
NetIQ Identity Manager Home and Provisioning Dashboard User Guide

January 2016

Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

© 2014 NetIQ Corporation. All Rights Reserved.

For information about NetIQ trademarks, see <https://www.netiq.com/company/legal/>.

Contents

About this Book and the Library	5
About NetIQ Corporation	7
1 Overview	9
1.1 Identity Manager Home	9
1.2 Provisioning Dashboard	10
2 Accessing Identity Manager Home	11
3 Configuring Identity Manager Home	13
3.1 Configuring Identity Manager Home Items	13
3.2 Configuring Featured Items	14
3.3 Customizing the User Interface	15
3.4 Localizing Identity Manager Home and the Provisioning Dashboard	17
3.5 Configuring Forgot Password Functionality	18
3.6 Configuring Localized User Names	18
3.7 Configuring Email Notification Templates	19
3.8 Enabling Localized User Names in Typeahead Fields	20
4 Making and Managing Requests	21
4.1 Viewing Your Permissions	21
4.2 Requesting Permissions	22
4.2.1 Requesting Permissions for You	22
4.2.2 Requesting Permissions for Others	23
4.3 Claiming Tasks	24
4.4 Managing Your Tasks	24
4.5 Removing Permissions	25
4.6 Viewing Your History	25
4.6.1 Viewing Your History as a User	26
4.6.2 Viewing Your History as a Requester	26
5 Using Identity Manager Home Links	29
5.1 Searching for Users, Groups, or Teams	29
5.2 Updating Your Profile	29
5.3 Changing Your Password	29
5.4 Viewing Your Organization Chart	30
5.5 Managing Roles and Resources	30
5.6 Managing Users and Groups	30
5.7 Managing Teams	30
5.8 Configuring User Application Access	30
5.9 Getting Help	30

6	Troubleshooting Identity Manager Home	31
6.1	Incorrect Keystore Configuration Causes Browser to Display Flashing Web Page	31
6.2	Recreating Identity Manager Home Database Tables in PostgreSQL	31
A	Identity Manager Home REST APIs	33
A.1	POST /api/util/permssort (sort a list of permissions by display name)	33
A.2	POST /api/util/usersort (sort a list of users by full name)	34
A.3	POST /api/util/tasksort (sort a list of tasks by the specified column)	35

About this Book and the Library

The *User Guide* provides information about installing, configuring, and using the NetIQ Identity Manager Home and NetIQ Identity Manager Provisioning Dashboard add-on user interfaces for the Identity Manager Roles Based Provisioning Module.

Intended Audience

This book provides information for individuals responsible for using the Identity Manager Roles Based Provisioning Module to make and approve process requests of various types. The primary audience for this book is an end user of the User Application interface who needs simple, easy-to-understand access to user-facing RBPM functions.

Other Information in the Library

For more information about the library for Identity Manager, see the [Identity Manager documentation Web site \(https://www.netiq.com/documentation/idm45/\)](https://www.netiq.com/documentation/idm45/).

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- ◆ Identity & Access Governance
- ◆ Access Management
- ◆ Security Management
- ◆ Systems & Application Management
- ◆ Workload Management
- ◆ Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log on. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit community.netiq.com.

1 Overview

NetIQ Identity Manager Home and the NetIQ Identity Manager Provisioning Dashboard are end user-focused interfaces that allows you to access an easily-customized view of your Identity Manager User Application functionality. These add-on interfaces provides a targeted view of Identity Manager data and roles-based provisioning functions.

Identity Manager Home and the Provisioning Dashboard provide a single access point for all Identity Manager users and administrators and allows access to all existing Roles-Based Provisioning Module (RBPM) and User Application functionality. In addition, Identity Manager Home and the Provisioning Dashboard include new user-oriented features. Users can access the new user interfaces using any supported Web browser, from either a desktop computer or a tablet.

Identity Manager Home and the Provisioning Dashboard target end users, not administrators. Administrators need to access the existing User Application user interface to perform most administrative functions and tasks. Identity Manager Home links directly to some of these areas and can be configured to link to other User Application areas as necessary.

Identity Manager users who log into Identity Manager Home or the Provisioning Dashboard can then access the User Application without logging in again, and vice versa.

1.1 Identity Manager Home

Identity Manager Home provides a single access point for all Identity Manager users and administrators and allows access to all existing Roles-Based Provisioning Module and User Application functionality, as well as new user-oriented features.

Administrators can customize Identity Manager Home to show only the items and links their users need to see, organized into categories that make sense, and add their own links or REST endpoints.

Administrators can configure items on Identity Manager Home to include badges. Badges can, for example, display how many items of a certain type a user has access to. For information about configuring Identity Manager Home items, see [“Configuring Identity Manager Home Items” on page 13](#).

Identity Manager Home and the Identity Manager Provisioning Dashboard are separate user interfaces, with Identity Manager Home linking to different areas of the Dashboard. Identity Manager Home includes the following default set of links for an administrator user:

- ◆ Request Access
- ◆ My Approvals
- ◆ My Request History
- ◆ My Access
- ◆ My Profile
- ◆ Change My Password
- ◆ Search
- ◆ Assign Roles
- ◆ Assign Resources

- ◆ [Create Users and Groups](#)
- ◆ [Manage Roles](#)
- ◆ [Manage Resources](#)
- ◆ [Navigation and Access](#)
- ◆ [Identity Reporting](#)

Additionally, as an administrator, you can configure what features you want your users to be able to access. Identity Manager Home can be easily localized in multiple languages.

1.2 Provisioning Dashboard

While Identity Manager Home provides a single point of entry to the Identity Manager Roles Based Provisioning Module functionality, the Identity Manager Provisioning Dashboard is a personalized view of each user's permissions, tasks, and requests. Identity Manager Home links to the appropriate location on each user's Dashboard.

The Provisioning Dashboard focuses on the following basic areas of functionality:

I want something. If a user needs an item or needs to request an item for other users within the organization, the user can use the **Make a Request** functionality to request that item. The item can be a piece of equipment like a laptop or something intangible like access to a particular server or application. The user can search for an item by entering all or part of a search term in the **Permissions** field. If a user wants to request a permission for others users, the user can search for the targeted recipients for the permission in the **Recipients** field. For information about making requests, see [“Requesting Permissions” on page 22](#).

