu layout - in other words in the menu structure, the FDP and CFT are attributes of the specific model entry for that menu layout. This means that:

- Different FDPs and CFTs for a specific model can define menu layout variations for that model.

- The required FDP and CFT should be available and defined before creating new menus.

Default menu layouts are provided with Cisco Unified Communications Domain Manager 10.6(1). These include defaults for pre-defined hierarchy based user roles, namely HcsAdmin, HcsProviderAdministrator, HcsCustomerAdministrator and HcsSiteAdministrator. The details of these default menu layouts can be viewed and easily edited to either remove or add entries, update entries (for example with an alternative FDP), change default values (for example with an alternative CFT), or change the order and groupings of the items.

The menu layout is an attribute of the user role. Each user must be assigned a User Role, thus the user will see the menu layout based on this user role. Refer to the User Role topic.

Menu layouts can also be copied via the Clone option so they can be edited or exported and re-imported.

Designers who have access to tag or version tag can apply these to a menu layout so that it can be uniquely identified to track and control changes.

Create a Menu Layout

Before You Begin

To work on an existing menu layout, it is recommended to clone the menu layout and work on the clone.

Procedure

Step 1 Login as hcsadmin, provider, or reseller administrator.

Step 2 Choose the hierarchy for the menu layout.

Step 3 From the left menu, select **Role Management > Menu Layouts**.

Step 4 Click **Add**.

Step 5 Enter a name and a description for the menu layout.

Step 6 Optionally, click the nest + button on the **Menu Items** field and fill in data for the necessary fields.

Step 7 Click the **Save**.

What to Do Next

Assign the Menu Layout to the appropriate Role.

Menu Layout Field Reference

Title	Field Name	Description
Name *	name	The name that is given to the Menu Layout.
Description	description	A description of the Menu Layout.
Menu Items	menu_items	The list of menu items and -sub items that belong to the Menu Layout.

Menu Items

Title	Field Name	Description
Title	title	The menu item title as it will show on the menu.
Type	type	The selected model type from the Type drop-down list to associate with the Title.
Href	href	If a direct reference to a model type is used for the menu item, the specified path.

Title	Field Name	Description
Field Display Policy	field_display_policy	The selected Field Display Policy that is associated with the Menu Item.
Configuration Template	configuration_template	The selected Configuration Template that is associated with the Menu Item.
Display As	display	Select the display format of the model types of the menu item. The format can be a Form for a single instance, or a Tree or List for more than one instance.
Menu Items	menu_items	The list of nested menu items that belong to the Menu Layout.

Landing Pages

This is the user's home page, which is seen when the user logs in and then uses the application **Home** button.

The landing page configuration options provide an opportunity to set up short-cut links to frequently used functionality, and to enhance the look and feel on the user's GUI. Images and links can be added in vertical or horizontal patterns with unlimited boxes and shortcuts which can then be assigned to a user's role.

A default page is loaded in the system and associated to pre-defined roles in the hierarchy, for example Provider, Customer, and Site administrators.

These editable configurations provide an easy mechanism to define direct links to areas in the system which can be used as short-cuts by the administrators in line with their role.

Existing images can be used or new images can be added in line with branded look and feel.

Landing pages can also be copied via the Clone option so they can be edited or exported and re-imported.

For designers with access to the tag function, this enables the landing page to be uniquely identified and a tag version can be applied to track and control changes.

The CSS of the Theme can be used to control the layout of the landing page.

Create a Landing Page

Before You Begin

To work on an existing Landing Page, it is recommended to clone it and work on the clone.

Procedure

Step 1   Login as the provider admin.

Step 2   Choose the hierarchy for the Landing Page.

Step 3   From the left menu, select **Role Management > Landing Pages**.

Step 4   Click **Add**.

Step 5   On the **Base** tab, enter a name for the Landing page.

Step 6   Click the + button on the **Meta Tasks** field and fill in the necessary information.

Step 7   Click the + button on the **Sections** field and fill in the necessary information.

Step 8   On the **Welcome Header** tab, enter the required Header Text, which is a single line static welcome message displayed on top of the Landing page.

