User Management

Working with User Roles

User roles define the following:

- what a user sees when they log in to the Uptime Infrastructure Monitor Monitoring Station
- the items that a user can add, view, edit, or delete when using the Monitoring Station

The user roles that you create should reflect that needs of the users to whom the roles apply. For example, a user who needs to generate only graphs and reports does not need to be able to view or add accounts for other Uptime Infrastructure Monitor users.

Adding User Roles

To add user roles, do the following:

1. Click **Users**.
2. In the tree panel, click **Add New User Role**.
   The **Add User Role** window appears.
3. Type a name for this role in the **Name of User Role** field.
   This name appears in the Uptime Infrastructure Monitor Web interface.
4. Optionally, provide a **Description of User Role**.
5. In the first **Permissions** area of the **Add User Role** window, you assign the user permissions to **View**, **Add**, **Edit**, or **Delete** the following items by clicking the check box beside each item:
   - Users
   - Elements
   - Services
   - Element Groups
   - Action Profiles
   - Alert Profiles
   - Time Periods
   - Service Level Agreements
   - Element Views
6. Optionally, in the second **Permissions** area enable one or more of the following options by clicking the **Allowed** check box:
   - Administrator
     The user can perform all Uptime Infrastructure Monitor administration tasks.
   - Acknowledge Alerts
     The user can acknowledge an alert. See Understanding Alerts for more information.
   - Save Reports
     The user can save reports. Links to the saved reports appear in **My Portal**, or the user can save reports to a local or network drive. See Saving Reports for more information.
   - Manage Plugins and Gadgets
     The user can manage custom service monitors and dashboard gadgets using the Extension Manager. See Plugin Monitors or Managing Gadgets for more information.
   - Manage Dashboards
     The user can create a new dashboard layout and add gadgets to it. See Custom Dashboards for more information.
7. Click **Save**.

Viewing User Roles

You can view a user role to ensure that the permissions for the role are properly configured.

To view user roles, click **View User Roles** in the tree panel.

A list of the user roles appears in the **Users** subpanel. Clicking a user role displays a table that summarizes the role's configured permissions; those which are granted as denoted by a green check mark.

Editing User Roles

To edit user roles, do the following:

1. In the tree panel, click **View User Roles**.
2. Click the name of the user role that you want to edit, and then click **Edit User Role** in the **Users** subpanel.
   The **Edit User Roles** window appears.
3. Edit the user role information as described in the section Adding User Roles.

Working with Users

Users are the individuals who have access to Uptime Infrastructure Monitor and its various functions. You can grant permissions to users to do any or all of the following:

- view information about specific systems in your environment
- generate and save reports about specific systems
- receive alerts

Adding Users

To add users, do the following:

1. In the tree panel, click **Add New User**.
   The **Add User** window appears.
2. In the **Username** field, type a name for the user, which is used to log into Uptime Infrastructure Monitor.
   If you are using Active Directory or an LDAP directory to authenticate Uptime Infrastructure Monitor users, the user name you input should be identical to the user's name in the central directory.
3. If AD/LDAP is enabled for user authentication, leave the **Password** field blank; otherwise enter a password that is stored in the Uptime Infrastructure Monitor DataStore.
   If using an AD or LDAP directory to authenticate users, Uptime Infrastructure Monitor refers to the directory for password information during user login. For more information, see Changing How Users Are Authenticated.
4. If you have set a user password, re-enter it in the **Confirm Password** field.
5. Enter the full name of the user in the **First Name** and **Last Name** fields.
6. Optionally, enter the user's geographical location or department in the **Location** field.
7. If the user is receiving alerts via email, enter the user's email address in the **Email Address** field.
8. Select one of the following options from the **Time Period for Emailing** dropdown list:
   - 24x7
   - Never
   - 9am to 5pm weekdays
   - another Monitoring Period that you have previously created
9. If the user receives alerts on a cell phone or pager, enter the email address of the user's cell phone or pager in the **Pager/Cellphone Address** field.
   The email address takes the following format:
   `<number>@mobile_provider_domain`
   Where `<number>` is the user's cell phone number, and `mobile_provider_domain` is the Internet domain of the user's mobile phone service.
   For example, `4165551234@mymobile.com`.
10. Select an option from the **Time Period for Pager/Cellphone Messages** dropdown list.
    The options are the same as the ones listed in Step 8.
11. If the user receives alerts via the Window messaging service, enter the name of the user's computer in **User's Windows Desktop Hostname** field.

    > To receive popup alerts, you must enable the Windows messaging service on the user's computer. See Enabling the Windows Messaging Service for information.