I need to do something. If a user wants to know what tasks they need to manage, **My Approvals** shows all of a user's pending tasks in the Identity Manager system. For information about managing and addressing pending tasks, see [“Managing Your Tasks” on page 24](#).

What do I have? If a user wants to see everything they can currently access, **My Access** shows a user all of the roles and resources to which they have access and organizes those items into a list. For information about viewing your current permissions, see [“Viewing Your Permissions” on page 21](#).

How did I get it? If a user wants to see a list of past requests as a requester and as a recipient, **History** shows a user everything they have requested recently, as well as the status of all their pending requests. For information about viewing a user's request history, see [“Viewing Your History” on page 25](#).

2 Accessing Identity Manager Home

To access Identity Manager Home and the Provisioning Dashboard:

- 1 Open a Web browser and navigate to one of the following URLs, depending on whether SSL is configured in your environment:

```
https://IDMServer:8180/landing
```

```
https://IDMServer:8180/landing
```

Where *IDMServer* is the fully-qualified name or IP address of your Identity Manager Roles Based Provisioning Module server. If you do not know the address you need to use, contact your Identity Manager administrator.

- 2 Provide your Identity Manager user name and password.

NOTE

- ◆ If you have previously accessed the Identity Manager User Application, you may be able to use the same user name and password to access Identity Manager Home.
- ◆ You cannot access Identity Manager Home using an account that includes any of the following characters in the name:

```
\ / , * ? . $ # +
```

- 3 Select **Login**.

3 Configuring Identity Manager Home

After you install Identity Manager Home components in your User Application environment, you must configure Identity Manager Home to allow your users to perform their necessary tasks.


3.1 Configuring Identity Manager Home Items

As an administrator, you can customize the default Identity Manager Home items your users can access. You can add or remove Home items as needed or add your own new custom items.

NOTE

- ♦ If you want to add the available iManager item to Identity Manager Home, you must configure the link to point to your iManager installation. If you add the item to Identity Manager Home without configuring the link, the link returns an error.
- ♦ Users can only see the items to which they have access. If you want to restrict users' access to specific Home items, use the User Application Administration module.

To customize the default Identity Manager Home items displayed:

- 1 Log in to Identity Manager Home using a Role, Resource, Provisioning, and Security domain administrator account.
- 2 On Identity Manager Home, select **Edit**, located in the top right-hand corner of the page.
- 3 (Optional) If you want to add the provided iManager item to Identity Manager Home, complete the following steps:
 - 3a In the **New and available items** column, mouse over **iManager** and select the **Edit** icon.
 - 3b In the **Link** field, specify the URL for your iManager installation.
 - 3c Select **Save**.
 - 3d Select and drag **iManager** from the **New and available items** list to one of the categories displayed on the right side of the page.
- 4 (Optional) If you want to add a new category to Identity Manager Home, complete the following steps:
 - 4a Select **New Category**. The user interface adds a new untitled category at the bottom of your current set of categories.
 - 4b Select the title `Untitled Category` and specify the name you want to use for the category.
 - 4c Select on the page outside of the category title to save the new name.
- 5 (Optional) If you want to delete a category, select the **Delete this category** icon  under **Categories**.

NOTE: If you delete a category, Identity Manager Home automatically moves any items in that category back to the **New and available items** list.

- 6 (Optional) If you want to add or remove an Identity Manager Home item, select and drag the item to and from the **New and available items** list and one of the categories displayed on the right side of the page. You can also drag and drop items from one category to another category.
- 7 (Optional) If you want to add a new Identity Manager Home item to the **New and available items** list, complete the following steps:
 - 7a Select **New item**.
 - 7b Specify a **Name** and **Description** for the new item.

Specify the description of the item with parameters like {0} and {1} and substitute this value with the value obtained from the **API URL** field.

For example:

```
View my {0} Identity Manager tasks approval.
```
 - 7c To specify an image to use for the item, select **Browse**, navigate to the image, and select **Open**.
 - 7d (Optional) If you want the new item to link to a specific URL, either within the User Application or outside of Identity Manager, specify the URL in the **Link** field.
 - 7e (Optional) The **API URL** points to the REST endpoint with JSON data which provides extra details like the value of parameters and a badge. The value mentioned here is substituted with the parameter mentioned in the **Description** field.

For example: with respect to the example mentioned in the **Description** field, the parameter {0} is substituted with the following value.

```
{
  "badge": 0,
  "params": [
    {
      "id": "0",
      "value": "0"
    }
  ]
}
```
 - 7f Select **Save**.
- 8 When finished configuring Identity Manager Home items, select **I'm done**.

3.2 Configuring Featured Items


When configuring your Identity Manager Home environment, you can create and configure any Featured Items you want all users to be able to access in their personal Provisioning Dashboards. This feature is not supported for requesting on behalf of other users in your organization.

NOTE: If you do not add any items to a Featured Items category, the Dashboard does not display the category.


- 1 Log in to Identity Manager Home using a Role, Resource and Provisioning domain administrator account.
- 2 Select **Request Access**.
- 3 Select **Edit Featured Items**.
- 4 Select **Add an item**.

- 5 In the **Add an uncategorized item** field, specify the role, resource, or process request you want to include as a Featured Item. The Dashboard automatically displays any existing roles, resources, or PRDs matching the specified text.
- 6 Select the item you want to include.
- 7 (Optional) If you want to specify a particular image to use for the Featured Item, select **Browse**, select the image, and select **Open**.

NOTE: You can specify an image with a maximum file size of 512 KB, in JPG, GIF, PNG, or SVG format.

- 8 Select **Save**.
- 9 (Optional) If you want to create a specific Featured Item category, select **New category**, then specify a name for the category and press **Enter**.
- 10 Select the new item in the **New and available items** list and drag the item to the category where you want to display the item. You can also drag and drop items from one category to another category.
- 11 Repeat [Step 4](#) through [Step 10](#) for each Featured Item you want to add.
- 12 (Optional) If you want to modify an existing item, mouse over the item and select the **Edit** icon. You can then modify the image for the item or select **Delete** to delete the item completely.
- 13 (Optional) If you want to delete a category, select the **Delete this category** icon  under **Categories**.

