July 2016

Xerox® Healthcare Policy Manager
Account Management Guide

Publication Date: July 2016.

This document supports Xerox Healthcare Policy1.0.

Table of Contents

1

Introduction

Within your healthcare organization, you and your colleagues depend on policies and procedures to establish and maintain standards on how various processes are conducted. Admitting patients, processing payments, protecting patient privacy, and administering medication are examples of actions that might be covered by a policy or procedure.

The Xerox® Healthcare Policy Manager solution streamlines the creation, review, approval, and distribution of your healthcare organization's documents. Once distributed, policy and procedure documents are centrally located and managed for quick access to the most current information. With your healthcare organization's documents electronically and securely managed, patient care is improved while noncompliance risks are minimized.

Purpose of this guide

The purpose of this guide is to aid Healthcare Policy Manager users, specifically Policy Coordinators, Authors, and Review Board members, in using the Policy Manager **Users & Groups** pages to perform administrative tasks on user and group accounts.

Use of LDAP with Healthcare Policy Manager

Healthcare Policy Manager connects to your organization's LDAP (Lightweight Directory Access Protocol) server to validate users. Therefore, your LDAP server needs to include the users who will access and use the solution. Each user needs a valid email address for task notification.

Policy Coordinator with administrator access

Xerox assigned the Policy Coordinator role (with the corresponding Administrator role) to a designated user in your organization and added the user to the Policy Manager registry. That user is the only person who can initially access Healthcare Policy Manager and set up the solution for other users to access.

Healthcare Policy Manager initial use

1. When your Healthcare Policy Manager site is ready for use, the initial user connects to the site and logs in using the account login information that Xerox provided. The initial user account resides on the site LDAP server, so that server must be configured and running.
2. Once on the site, the initial user goes to **Users & Groups l LDAP Settings l Synchronization**, locates the users who will be part of Policy Manager, assigns those accounts the appropriate system roles and synchronizes them. For more information, refer to Run manual synchronization on page 10.
3. The initial user then goes to **Users & Groups l Policy Manager Roles**, and using **Join Additional Users**, assigns the new accounts to the appropriate Policy Manager roles. For more information, refer to Assign user accounts to roles on page 12.
4. The initial user then provides the site users with the Policy Manager URL information.

LDAP tools 2

This chapter does not provide instructions for implementing either LDAP or AD (Active Directory). The information in this guide assumes the LDAP server is already in place and running, accounts for Healthcare Policy Manager have been created, and the server is being managed by an LDAP administrator.

Solution roles and user accounts

Healthcare Policy Manager provides six roles: Policy Coordinators, Authors, Review Board, Approval Committee, Policy Acknowledgers, and Policy Guests. The Policy Manager package your organization purchased determines how many roles are available. The Compliance package includes all of the solution roles, while the Essential and Review packages provide subsets of the roles.

This solution role...	Has these functions...
Policy Coordinator	Responsible for assigning roles to users and managing document tasks.
Author	Responsible for setting up the document structure, assigning stakeholders to document tasks, and writing and updating documents before they are sent to the Review Board.
Review Board	Responsible for setting up the document structure, assigning stakeholders to document tasks, and optionally writing and updating documents. They also review and provide input on documents before they are sent for approval as well as monitor the document life cycle.
Approval Committee	Responsible for approving policy and procedure documents prior to publication. They also view the level of compliance to policy and procedure documents.
Policy Acknowledger	Users who refer to published documents in their day-to-day work and who acknowledge receipt of the documents.
Policy Guest	Users who refer to published documents in their day-to-day work, but are **not** required to acknowledge receipt of the documents.

Determine what solution role you want each user to perform in Healthcare Policy Manager. The solution role must map to a system role. You will assign each user account a system role when you synchronize users accounts. Also, make sure each account has a valid email address. This is required for sending user task notifications.

System roles required for each solution role

Use the table below to map the user solution role to the correct system role. Be aware that the total number of solution and system roles is determined by your Healthcare Policy Manager license. The license sets the maximum number available for each role.