Step 9   Enter the required Line Text, for the welcome line displayed under the header.

Step 10 Click Add adjacent to links, for each required link in the section, and enter the link details.
The available fields are for menu items when creating Menu Layouts. If Type is selected, field display policies and configuration templates can be applied. The link Type is displayed as the chosen Display As item:

- Form - Show an input form (for an Href value, a resource ends with "/add/").
- List - List view of a resource referenced by Type or Href.
- Tree - A tree view of resource to display (if the system Href provides a tree path).
- Wizard - Execute a wizard referenced by the Href. The wizard resource URL ends with "/0/".
- IFrame - A URL specified as the Href value opens as an IFrame for cross-launching.

Step 11 Arrange the desired order of the sections by clicking the up or down arrows to move the sections up or down respectively.

Step 12 Click **Save**.

What to Do Next

Assign the Landing Page to the appropriate Roles.

Landing Page Field Reference

Welcome Header

Title	Field Name	Description
Header Text *	header	A single line static welcome test displayed on top of the landing page.
Line Text *	line	Text for the welcome line displayed under the header. Use [userrole] as a placeholder to insert the current user's role.

Title	Field Name	Description
Meta Tasks	meta_tasks	Definitions for the meta task shortcut buttons

Base

Title	Field Name	Description
Meta Tasks	meta tasks	Definitions for the meta task short-cut buttons.
Sections	sections	The list of section items that belong to the Landing Page.

Meta Tasks

Title	Field Name	Description
Display As	display	Select the display format of the model types of the menu item. The format can be a Form for a single instance, or a Tree or List for more than one instance.
Button Text	button_text	Text for the button
Type	type	The selected model type from the Type drop-down list to associate with the Title.
Href	href	If a direct reference to a model type is used for the menu item, the specified path.
Field Display Policy	field_display_policy	The selected Field Display Policy that is associated with the Menu Item.
Configuration Template	configuration_template	The selected Configuration Template that is associated with the Menu Item.

Sections

Title	Field Name	Description
Title *	title	The section title as it will show on the Landing page.
Image URL	image	Optional URL to image to be displayed as section image.
Links	links	List of links that belong to section.

Links

Title	Field Name	Description
Display As	display	Select the display format of the model types of the menu item. The format can be a Form for a single instance, or a Tree or List for more than one instance.
Display Multiple Columns	is_multicolumn	Determines if link is shown as multiple columns or not
Link Text	link_text	Text for the link
Columns	columns	Determines if links are shown as single or multiple columns
Type	type	The selected model type from the Type drop-down list to associate with the Title.
Href	href	If a direct reference to a model type is used for the menu item, the specified path.
Field Display Policy	field_display_policy	The selected Field Display Policy that is associated with the Menu Item.
Configuration Template	configuration_template	The selected Configuration Template that is associated with the Menu Item.

Landing Page Definition

The landing page definition comprises the following:

- Name - A landing page name.

- Meta Tasks - Allows you to add one or more shortcut buttons at the top of the home page screen (directly below the line text - if configured).

- Sections - One or more items displayed as a distinct block on the landing page. Sections are further broken down to:

  ◦ Title - The heading given to the section.

  ◦ Image URL - The image or icon that is displayed for a section. For example, if a theme was uploaded with landing page images and inside a sub folder of the theme folder is a file called *mytheme/img/landingpage/landing1.png*, then the URL would be: */www/themes/mytheme/img/landingpage/landing1.png*.

  ◦ links - One or more links for a section, described in the table below.

Also refer to data/LandingPage on-line help.