NOTE: If you delete a category, Identity Manager Home automatically moves any items in that category back to the **New and available items** list.

- 14 When finished configuring your Featured Items, select **I'm done**. The Dashboard lists your new items under **Featured Items**.
- 15 Select the **Home** icon .

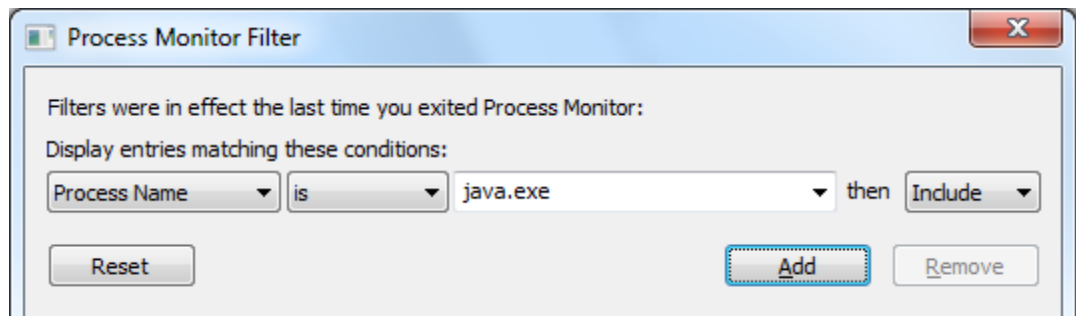
3.3 Customizing the User Interface

You can change the appearance of the Home (landing) and Provisioning Dashboard (dash) user interface by using your own custom css file. The `dash war` looks for the `custom.css` file in the `netiq_custom_css` directory within the home directory of the user that started the application server.

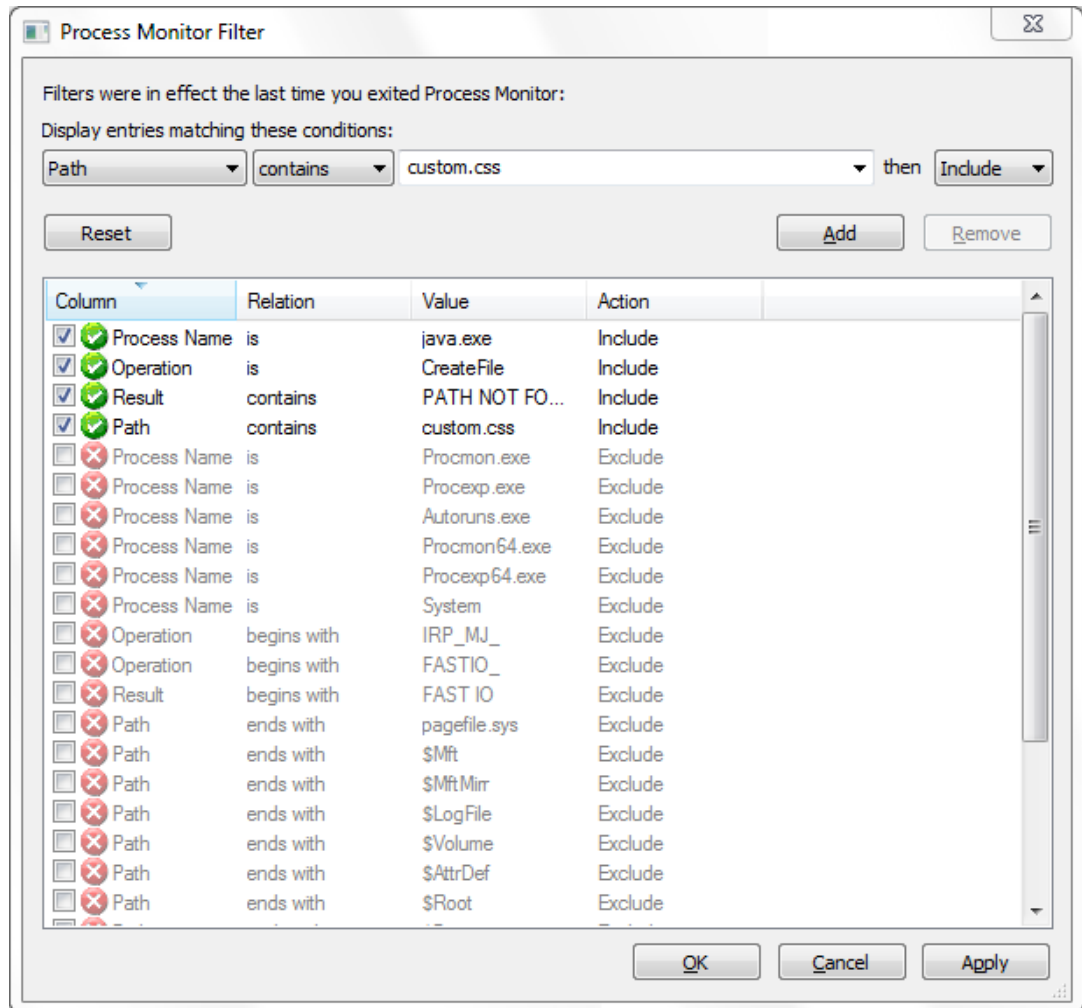
On Tomcat, this user is `novlua`, so the home directory is `/opt/netiq/idm/apps/novlua`. On WebSphere and Jboss, this user is `root`, so the home directory is `/root`. If the `custom.css` file exists, it overrides the default style sheet file provided with Home and Provisioning Dashboard.

To customize the user interface using the custom css file,

- 1 Download the `ProcessMonitor.zip` file from the [Microsoft website](#) to a temporary location on your computer.
- 2 Extract the contents of the unzipped file.
- 3 Navigate to the folder where you extracted the file, execute the `Procmon.exe` file.
- 4 Click the **App-V** icon to display the Process Monitor Filter page.
- 5 In the Process Monitor Filter page, perform the following actions:
 1. Create a rule that says **Process name is java.exe**, then click **Add**.