To perform the solution role of...	Assign the system role of...
Policy Coordinator with access to LDAP Settings	Administrator
Policy Coordinator	Coordinator
Author	Coordinator
Review Board	Coordinator
Approval Committee	Contributor
Policy Acknowledger	Consumer
Policy Guest	Consumer

LDAP settings

The **LDAP Settings** tab is located under Users & Groups, and provides the tools necessary to configure and manage the LDAP servers that are connected to the Healthcare Manager Policy site.

The **LDAP Settings** page provides tabs for navigating the various LDAP management pages.

- **Connection Settings**

  Use to reconfigure LDAP server settings or to add a new LDAP server.

- **Synchronization**

  Use to reconfigure automatic synchronization of users and groups information, and to run a manual synchronization bypassing the set automatic synchronization.

- **Property & Class Mapping**

  Use to map system properties to LDAP attributes.

- **User & Group Search**

  Use to search for users and groups in a selected LDAP server.

⚠ **WARNING**

The first time you click LDAP Settings, an LDAP Server field displays at the top of the page. Displayed in that field is the name of the system LDAP server – Xerox Cloud Administration. Do not edit the connection settings for this server. Doing so will break the solution and will require Xerox to correct.

Add an LDAP server

Healthcare Policy Manager requires the use of an LDAP server to store and manager user accounts.

To create a connection to an LDAP server:

1. On the navigation bar, click **Users & Groups**.
2. Click the **LDAP Settings** tab.
3. On the **Connection Settings** page, click **Add Server**.

   Step 1 of 3 is displayed.

Step 1 of 3: Connect to the LDAP server

Server Information

1. In the **Server Name** field, enter a friendly name for the LDAP server. A friendly name is something easily read and remembered, as opposed to a long pathname or IP address.
2. In the **Host Id** field, enter the host name or IP address of the server.
3. In the **Port** field, enter the port number used by this server.
4. If the server uses SSL, select **Enable SSL**.
5. In the **Fallback Host ID(s)** field, enter the host names or IP addresses of servers to use in case the main LDAP server fails. Use a comma to separate each server entry.
6. Select **Enable LDAP Server** to enable the server.

Directory Service Settings

1. From the **Type** menu, select the directory service that the server uses.
2. In the **DIT Root** field, enter the directory information tree root.
3. Select **Enable Subtree Search** to enable the subtree search under the configured DIT root.
4. To map object properties to LDAP attributes, click **Show Advanced Settings** and fill in the required fields.

   User

   a. In the **RDN Key** field, enter the attribute for common name; such as uid or cn.

   b. In the **Object Class** field, enter the attribute for the object class; such as person.

   c. In the **MemberOf Attribute** field, enter the attribute that specifies to which group this object belongs.

   Group

   a. In the **RDN Key** field, enter the attribute for group name; such as cn.

   b. In the **Object Class** field, enter the attribute for the object class; such as groupOfUniqueNames.

   c. In the **Member Attribute** field, enter the attribute that specifies all of the users belonging to this group; such as uniqueMember.

d. In the **MemberOf Attribute** field, enter the attribute that specifies to which groups this object belongs.

Access Restriction Filter

a. In the **LDAP Access Filter** field, filter out specific users or groups by entering specific classnames or attributes.

Service Account

1. From the **Login Type** menu, select either Account or Anonymous, depending on the service account used for communication between the system and the LDAP server.
2. If you selected **Account**, then enter the name used to log into the LDAP server into the **Service Account** field. Use attributes such as uid=admin,ou=system.
3. If you selected **Account**, then enter the password for the service account you entered in step 2 in the **Password** field.

   If you selected Anonymous as the Login Type, the Service Account and Password fields are not displayed.

Test Connection

1. When you have finished configuring the server, click **Test Connection** to use the Service Account to validate the server information that you entered.

   The system will respond with either a success or a failure message.
2. Click **Next**.