Meta Tasks / Links Field	Description
Display As	Determines how the link is displayed. The options are: • Form - The link opens using a form widget. • Inline List - The link points to the first five list of items. • List - Link target is rendered using the list widget. • Tree - Display the link target using a tree widget. • Wizard - Display the link target as a wizard. • IFrame - Display the link target in an iFrame. Used for x-launch. If the Inline List option is chosen, the Display Multiple Columns field is visible. The first five items are displayed in the section. If the list is longer than five items, a link to the whole list is displayed after the first five.
Display Multiple Columns	If Display As is set to Inline List, the check box determines if the single field or multiple fields are to be shown. If enabled, the Link Test field is hidden and replaced by the Columns field.
Button Text (Meta Tasks section only)	Text that is displayed in the task's button.
Link Text (Links section only)	Text that is displayed in the link's button.
Columns	The names of the columns to be displayed from the list of fields returned by the API. This field is mutually exclusive with Columns. The fields are displayed as links to the target list items. For example, if `first_name` and `last_name` are selected for `data\User`, then the first five users are listed as rows with columns for the first name and last name.
Type	The Model Type that is displayed or targeted by the link. If this field is populated, then the Href field (below) should be blank. For example, if **Model Type** is selected as `data/User` and the **Display As** option is `List`, then the menu link shows the list of instances of `data/User`.
Href	API URL on which the client performs retrieves the link's data from If this field is populated, then the Type field (above) should be blank. An example **API URL** would be /api/v0/relation/SubscriberPhone/ for a list of items of type relation/SubscriberPhone.

Meta Tasks / Links Field	Description
Field Display Policy	If specified, the Form URI is extended to apply the policy to the returned form.
	For example, if **Model Type** is selected as `data/User/add` and **Display As** option is `Form`, then a Field Display Policy that is available for `data/User` can be selected to apply to the form in order to for example hide or rename input fields.
Configuration Template	If specified, the Form URI is extended to apply the template to the returned form.
	For example, if **Model Type** is selected as `data/User/add` and **Display As** option is `Form`, then a Configuration Template that is available for `data/User` can be selected to apply to the form in order to, for example, provide default values.
Link Text	The text that is displayed as the link. If the link is displayed as Inline Form, then a field name from returned data type may be specified instead. This field is mutually exclusive with Columns.
	Note that if the display is Inline List, then all displayed links show this text.

Field Display Policies

Field Display Policies are applied to certain item types in order to modify the default form that is displayed when these items are created or accessed.

With Field Display Policies, the fields on an item detail form can be grouped, hidden; on-line help text can be added and a field can be set as read-only. A field can be provided with a new label and its order on the form can be re-sequenced. The order parameter is the relative position in the group.

More than one Field Display Policy can apply to a particular item type so that the selection of a particular policy will present another view of the form.

A Field Display Policy for an item type can be applied from a Menu Layout by selecting and associating it with the item on the Menu Layout. The Menu Layout is then selected to be part of a user Role so that users who have this role and log in will be able to have the item displayed according to the relevant Field Display Policy.

For example, a system may have users at Provider, Customer and Site administration hierarchy levels - all of whom may access the same items, but perhaps some item fields need to be hidden for administration users at a certain level. Field Display Policies can then be made that are applied to the Menu Layout associated with the administration users at these levels.

A quick way to carry out this task is to clone an existing Field Display Policy, modify it as required and then to select it for the model on a user's menu layout. In this way a user's interface can be modified from the point of user access to the model on the menu.

There is a unique constraint on the name of the clone per hierarchy level, so the same name as the original can be used on another hierarchy, but a new name is needed at the same hierarchy.

A Field Display Policy can also be selected for a form that is part of a Wizard.

If a Field Display Policy is called 'default', it will apply to a model by default.

Clone a Field Display Policy

Procedure

Step 1	Login as hcsadmin or provider administrator.
Step 2	Choose the desired hierarchy.
Step 3	From the left menu, select **Role Management** > **Field Display Policies**.
Step 4	Click on the Field Display Policy that you want to clone.
Step 5	Click the **Actions** button and choose **Clone**.
Step 6	Update the necessary fields for the cloned Field Display Policy.
Step 7	Click the **Save** button.

Field Display Policy Field Reference

Title	Field Name	Description
Name *	name	The name that is given to the Field Display Policy.
Description	description	A description for the Field Display Policy instance.
Target Model Type *	target_model_type	The target model type to which the Field Display Policy applies.
Groups	groups.[n]	The groups that describe groupings of attributes that are displayed together on the user interface.
Title *	title	The name of a specific group of attributes.
Display as Fieldset	display_as_fieldset	Render this group as a fieldset in the form.
Number of Columns	num_cols	The number of columns of fields.
Policy *	policy	The specific policy application to attributes of the target model type of the Field Display Policy.