2. Create a rule that says **Operation is CreateFile**, then click **Add**.
3. Create a rule that says **Result contains PATH NOT FOUND**, then click **Add**.
4. Create a rule that says **Path contains custom.css**, then click **Add**.
5. Deselect the entries that are not added from the list and click **Apply**.
6. Click **OK** to exit the window.



6 The Process Monitor page displays a prompt indicating that custom.css file is not found in the following location:

C:\Windows\system32\config\systemprofile\novl_rpt_custom\custom.css

This implies that you need to create a folder named `novl_rpt_custom` and add `custom.css` file in this folder.

7 After creating the file and the folder, restart the application server.

3.4 Localizing Identity Manager Home and the Provisioning Dashboard

You can localize or customize the text displayed on Identity Manager Home and Provisioning Dashboard by modifying a set of language-specific properties files provided by Identity Manager. Localization properties files use the `.properties` extension.

Identity Manager Home includes the following properties files by default:


Language	Locale Designation
Chinese (China)	zh_CN
Chinese (Taiwan)	zh_TW
Danish	da
Dutch	nl
English	en
French	fr
German	de
Italian	it
Japanese	ja
Portuguese	pt
Russian	ru
Spanish	es
Swedish	sv

To customize Identity Manager Home strings for your environment, complete the following steps:

- 1 Log in to Identity Manager Home using an domain administrator account that is assigned the Role Administrator, Resource Administrator, Provisioning Administrator, and Security Administrator roles.
- 2 On Identity Manager Home, select **Edit**.
- 3 Select **Localize**.
- 4 Select the locale for which you want to localize and save the properties file to your local computer.
- 5 Open the properties file in a text editor and specify text for each property listed. For example, if you download the `sv.properties` file to localize Identity Manager Home and the Provisioning Dashboard in Swedish, modify the properties file as follows:

```
# English value: My Category
category-featured-47-name = Min kategori
```

NOTE: If you want to use double-byte or extended characters in the properties file, ensure that you save the file using the correct encoding.

- 6 Save and close the properties file.
- 7 On Identity Manager Home, select the **File Upload** icon  for the locale.
- 8 Navigate to the properties file on your local computer and select **Open**.
- 9 Repeat [Step 4](#) through [Step 8](#) for each locale you want to enable.
- 10 Select **Back to edit**, then select **I'm done**.

3.5 Configuring Forgot Password Functionality

If you want to set up the Identity Manager Home login page to display the **Forgot password?** link, you must configure the Password Management Settings in the **Authentication** tab of the ConfigUpdate Section and then restart the Tomcat application server.

To enable the **Forgot password?** link for Identity Manager Home:

- 1 Launch the ConfigUpdate utility from the command line: `configupdate.sh` or `configupdate.bat`
- 2 Click the **Authentication** tab, scroll down to the Password Management section and select **Forgot Password**.
- 3 Click **OK**.
- 4 Click **Logout**.
- 5 To start Tomcat, enter the following command in a command prompt:

```
/etc/init.d/idmapps_tomcat_init restart
```
- 6 After Tomcat finishes restarting, go to the Identity Manager Home login page and verify the page displays the **Forgot password?** link.

3.6 Configuring Localized User Names

Identity Manager Home, the Provisioning Dashboard, and the User Application allow you to configure the format of displayed user names in your environment based on the user's current locale.

You can then use localized user names in Approval forms in the User Application, using the literal `%LocaleFormattedFullName%` for forms with the `User` entity definition key. For more information about creating or configuring User Application forms in Designer, see "Creating Forms for a Provisioning Request Definition," in the *NetIQ User Application: Design Guide*.

To configure localized name formatting, use Designer to edit the `Full Name` entity in the Directory Abstraction Layer (DAL):

- 1 Start Designer.
- 2 Open your current project and click the project name in the Outline view.
- 3 In the Provisioning view, right-click **Full Name** and select **Edit**.
- 4 In the Directory Abstraction Layer editor, expand **Entities > Full Name**.
- 5 Select the locale name pattern you want to modify.

- 6 Modify the **Calculated Attribute** expression to specify the format you want to use for the locale. For example, if you want to display the user's surname first and given name second, modify the expression as follows:

```
attr.getValue("Surname") + " " + attr.getValue("Given Name")
```

You can either modify the expression manually in the Expression field or click the **Build ECMAScript Expression** icon and use the ECMA Expression Builder to modify the expression. For more information about modifying ECMAScript expressions, see "Working with ECMA Expressions," in the *NetIQ User Application: Design Guide*.

- 7 Save your changes to the locale name pattern.
- 8 Repeat [Step 5](#) through [Step 7](#) for each name pattern you want to configure.
- 9 When finished, close the Directory Abstraction Layer editor.
- 10 In the Modeler, right-click the User Application driver and select **Driver > Deploy**.
- 11 Click **Deploy**, then click **Yes** to restart the driver.
- 12 Click **OK**.

3.7 Configuring Email Notification Templates

By default, email notification templates in Identity Manager direct recipients to the User Application user interface. If you want email notification templates to direct recipients to Identity Manager Home and the Provisioning Dashboard, you must modify the default templates in Designer.

NOTE

- ♦ Only some default notification templates include links to the User Application.
- ♦ Modifying an existing notification template marks that template as customized in Designer.

To configure email notification templates for Identity Manager Home, complete the following steps:

- 1 Start Designer.
- 2 Make sure you have imported email notification templates into your Designer project.
- 3 In the Outline view, right-click the notification template you want to modify and select **Copy**.

NOTE: We recommend you create and modify a copy of the original notification template you want to configure, rather than modifying the original. You can then specify the "Identity Manager Home" version of the template in any workflows where you want users to use Home and the Provisioning Dashboard, and not modify the workflows where you want users to use the User Application.