12. Enter the workgroup or domain to which the user's computer belongs in the **User's Windows Desktop Workgroup** field.
13. Select an option from the **Time Period for Windows Popups** dropdown list
    The options are the same as the ones listed in Step 8.
14. Select the user's **Default Login Dashboard**.
15. If the user receives alerts, select the **Should the user receive alerts?** option.

    > If you select this option, you must also enter information in the Email Address or Pager/Cellphone Address fields.

16. If you selected the **Should the user receive alerts?** option in the previous step, select one or more of the following options:
    - **Alert on Critical**: the user receives an alert when Uptime Infrastructure Monitor detects a critical problem with one or more of monitored services
    - **Alert on Warning**: the user receives an alert when Uptime Infrastructure Monitor detects a potential problem with one or more monitored services
    - **Alert on Unknown**: the user receives an alert when Uptime Infrastructure Monitor detects an error in the configuration of the monitor, or if Uptime Infrastructure Monitor cannot execute the service check
    - **Alert on Recovery**: the user receives an alert when the service recovers from an error (e.g., an application, process or service restarts, or a server reboots)
17. Click the **Show Tips** option to disable graphical tool tips on pages like **View Notification Groups**.
18. Select a role for the user from the **User Role** dropdown list.
    For more information on user roles, see the section Working with User Roles.
19. In the **Available User Groups** field, select the user group to which you want to add this user, and then click **Add**.
    For more information on user groups, see the section Working with User Groups.
20. Click **Save**.

Viewing Users

To view all Uptime Infrastructure Monitor users, click **Users** on the main toolbar. When you are viewing other information on this **Users** panel, you can also click **View Users** in the tree panel.

Editing User Information

To edit user information, do the following:

1. Do one of the following:

   - Click the Edit icon beside the name of the user.
   - Click the name of the user whose information you want to edit, and then click **Edit User** on the **User** information page.

   The **Edit User** window appears.
2. Edit the information as described in the Adding Users section.

Deleting Users

To delete a user, click its corresponding Delete icon on the main Users page.

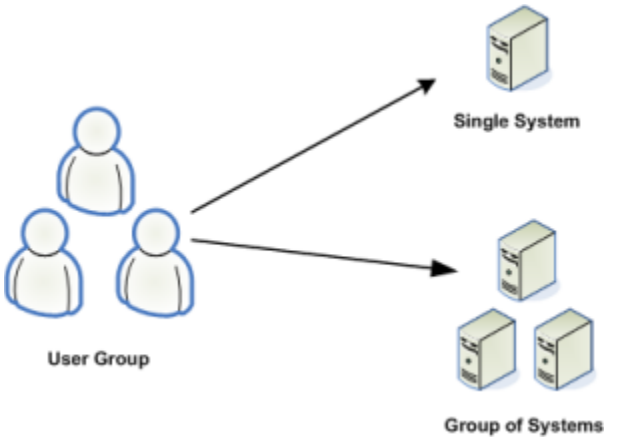
Because user accounts, user roles, and user groups are autonomous entities in Uptime Infrastructure Monitor, deleting a specific user account does not affect the role it was assigned, or the group to which it belonged. However, any reports or custom dashboards created and shared with a user group also are deleted. Before deleting a user account, ensure you re-create the account's reports and dashboards on another account.

Working with User Groups

User groups are sets of Uptime Infrastructure Monitor users who are assigned similar privileges. These privileges enable the members of a group to do the following:

- work with specific systems or network devices
- receive Uptime Infrastructure Monitor alerts from those systems and devices
- participate in any number of defined service alert monitoring escalation paths

A member of a user group can view either individual systems or multiple systems in a system group:



Each Uptime Infrastructure Monitor user must belong to at least one user group. In a small installation of Uptime Infrastructure Monitor there may only be one user and one user group. In larger installations, you can set up such user groups as Operators, Help Desk, System Administrators, Network Administrators, DBAs, Development, QA, Operations Management, and the like.

Adding User Groups

To add user groups, do the following:

1. Click **Users**.
2. In the tree panel, click **Add New User Group**.
3. Enter a name for this group in the **User Group Name** field.
4. Optionally, type a short description in the **User Group Description** field.
5. Select the users to add to the group in the **Available Users** list, then click **Add**.
6. Optionally, select one of the systems or Elements from the **Available Elements** list, then click **Add**.
7. Optionally, select one of the groups from the **Available Element Groups** list, then click **Add**.
8. Optionally, select one of the views from the **Available Element Views** list, then click **Add**.
9. Click **Save**.

Viewing User Groups

To view user groups, click **View User Groups** in the tree panel.

A list of user groups appears in the **User Groups** subpanel.