Step 2 of 3: Set up synchronization settings

Synchronization Mode

1. From the **Synchronization Mode** menu, select the type of mode to use for the server. The choices are **LDAP Listener (Push)** and **Site Polls (Pull)**.

User Synchronization

1. System accounts are auto-created by synchronizing with accounts created on the LDAP server. Controls restrict new accounts if a license limit is reached for the selected role.

   a. Select **Account Auto-Creation** to create a user account on the solution whenever a new LDAP account is found during synchronization.

   b. From the **Default Role** menu, select the system role type for new accounts. No new accounts are created when the license limit is reached for a selected default role.

   c. (Optional) In the **Assign Roles and Access Lists to Specific DIT Roots** field, enter the DIT Root and select the system role. The system role should map to a solution role.

   d. Click **Add** to add additional DIT Root/Role/ACLs. Click **Remove** to delete the last DIT Root/Role/ACL assigned.

   e. In the **Account Property Synchronization** field, select **Synchronize user properties** to synchronize user account properties with LDAP attributes when running a synchronization.

Group Synchronization

1. In the **Group Auto-Creation** field, select **Create LDAP Groups not on the site** to create a group account on the system whenever a new LDAP account is found during synchronization.
2. Select **Group Property Synchronization** to synchronize group account properties with LDAP attributes when running a synchronization.

Synchronization Schedule

1. From the **Synchronization Schedule** menu, select when you want to run as ynchronization.
2. When you are finished setting up synchronization, click **Next**.

Step 3 of 3: Set up property mapping

Map system properties to LDAP attributes for both users and groups. This allows the system to correctly interpret LDAP user and group attributes.

1. The fixed system user properties are listed under **Site Property**. Enter the corresponding user attributes in the fields under **LDAP Property**.
2. The fixed system group properties are listed under **Site Property**. Enter the corresponding group attributes in the fields under **LDAP Property**.
3. When you are finished mapping, click **Done**.

Reconfigure an LDAP server

To reconfigure an existing LDAP server:

1. On the navigation bar, click **Users & Groups**.
2. Click the **LDAP Settings** tab.
3. From the **LDAP Server** menu, select the LDAP server that you want to reconfigure.

⚠ **WARNING**

Do not change any of the settings for the system LDAP server – Xerox Cloud Administration. Doing so will break the solution and will require Xerox to correct.

4. Follow the instructions in Add an LDAP server on page 7 of this guide to make any necessary changes to the LDAP configuration.

Run manual synchronization

You can run a manual synchronization to update the Healthcare Policy Manager registry with new LDAP accounts or changes made to existing LDAP accounts.

To run a manual synchronization on a selected LDAP server:

1. On the navigation bar, click **Users & Groups**.
2. Click the **LDAP Settings** tab.
3. From the **LDAP Server** menu, select the LDAP server on which you want to run a manual synchronization.
4. Follow the instructions in User Synchronization on page 8 or Group Synchronization on page 9 to select the accounts that you want to synchronize.
5. In the **Synchronization Mode** area, click **Sync Now** to run a manual synchronization.

Remap properties

You can remap system properties to LDAP attributes for both users and groups.

To remap properties on a selected LDAP server:

1. On the navigation bar, click **Users & Groups**.
2. Click the **LDAP Settings** tab.
3. From the **LDAP Server** menu, select the LDAP server on which you want to remap properties.
4. Follow the property mapping instructions in Step 3 of 3: Set up property mapping on page 9.

User & Group Search

You can browse for users and groups on a selected LDAP server. This is for informational purposes. Only LDAP administrators can change account properties.

To search for users and groups on an LDAP server:

1. On the navigation bar, click **Users & Groups**.
2. From the menu next to the **Search** button, select to search an LDAP server for either **Users** or **Groups**.
3. You can select **Options** to apply a **Filter** or select a specific **Property**.
4. In the **Search** field, enter a search parameter.
5. Click **Search**.

   The search returns the results.

Users and groups 3

Manage users

The User Accounts page, displayed under **Users & Groups**, displays the user accounts that have been set up for use with Healthcare Policy Manager. These accounts were created on an LDAP server, then synchronized to the Healthcare Policy Manager registry.