-
- 4 Specify a name for the copied template and click **OK**.
 - 5 Right-click the copied template and select **Edit**, then click **Yes** to confirm.
 - 6 (Optional) If you want to remove all links to the User Application, modify the message text as follows:
 - 6a Find and remove any instances of `$PROTOCOL$://$HOST$: $PORT$/$TASK_DETAILS$`. In the Provisioning Dashboard, users can no longer directly access the details of a task.
 - 6b Change any instances of the following:

```
$PROTOCOL$://$HOST$: $PORT$/$TASKLIST_CONTEXT$
```

to:

```
$PROTOCOL$://$HOST$: $PORT$/dash/#myTasks
```

- 7 (Optional) If you want to retain the existing User Application links, add text similar to the following line to the notification template message:

```
You can review your tasks list using the new Provisioning Dashboard at  
$PROTOCOL$://$HOST$: $PORT$/dash/#myTasks.
```

- 8 When finished, save and close the notification template.
- 9 Repeat [Step 3](#) through [Step 8](#) for each notification template you want to modify, including any localized templates.
- 10 Deploy the new templates to the Identity Vault.
- 11 Modify any workflows where the approver should use Identity Manager Home and the Provisioning Dashboard so the workflow uses the new notification templates.

3.8 Enabling Localized User Names in Typeahead Fields

After you configure the `Full Name` entity in the DAL, the identity applications automatically display user names formatted by locale.

However, to use user names with localized name formatting in typeahead fields within the identity applications, you must create one or more custom registry entries. The identity applications use typeahead controls when a supervisor wants to manage a specific or team, and the typeahead controls do not use the `%LocaleFormattedFullName%` literal.

- 1 In the `conf` directory of your application server installation, create an empty file with the file name `UIControlRegistry_CustomProps.xml`.
- 2 Open the User Application WAR, `IDMProv.war` by default, and extract the contents.
- 3 Locate the `UIControlRegistry.xml` file in the WAR's `WEB-INF` directory.
- 4 In the `UIControlRegistry.xml` file, locate the entries for the `UserDNLookup` and `UserInTeamDNLookup` keys.
- 5 Copy the `<registry>` element, `<ctrls>` element, and both keys to the `UIControlRegistry_CustomProps.xml` file.
- 6 Modify the `display-exp` property of each of the copied keys as follows:

```
<prop name="display-exp" type="string">  
  <value>FirstName LastName</value>  
  <value xml:lang="de">LastName FirstName</value>  
</prop>
```

- 7 Create an `xml:lang` value for each localized name format you want to use. You can include a value for each language supported by the User Application.
- 8 Save and close the `UIControlRegistry_CustomProps.xml` file.
- 9 Restart your application server.

4 Making and Managing Requests

Most users access Identity Manager Home because they need to request an item, approve someone else's request, or make a request on someone else's behalf. In Identity Manager Home and the Provisioning Dashboard, items users can request are generically called **permissions**.

Using Identity Manager Home and the Provisioning Dashboard, a user can request hardware, access to a particular server, or permission to use a particular application in their environment or place a request for other users in the organization. Your ability to request an item depends on your role and permission in the organization. For example, a team requester and other authorized employees can make requests on behalf of other users in the organization.

After a request is placed, when the manager logs into Identity Manager Home, the manager sees a pending task displayed in the My Tasks badge, and looks at that request in his My Tasks list and either approves or denies the request.

Users can also view their existing permissions in the My Access list on the Provisioning Dashboard, and see the status of their past requests in the History list on the Dashboard.

Identity Manager Home and the Provisioning Dashboard streamline the provisioning process for both end users and managers, allowing users and managers to make and approve requests quickly and easily.

NOTE: In Identity Manager, permissions are **roles**, **resources**, or **PRDs**.

You cannot configure roles, resources, PRDs, or categories using Identity Manager Home. For more information about configuring roles in Identity Manager, see "Configuring Roles," in the *NetIQ User Application: Design Guide*.

For more information about configuring resources in Identity Manager, see "Configuring Resources," in the *NetIQ User Application: Design Guide*.

For more information about configuring PRDs in Identity Manager, see "Configuring Provisioning Request Definitions," in the *NetIQ User Application: Design Guide*.

4.1 Viewing Your Permissions

To view the roles and resources to which you have access, select **My Access** on Identity Manager Home. On the Provisioning Dashboard, you can then select a specific permission in the **My Access** list for further details on that role or resource. The Dashboard displays details about the requester of that permission and any reasons provided for the permission assignment.

If you want to find a particular permission in a large list, enter all or part of the name of the permission in the **Search my access** field. The **My Access** list displays only those permissions matching the specified text.

4.2 Requesting Permissions

As with the existing User Application interface, you can use the new interface to do the following:

- ◆ Request new permissions for you
- ◆ Request permissions on behalf of other users

To request permissions on behalf of other users, you must be a team requester or a user who has the necessary permissions to place the request. Identity Manager allows the following roles to request permissions for other users in the organization.

- ◆ Security Administrator
- ◆ Domain Administrator
- ◆ Team Requester

NOTE: If you logged in as a different user, the **Provisioning Dashboard** does not display the **Request on Behalf** option.

You can make the same request for multiple users at the same time. The interface allows you to select objects such as users, groups, and teams for making requests. A team contains users who are authorized to make requests, end-users who are recipients of those requests, and permissions for the team. For more information about configuring teams, see [Managing Teams](#) in the [NetIQ Identity Manager Catalog Administrator User Guide](#).

You can view other requests for the users to determine what requests are necessary.

- ◆ [Section 4.2.1, “Requesting Permissions for You,” on page 22](#)
- ◆ [Section 4.2.2, “Requesting Permissions for Others,” on page 23](#)

4.2.1 Requesting Permissions for You

To request a permission for yourself:

- 1 Log in to Identity Manager Home.
- 2 Select **Request Access**.
- 3 On the Provisioning Dashboard, select **Self** in the **Request For** field.
- 4 Search for the specific permission you want to request in **Permissions**.

You can sort the resulting permissions by the closest matching result or in alphabetical order.

NOTE: You should not use punctuation when specifying a permission you want to request. If the name of the permission you want to request includes punctuation, omit the punctuation when searching.

- 5 Provide any required information, including the effective date, expiration date, or the reason for the request.

Different permissions require different information, depending on how the administrator has configured the form. If the permission requires detailed information, the Dashboard redirects you to a separate form window when you select the permission.