Configuration Templates

Configuration templates are used to define values for attributes of any model. The values can be fixed values or existing macros visible from the hierarchy context where the configuration template is applied. The templates provide a useful way to define default values for items that are exposed in the GUI (visible, invisible or read only). They also provides a mechanism to map data from data input via the GUI or device model events to other models or Provisioning Workflows in the system.

One may want to hide attributes of a model whilst setting them to a specific fixed value (e.g. a hardcoded setting); or one may wish to derive the value based on a macro (for example, look up the value based on data in the system).

For example, if a model has an attribute that is defined to be a date string, a Configuration Template for the attribute can be defined as a macro `{{fn.now \"%Y-%m-%d\"}}` in order to set the current date stamp as the value, such as `2013-04-18`. Designers can access reference material for details on macros.

Another example is a model such as the Quick Add Subscriber that limits the user input to a few fields, whilst deriving the value of other hidden attributes from various Configuration Templates that are each applied to different underlying models that make up a Subscriber (for example, Voicemail account settings, conference account settings, phone, line, device profile settings, and so on).

When an instance of the model is added or updated, the Configuration Template that has been enabled for the model applies. For array elements of data- and domain models, a list and a variable can be specified to be looped through so that a value is applied to each element in the model array.

More than one Configuration Template can be created for a model. These can then be used as needed. Configuration Templates can also be applied to models in the design of for example Provisioning Workflows and Wizards.

A Menu Layout that can be associated with a user role can also apply a Configuration Template to a model that is selected as a menu item.

For administrators at Provider Administrator level of higher, a quick way to create a Configuration Template would be to open a similar template from for example the **Role Management > Configuration Templates** menu and to customize a clone of it.

Administrators at levels above the Site Administrator can also customize these templates, including Field Display Policies.

Clone a Configuration Template

Procedure

Step 1   Login as hcsadmin or provider administrator.

Step 2   Choose the desired hierarchy.

Step 3   From the left menu, select **Role Management** > **Configuration Templates**.

Step 4   Click on the Configuration Template that you want to clone.

Step 5   Click the **Actions** button and choose **Clone**.

Step 6   Update the necessary fields for the cloned Configuration Template.

Step 7   Click the **Save** button.

Configuration Template Field Reference

Title	Field Name	Description
Name *	name	The name that is given to the Configuration Template.
Description	description	A description for the Configuration Template instance.
Foreach Elements	foreach.[n]	Iterates over the list returned by the macro and appends array elements to the specified field.
Property *	property	The field/property to iterate over.
Macro List *	macro_list	The macro that produces the list to iterate over.
Context Variable *	context_var	The context variable that will contain the data from the iteration.
Target Model Type *	target_model_type	The target model type and name that the Configuration Template applies to.
Template *	template	The contents of the template, such as defaults and macros. The names shown in the template are determined by the attribute names of the Target Model Type.

Access Profiles

Access profiles define model types that a user is permitted to access. Access profiles are assigned to users via Roles.

Clone an Access Profile

Procedure

Step 1 Login as hcsadmin.

Step 2 From the left menu, select **Role Management > Access Profiles**.

Step 3 Click on the Access Profile you want to clone.

Step 4 Click the **Actions** button and choose **Clone**.

Step 5 Enter the name, description and assign the necessary permissions for the Access Profile you are creating.

Step 6 Click the **Save** button.

Access Profile Field Reference

Title	Field Name	Description
Name *	name	The name that is given to the Access Profile.
Description	description	A description for the Access Profile.
Full Access	full_access	Enabling this flag, grants the user full system access.
Miscellaneous Permissions	miscellaneous_permissions	The list of miscellaneous operations permitted by this Access Profile.
Type Specific Permissions	type_specific_permissions	The list of types that are permitted by this Access Profile.

Type Specific Permissions

Title	Field Name	Description
Permitted Type *	type	The type that is permitted by this Access Profile. This field supports the use of the * wildcard.

Title	Field Name	Description
Permitted Operations	operations	The operations that are permitted by this Access Profile for the given type.