Assign user accounts to roles

Once a user account is in the Healthcare Policy Manager registry, assign the user to a role.

To assign user accounts to Policy Manager roles:

1. On the navigation bar, click **Users & Groups**.
2. Click the **Policy Manager Roles** tab.
3. Do one of the following:
   - From the displayed list, select a role.
   - From the role's **Actions** menu, select **Membership**.

   The Membership page displays the users who are currently assigned to the role.
4. To assign users to the role, click **Join Additional Users** and do the following:
   a. Type the name of a user in the search box.
   b. To narrow your search, click **Options**. From the **Search In** list, select the name of the property to search. Click **Options** to close the Options panel.
   c. Click **Search**.
   d. Click the plus sign next to a name to assign the user to the role.
   e. Click the **Save** button.
5. To assign groups to the role, click the **Group Members** tab and do the following:
   a. Click **Join Additional Groups or Add Roles**.
   b. Type the name of a group in the search box.
   c. To narrow your search, click **Options**. From the **Search In** list, select the name of the property to search. Click **Options** to close the Options panel.
   d. Click **Search**.
   e. Click the plus sign next to a name to assign the group to the role.
   f. Click the **Save** button.

The page displays the additional accounts assigned to the role.

Reassign system roles

There may be times when you need to reassign a user's system role. For example; you change a user's Policy Manager role from Policy Acknowledger to Author. In this case, you will need to change the system role currently assigned to the user from Consumer to Coordinator.

To perform the solution role of...	The user must have the system role of...
Policy Coordinator	Coordinator
Author	Coordinator
Review Board	Coordinator
Approval Committee	Contributor
Policy Acknowledger	Consumer
Policy Guest	Consumer

To reassign a system role:

1. On the navigation bar, click **Users & Groups**.
2. Locate the user account whose role you want to reassign.
3. To reassign the role for one user account, do the following:
   a. From the user account's **Actions** menu, select **Change System Roles**.
   b. From **Role** menu, select the new role.
   c. Click **Save**.
4. To reassign the role for several user accounts, do the following:
   a. Select the checkbox next to each user whose role you want change.
   b. From the **Selected Actions** menu, select **Change System Roles**.
   c. In the Change System Roles window, click **Next**.
   d. To assign the same role to all users, select the role next to **Assign role to all selected users**.
   e. To assign a different role to each user, select **Assign roles separately** and select a role for each user.
   f. Click **Save**.

Display user accounts

To display user accounts:

1. On the navigation bar, click **Users & Groups**.

   The list of user accounts is displayed.
2. To display the users assigned a specific system role, select the role from the **Role** menu.
3. To display users by status, select either **Active** or **Inactive** from the **Show** menu.

4. To change the user account information displayed, do the following:
   a. Click the **Show View Settings** icon.
   b. To customize which columns are displayed in the view, select the column title and click the ‹ or › button to add the title or remove the title from the **Selected** list.
   c. The order of column titles in the **Selected** list determines the left-to-right position of the columns in the view; the column title at the top of the list will be the furthest left. Select the column title and use the controls below the **Selected** list to change the order of the columns:
      - Click the ⌄ or ⌃ button to move the selected column title up or down one place in the list.
      - Click the ︾ or ︽ button to move the selected column title to the top or bottom of the list.
   d. Under **Other Options**, select additional view options as required:
      - **Paging Size**—From the menu, select how many accounts to display on the page.
      - **Primary and Secondary Sort**—From the menus, select the primary and secondary columns to sort by and if they will be sorted in ascending or descending order. For example, if you select **First Name** and **Ascending** from the **Primary Sort** menus and then select **Last Name** and **Ascending** from the **Secondary Sort** menus, names will display in alphabetical order under the **First Name** and **Last Name** columns.
      - **Show in groups**—Click the checkbox to group objects in the view. Objects will only be shown in groups when sorted by the type or date property. Groups can be expanded and collapsed by clicking the + or - button next to the group name.
   e. Click **Save**.