- 6 Select **Request** or **Submit**, depending on the type of permission requested.

You can request multiple permissions at the same time.

NOTE: Items that require additional detailed information may not be available for selection with other items. To request multiple permissions at once, the request forms for the various requests cannot require detailed information.

4.2.2 Requesting Permissions for Others

To request a permission for other users:

- 1 Log in to Identity Manager Home.
- 2 Select **Request Access**.
- 3 On the Provisioning Dashboard, select **Others** in the **Request For** field.
- 4 Search for the recipients for whom you want to request a permission.

A recipient can be one or more users. Multiple recipients can belong to a group or a team. To select more than one recipient, select the user individually. You can also select a group or a team as a recipient. When a team or a group is selected as a recipient and a permission requested for it, the Provisioning Dashboard internally expands the list of recipients within the team/group and raises separate requests for all the users within the team/group. It is also possible to select a few users from a group and request permissions for them. If you select the members of a group individually, the Provisioning Dashboard displays the names of the selected members in the **Recipients** field.

- 5 Search for the specific permission you want to request for the users in **Permissions**.

NOTE: You should not use punctuation when specifying a permission you want to request. If the name of the permission you want to request includes punctuation, omit the punctuation when searching.

- 6 Provide any required information, including the effective date, expiration date, or the reason for the request.

Different permissions require different information, depending on how the administrator has configured the form. If the permission requires detailed information, the Dashboard redirects you to a separate form window when you select the permission.

- 7 Select **Request** or **Submit**, depending on the type of permission requested.

IMPORTANT: You can request multiple permissions for multiple recipients at the same time. However, Identity Manager allows bulk requests for only one team at the same time. This does not include bulk requesting the complex PRDs.

As a Role Administrator or a Security Administrator, you can directly assign a role permission to the entire group by using the **Assign Role to Group** option. This option is not available for other roles.

- ♦ If you selected **Assign Role to Group**, the Provisioning Dashboard does not display other permissions except role permission.
- ♦ If you selected other permissions (PRDs and resources) while requesting a role permission for a group, the Provisioning Dashboard removes those permissions and considers only role permission request.

NOTE: Items that require additional detailed information may not be available for selection with other items. To request multiple permissions at once, the request forms for the various requests cannot require detailed information.

4.3 Claiming Tasks

After a request is initiated, you can approve the request with or without claiming it.

To claim your tasks in the Provisioning Dashboard:

- 1 Log in to Identity Manager Home.
- 2 Select the request from the **My Tasks** list.
- 3 Click the **Claim** button.

Once a task is claimed, an icon is displayed to indicate that task is claimed. If the Approver is a group, once a task is claimed, it cannot be viewed by other users. To enable other users to view the claimed task, click **Release**.

Task approval form or details page will have a **Claim** button if claim action is configured in Process Request Definition. You can approve or deny a claimed task. Task approval form will either have **Claim** or **Release** button depending on if task has been claimed or not.

You can **Claim**, **Release**, **Approve** or **Deny** multiple tasks in a single operation.

To view the comments of a task, click the task name.

4.4 Managing Your Tasks

If you are responsible for approving or denying requested permissions in Identity Manager, you can use the Provisioning Dashboard to manage your tasks as you would in the User Application.

You can approve or deny requests one at a time, or you can approve or deny multiple simple requests that do not require detailed information in bulk.

To manage your tasks in the Provisioning Dashboard:

- 1 Log in to Identity Manager Home.
- 2 Select **My Approvals**.
- 3 (Optional) If you want to approve or deny a specific request, complete the following steps:
 - 3a In the My Tasks list, select the request.
 - 3b Select **Complete Task**.
 - 3c On the form, provide any required information and select **Approve**, **Reject**, or **Deny**, as appropriate.
- 4 (Optional) If you want to approve or deny multiple requests at the same time, complete the following steps:
 - 4a In the My Tasks list, select the requests you want to approve or deny.

NOTE

- ◆ For a more complex request that requires detailed information, the Provisioning Dashboard does not display a check box. You must approve or deny those requests by selecting each request and following [Step 3a](#) through [Step 3c](#) above.
- ◆ When you select a more complex request to approve or deny, the Dashboard may need to open the request form in a separate browser tab.

4b Provide a comment explaining why you want to approve or deny the selected tasks.

4c Select **Approve X items** or **Deny X items**, as appropriate.

4.5 Removing Permissions

If you no longer want access to a role, resource, or a PRD, you can remove the permission using the Provisioning Dashboard.

NOTE

- ◆ If you add, remove, or modify a permission using the Provisioning Dashboard, the My Access list may not immediately reflect the change. Press **F5** to refresh the My Access list.
- ◆ You cannot remove permissions granted because of membership in a particular group in your Identity Manager environment. If you want to remove access to a role or resource assigned because of membership in a group, use the User Application to remove your account from that group.

-
- 1 Log in to Identity Manager Home.
 - 2 Select **My Access**.
 - 3 Select the name of the permission you want to remove.
 - 4 Select the displayed value under **Values**.
 - 5 Select **Remove**.
 - 6 Specify why you want to remove the assigned permission and select **Remove**.
 - 7 (Optional) If you want to remove multiple permissions at one time, select the permissions you want to remove on the Provisioning Dashboard.
 - 8 Specify why you want to remove the assigned permissions and select **Remove X permissions**, where **X** is the number of permissions selected.

4.6 Viewing Your History

- ◆ [Section 4.6.1, “Viewing Your History as a User,” on page 26](#)
- ◆ [Section 4.6.2, “Viewing Your History as a Requester,” on page 26](#)

4.6.1 Viewing Your History as a User







To view the history of previous requests that you requested or that another user has requested on your behalf, tasks, and assignments, select **My Request History** on Identity Manager Home.

You can also cancel a pending request that you placed from the History list, by selecting the request in the list and selecting **Cancel this request** on the subsequent window. However, you cannot cancel a pending request that was requested by another user on your behalf.

NOTE: After you make a request, you cannot select a request in the **My Request History** list until Identity Manager finishes processing. If you access the Dashboard using a slow connection, you may need to wait for the Dashboard to allow you to click the request name in the list.

The History list on the Provisioning Dashboard uses the following icons to indicate the status of a request:

Table 4-1 Icons in the History List




Icon	Status	Description
	Pending	The submitted request needs to be approved or denied.
	Approved	The request reviewer approved the request.
	Completed	The request has been completed and fulfilled, if necessary.
	Denied	The request reviewer denied the request.
	Canceled	The requester canceled the pending request.
	Error	Identity Manager encountered an error processing the request.




4.6.2 Viewing Your History as a Requester

To view the status of the requests that you have requested for other users, select **My Request History** on Identity Manager Home.

The History list uses the following icons to indicate the status of a request for the requester:

Table 4-2 Icons in the History List for Requesters

Icon	Status	Description
	Pending	The submitted request needs to be approved or denied.
	Approved	The request reviewer approved the request.
	Completed	The request has been completed and fulfilled, if necessary.

Icon	Status	Description
	Denied	The request reviewer denied the request.
	Canceled	The requester canceled the pending request.
	Error	Identity Manager encountered an error processing the request.

5 Using Identity Manager Home Links

In addition to making and managing requests in Identity Manager Home and the Provisioning Dashboard, you can use Identity Manager Home to access other User Application functionality. Identity Manager Home provides default links to several areas of the User Application, streamlining the basic tasks end users and administrators need to perform in Identity Manager.

NOTE: To return to Identity Manager Home from anywhere within the User Application, click the Home icon in the top right corner.

Identity Manager Home can also include links to other areas of the User Application or to other Identity Manager components, like the Identity Reporting Module or iManager.

5.1 Searching for Users, Groups, or Teams

To search for users, groups, or teams in your Identity Manager environment, you can go to Identity Manager Home and select **Search**. The Identity Manager Home link redirects you to the Directory Search area of the Identity Self-Service tab in the User Application.

For more information about searching for users in Identity Manager, see “Using Directory Search,” in the *NetIQ User Application: User Guide*.

5.2 Updating Your Profile

To view or modify your Identity Manager profile information, you can go to Identity Manager Home and select **My Profile**. The Identity Manager Home link redirects you to the My Profile area of the Identity Self-Service tab in the User Application.

For more information about updating your profile in Identity Manager, see “Using My Profile,” in the *NetIQ User Application: User Guide*.

5.3 Changing Your Password

To change your Identity Manager password, go to Identity Manager Home and select **Change My Password**. The Identity Manager Home link redirects you to the Change Password area of Self Service Password Reset application.

For more information about changing your Identity Manager password, see “Performing Password Management,” in the *NetIQ User Application: User Guide*.

5.4 Viewing Your Organization Chart

To view your organization chart in Identity Manager, go to Identity Manager Home and select **Org Chart**. The Identity Manager Home link redirects you to the Organization Chart area of the Identity Self-Service tab in the User Application.

For more information about using the Identity Manager organization chart, see “Using the Organization Chart,” in the *NetIQ User Application: User Guide*.

5.5 Managing Roles and Resources

If you are an administrator and you want to create or modify roles or resources in your Identity Manager environment, go to Identity Manager Home and select **Manage Roles** or **Manage Resources**, as applicable. The Identity Manager Home links redirect you to either the Roles Catalog or Resources Catalog in the Catalog Administrator.

For more information about managing roles and resources in Identity Manager, see the *NetIQ Identity Manager Catalog Administrator User Guide*.

5.6 Managing Users and Groups

If you are an administrator and you want to create or modify users or groups in your Identity Manager environment, go to Identity Manager Home and select **Create Users and Groups**. The Identity Manager Home link redirects you to the Identity Self-Service tab in the User Application.

For more information about creating users and groups in Identity Manager, see “Creating Users or Groups,” in the *NetIQ User Application: User Guide*.

5.7 Managing Teams

If you are an administrator and you want to create, modify, or delete teams or groups in your Identity Manager environment, go to Identity Manager Home and select **Manage Teams**. The Identity Manager Home link redirects you to the Team Configuration page. For more information about managing teams, see [Managing Teams](#) in the [NetIQ Identity Manager Catalog Administrator User Guide](#).

5.8 Configuring User Application Access

If you are an administrator and you want to configure access to Identity Manager User Application components, go to Identity Manager Home and select **Provisioning and Security**. The Identity Manager Home link redirects you to the Navigation Access Permissions area of the RBPM Provisioning and Security Configuration tab in the User Application.

For more information about configuring access to the User Application, see “Navigation Access Permissions,” in the *NetIQ Identity Manager User Application: Administration Guide*.

5.9 Getting Help

While working in the Identity Manager Home and Provisioning Dashboard, click the **Help** link to display the online version of this guide.

6 Troubleshooting Identity Manager Home

This section contains information for troubleshooting Identity Manager Home and the Provisioning Dashboard.

6.1 Incorrect Keystore Configuration Causes Browser to Display Flashing Web Page

If you configure the application server you use to run Identity Manager Home, the Identity Manager Provisioning Dashboard, and the Identity Manager User Application to use Transport Layer Security/Secure Sockets Layer (TLS/SSL), you must ensure the trusted root certificate of the web container running One SSO Provider (OSP) is installed in the truststore for the application server running Home, the Dashboard, and the User Application.

Typically, you should put the trusted root certificate from the keystore you used to configure the OSP container TLS/SSL into the `cacerts` keystore for the JRE used by the application server.

If you do not correctly configure the truststore when using TLS/SSL, if a user tries to log in to Identity Manager Home or the Provisioning Dashboard, the browser displays a flashing web page that never fully loads.