View and change user account properties

You can change any user account properties that are specific to Healthcare Policy Manager.

To view and change user account properties:

1. On the navigation bar, click **Users & Groups**.
2. Locate the user account whose properties you want to view.
3. From the user account’s **Actions** menu, select **Settings**.
4. Click the **Edit Properties** tab to change the properties. Then click **Save**.
5. Click the **Group Membership** tab to view the groups the user is a member of.

View the user’s activity history

Healthcare Policy Manager keeps track of all user activity, which provides an audit trail of the actions of each user.

To view a user’s activity history:

1. On the navigation bar, click **Users & Groups**.

2. Locate the user account whose activity history you want to view.
3. From the user account's **Actions** menu, select **Settings**.
4. Click the **Activity History** tab.
5. From the **Select Activity Events** menu, choose to view **All Events** or **Selected Events**.
6. To display the activity during a specific date range, enter start and end dates.
7. Click **Download Results** to download a comma-separated values file of the events.

Add users to a local group

From the Users & Groups page, you can add users to any local groups that you have added. For more information, refer to Add local groups on page 18. You cannot add users to LDAP groups.

To add a user to a local group:

1. On the navigation bar, click **Users & Groups**.
2. Locate the user account that you want to add to a local group.
3. From the user account's **Actions** menu, select **Group Membership**.

   A page displays the groups of which the user is currently a member.
4. Click **Join Additional Groups**.
5. To select the group to add the user to:
   a. Type the name of a group in the search box.
   b. To narrow your search, click **Options**. From the **Search In** list, select the name of the property to search. Click **Options** to close the Options panel.
   c. Click **Search**.
   d. Click the plus sign next to a name to add the user or group to the group.
   e. Click the **Save** button.

The page now displays the new group.

Remove users from a group

As needed, you can remove users from a local group.

To remove a user from a local group:

1. On the navigation bar, click **Users & Groups**.
2. Locate the user account that you want to remove from a local group.
3. From the user account's **Actions** menu, select **Group Membership**.

   A page displays the groups of which the user is currently a member.
4. Locate the group that you want to remove the user from.
5. From the group's **Actions** menu, select **Remove from Membership**.

Deactivate or reactivate a user account

You can deactivate a user account when the user no longer needs access to Healthcare Policy Manager. Deactivated user accounts are not counted towards the number of licensed users. However, deactivated user accounts remain in the system so you can later reactivate an account.

Note: Deactivating a user account does not delete the account from the LDAP server.

To deactivate or reactivate a user account:

1. On the navigation bar, click **Users & Groups**.
2. Locate the user account that you want to deactivate.
3. From the user account's **Actions** menu, select **Deactivate**.
4. To reactivate the user account, locate the account and then select **Reactivate** from the account's **Actions** menu.

Manage groups

Healthcare Policy Manager includes one local (non-LDAP) group: All Users Group, which contains all of the users in the solution registry. This group along with LDAP and other local groups are displayed on the Groups page, under **Users & Groups**.

Display groups

To display groups:

1. On the navigation bar, click **Users & Groups**.
2. Click the **Groups** tab.
3. To display groups by type, select either **LDAP Groups** or **Local Groups** from the **Show** menu.
4. To change the group information displayed, do the following:

   a. Click the **Show View Settings** icon.

   b. To customize which columns are displayed in the view, select the column title and click the ‹ or › button to add the title or remove the title from the **Selected** list.

   c. The order of column titles in the **Selected** list determines the left-to-right position of the columns in the view; the column title at the top of the list will be the furthest left. Select the column title and use the controls below the **Selected** list to change the order of the columns:

   - Click the ⌄ or ⌃ button to move the selected column title up or down one place in the list.
   - Click the ︾ or ︽ button to move the selected column title to the top or bottom of the list.

   d. Under **Other Options**, select additional view options as required:

   - **Paging Size**—From the menu, select how many accounts to display on the page.
   - **Primary and Secondary Sort**—From the menus, select the primary and secondary columns to sort by and if they will be sorted in ascending or descending order. For example, if you select **Create Date** and **Ascending** from the **Primary Sort** menus and then select **Modified Date** and **Ascending** from the **Secondary Sort** menus, dates will display in chronological order under the **Create Date** and **Modified Date** columns.
   - **Show in groups**—Click the checkbox to group objects in the view. Objects will only be shown in groups when sorted by the type or date property. Groups can be expanded and collapsed by clicking the + or - button next to the group name.

   e. Click **Save**.