6.2 Recreating Identity Manager Home Database Tables in PostgreSQL

If you encounter an error in your environment and need to delete and recreate your `idmuserappdb` database tables, you can run the following Java command to rebuild the database:

```
/JavaPath/jdk1.7.0_65/bin/java -Xms256m -Xmx256m -Dwar.context.name=Context -
Ddriver.dn="DriverDN" -Duser.container="UserDN" -jar /UserAppPath/liquibase.jar --
databaseClass=liquibase.database.core.PostgresDatabase --
driver=org.postgresql.Driver --classpath=/PostgreSQLPath/postgresql/postgresql-
8.4-701.jdbc4.jar:/DeployPath/IDMProv.war --changeLogFile=DatabaseChangeLog.xml --
url="jdbc:postgresql://localhost:5432/idmuserappdb" --contexts="prov,newdb" --
logLevel=info --logFile=/LogPath/db.out --username=DBAdmin --
password=DBAdminPassword update
```

Where *JavaPath* is the path to your updated JDK or JRE, *Context* is the context you specified when you installed the User Application (IDMProv, by default), *DriverDN* is the full DN of the User Application driver, *UserDN* is the container where users reside, *UserAppPath* is the path to your main User Application installation directory, *PostgreSQLPath* is the path to your PostgreSQL installation directory, *DeployPath* is the path to your User Application and Identity Manager Home Tomcat `deploy` directory, *LogPath* is the path to the directory where you want to save the database log, *DBAdmin* is the database administrator account, and *DBAdminPassword* is the database administrator password.

For example:

```
/opt/netiq/idm/jre/bin/java -Xms256m -Xmx256m -Dwar.context.name=IDMProv -
Ddriver.dn="cn=User Application Driver,cn=driverset1,o=system" -
Duser.container="o=data" -jar /opt/netiq/idm/apps/UserApplication/liquibase.jar --
databaseClass=liquibase.database.core.PostgresDatabase --
driver=org.postgresql.Driver --classpath=/opt/netiq/idm/apps/postgresql/
postgresql-9.3-1101.jdbc41.jar opt/netiq/idm/apps/UserApplication/IDMProv.war --
changeLogFile=DatabaseChangeLog.xml --url="jdbc:postgresql://localhost:5432/
idmuserappdb" --contexts="prov,newdb" --logLevel=info --logFile=/opt/netiq/idm/
apps/UserApplication/db.out --username=***** --password=***** update
```

A Identity Manager Home REST APIs

Identity Manager Home incorporates several REST APIs that enable different features within the user interface.

A.1 POST /api/util/permssort (sort a list of permissions by display name)

Sort the specified list of permissions by display name.

NOTE: This REST API does not require authentication.

Used In

Team compare view

URL Parameters

None

Data to Send

```
{
  "perms": [
    {
      "id": "cn=changepwd,cn=RequestDefs,cn=AppConfig,cn=User Application
Driver,cn=driverset1,o=system",
      "name": "Change Password"
    },
    {
      "id":
"cn=billing,cn=Level10,cn=RoleDefs,cn=RoleConfig,cn=AppConfig,cn=User Application
Driver,cn=driverset1,o=system",
      "name": "Billing Department Access"
    }
  ]
}
```

Response payload for status code: 200 OK

```
{
  "perms": [
    {
      "id":
      "cn=billing,cn=Level10,cn=RoleDefs,cn=RoleConfig,cn=AppConfig,cn=User Application
      Driver,cn=driverset1,o=system",
      "name": "Billing Department Access"
    },
    {
      "id": "cn=changepwd,cn=RequestDefs,cn=AppConfig,cn=User Application
      Driver,cn=driverset1,o=system",
      "name": "Change Password"
    }
  ]
}
```

A.2 POST /api/util/usersort (sort a list of users by full name)

Sort the specified list of users by full name.

NOTE: This REST API does not require authentication.

Used In

Team compare view

URL Parameters

None

Data to Send

```
{
  "users": [
    {
      "id": "cn=bbender,ou=users,o=novell",
      "name": "Bill Bender"
    },
    {
      "id": "cn=cnano,ou=users,o=novell",
      "name": "Chip Nano"
    },
    {
      "id": "cn=ablake,ou=users,o=novell",
      "name": "Allison Blake"
    }
  ]
}
```

Response payload for status code: 200 OK

```
{
  "users": [
    {
      "id": "cn=ablake,ou=users,o=novell",
      "name": "Allison Blake"
    },
    {
      "id": "cn=bbender,ou=users,o=novell",
      "name": "Bill Bender"
    },
    {
      "id": "cn=cnano,ou=users,o=novell",
      "name": "Chip Nano"
    }
  ]
}
```

A.3 POST /api/util/tasksort (sort a list of tasks by the specified column)

Sort the specified tasks by the specified column.

NOTE: This REST API does not require authentication.

Used In

Dashboard task view

URL Parameters

None

Data to Send

```
{
  "sortBy": "recipientName",
  "sortOrder": "ASC",
  "tasks": [
    {
      "taskId": "85a180b8fad3425fb58a6d906075571a",
      "processName": "Anonymous Access - Create New User",
      "creationTime": "1337273009422",
      "expirationTime": "1338482609422",
      "recipient": "cn=bmalley,ou=users,o=novell",
      "recipientName": "Bill Malley",
      "simpleForm": true
    },
    {
      "taskId": "85a180b8fad3425fb58a6d906075571a",
      "processName": "Anonymous Access -Delete User",
      "creationTime": "1337273009422",
      "expirationTime": "1338482609422",
      "recipient": "cn=ablake,ou=users,o=novell",
      "recipientName": "Allison Blake",
      "simpleForm": true
    }
  ]
}
```

NOTE

- ♦ The `recipientName` value must be a value in the JSON data.
 - ♦ For the `sortOrder` value, you can specify either `ASC` (ascending order) or `DESC` (descending order).
-

Response payload for status code: 200 OK

```
{
  "sortBy": "recipientName",
  "sortOrder": "ASC",
  "tasks": [
    {
      "taskId": "85a180b8fad3425fb58a6d906075571a",
      "processName": "Anonymous Access -Delete User",
      "creationTime": "1337273009422",
      "expirationTime": "1338482609422",
      "recipient": "cn=ablake,ou=users,o=novell",
      "recipientName": "Allison Blake",
      "simpleForm": true
    },
    {
      "taskId": "85a180b8fad3425fb58a6d906075571a",
      "processName": "Anonymous Access - Create New User",
      "creationTime": "1337273009422",
      "expirationTime": "1338482609422",
      "recipient": "cn=bmalley,ou=users,o=novell",
      "recipientName": "Bill Malley",
      "simpleForm": true
    }
  ]
}
```