Add local groups

Depending on your organizational needs, you can add any number of local groups. For instance, you might want to add a different policy review group for each department.

To add a local group:

1. On the navigation bar, click **Users & Groups**.
2. Click the **Groups** tab.
3. Click **Add Local Group**.
4. Enter a group **Title** and an optional **Summary**, and then click **Next**.
5. To select the users and groups to add to the group:
   a. Type the name of a user or group in the search box.
   b. To narrow your search, click **Options**. Use **Show Object Type** to specify **User** or **Group**. From the **Search In** list, select the name of the property to search. Click **Options** to close the Options panel.
   c. Click **Search**.
   d. Click the plus sign next to a name to add the user or group to the group.
   e. Click the **Done** button.

The new group is displayed on the Groups page. You can later add additional users or groups (LDAP or local) to a local group by clicking the displayed local group name, and then clicking **Join Additional Users** on the User Members page or **Join Additional Groups or Add Roles** on the Group Members page.

Delete a local group

To delete a local group:

1. On the navigation bar, click **Users & Groups**.
2. Click the **Groups** tab.
3. Locate the group that you want to delete.
4. From the group's **Actions** menu, select **Permanently Delete**.
5. In the confirmation window, click **Delete Permanently**.

View and change group properties

You can change group properties that are not associated with LDAP group attributes.

To view and change group properties:

1. On the navigation bar, click **Users & Groups**.
2. Click the **Groups** tab.
3. Locate the group whose properties you want to view.
4. From the group's **Actions** menu, select **Settings**.

5. Click the **Edit Properties** tab to change the properties. Then click **Save**.
6. Click the **Membership** tab to view the users who are members of the group.

View the group's change history

Healthcare Policy Manager keeps track of the changes made to a group.

To view a group's change history:

1. On the navigation bar, click **Users & Groups**.
2. Click the **Groups** tab.
3. Locate the group whose change history you want to view.
4. From the group's **Actions** menu, select **Settings**.
5. Click the **Change History** tab.
6. From the **Select Change Events** menu, choose to view **All Events** or **Selected Events**.
7. Click the **Choose** button and select the user who made the changes:
   a. Type the name of a user in the search box.
   b. To narrow your search, click **Options**. From the **Search In** list, select the name of the property to search. Click **Options** to close the Options panel.
   c. Click **Search**.
   d. Click the plus sign next to a name to add the user or group to the group.
   e. Click the **Save** button.
8. To display the changes during a specific date range, enter start and end dates.
9. Click **Download Results** to download a comma-separated values file of the events.

Send email messages to group members

You can send an email to the members of a group. The email is sent to each user in the group as well as to the users in any groups in the group.

To send an email to group members:

1. On the navigation bar, click **Users & Groups**.
2. Click the **Groups** tab.
3. Locate the group that you want to send an email to.
4. From the group's **Actions** menu, select **Email Group Members**.
5. Enter a subject for the email in the **Subject** field.
6. Type the email message in the **Body** field.

   Use the editing tools to format the body text, create numbered and bulleted lists, and add links, graphics, or tables.
7. To format the email body text as HTML click the **Format Text as HTML** checkbox. To format text as plain text, ensure the box is unchecked.

8. Enter the email addresses of additional recipients in the **To:**, **CC:** and **BCC:** fields. If multiple addresses are entered in a single field, separate each address with a semicolon.
9. Click the **Send copy to me** checkbox to receive a copy of the email.
10. Click **Send**. A confirmation message is displayed.

Index