Editing User Groups

To edit user groups, do the following:

1. In the tree panel, click **View User Groups**.
2. Do one of the following:
    - Click the **Edit** icon beside the name of the user group.
    - Click the name of the user group whose information you want to edit, and then click **Edit User Group** in the **User Group** subpanel.

   The **Edit User Group** window appears.
3. Edit the information as described in the section Adding User Groups.

Deleting User Groups

To delete user groups, do the following:

1. In the tree panel, click **View User Groups**.
2. Click the **Delete** icon beside the name of the user group that you want to delete.
   Note that you cannot delete the SysAdmin user group.
3. On the warning dialog box that appears, click **OK**.

Managing Distribution Lists

A Distribution List allows you to use an email alias to send alerts to end users who, aside from wanting to be informed of status alerts, have no other reason to use Uptime Infrastructure Monitor. Using a Distribution List is an easy way to broadcast to a large group of users without having to create and manage individual Uptime Infrastructure Monitor user profiles for each member.

Distribution Lists, like individual user profiles, are associated with Notification Groups, and can be configured to broadcast specific types of status alerts (for example, only Critical-level and Recovery alerts).

Adding Distribution Lists

To add Distribution Lists, do the following:

1. Click **Users**.
2. In the tree panel, click **Add New Distribution List**.
3. Type a descriptive name in the **Display Name** field.
   Select this name when defining a Notification Group.
4. Enter the **Email Address** field, enter the email alias you are using to notify non-Uptime Infrastructure Monitor users.
5. Select a Monitoring Period from the **Time Period for Emailing** list:
   - 24x7
   - 9am to 5pm weekdays
   - another Monitoring Period that you have previously created
6. Select the **Should the Distribution List receive alerts?** check box.
7. Configure the type of alerts those on the Distribution List receive by selecting one or more of the following check boxes:
   - **Alert on Critical**. The user receives an alert when Uptime Infrastructure Monitor detects a critical problem with one or more monitored services
   - **Alert on Warning**. The user receives an alert when Uptime Infrastructure Monitor detects a potential problem with one or more monitored services
   - **Alert on Unknown**. The user receives an alert when Uptime Infrastructure Monitor detects an error in the configuration of the monitor, or if Uptime Infrastructure Monitor cannot execute the service check
   - **Alert on Recovery**. The user receives an alert when the service recovers from an error (for example, an application, process or service restarts, or a server reboots)
8. Click **Save**.

Viewing Distribution Lists

You can view the details of a Distribution List to ensure is properly configured. The details of a Distribution List include an email address, and the conditions under which alerts are sent.

To view Distribution Lists, do the following:

1. Click **Users**.
2. In the tree panel, click **View Distribution Lists**.
   A list of Distribution Lists appears in the **Distribution Lists** subpanel.
3. Click the name of the Distribution List that you want to view.

The details of the group appear in the **Distribution Lists** subpanel.

Editing Distribution Lists

If you find that a Distribution List is not properly configured, you can edit that list.

To edit Distribution Lists, do the following:

1. Do one of the following:
   - Click the **Edit** icon beside the name of the Distribution List.
   - Click the name of the Distribution List you want to edit, then click **Edit Distribution List** on the **Distribution List Information** page.

   The **Edit Distribution List** window appears.
2. Edit the group as described in Adding Distribution Lists.

Working with Notification Groups

When Uptime Infrastructure Monitor detects a problem with a system or service in your environment, it can issue alerts to specific users. If a group of users in your enterprise should receive certain notifications, you can ensure that they do by defining Notification Groups and adding those users to the group.

A Notification Group specifies the users who receive the notifications, as well as the Alert Profile that is used to react to the problems. See the section Alert Profiles for more information.

Users can only view the Notification Groups to which they are members. While users can see the members of Notification Groups to which they belong, they can only view detailed user information for users that belong to the same user groups.

Adding Notification Groups

To add Notification Groups, do the following:

1. Click **Users**.
2. In the tree panel, click **Add New Notification Group**.
3. Type a descriptive name in the **Name of Notification Group** field.
   Select this name when defining Alert Profiles. For more information on Alert Profiles, see Alert Profiles.
4. Optionally, type a description of the group in the **Description of Notification Group** field.
5. Select one or more Alert Profiles to apply to the group from the **Available Alert Profiles** list, then click **Add**.
6. Select one or more users to add to the group from the **Available Users** list, then click **Add**.
7. Select one or more Distribution Lists to add to the group from the **Available Distribution Lists**, then click **Add**.
8. Click **Save**.

Viewing Notification Groups

You can view the details of a Notification Group to ensure that the group is properly configured. The details of a Notification Group include:

- the Alert Profiles assigned to the group
- the users in the group
- whether the users are configured to receive alerts
- the conditions on which alerts are sent to the users

To view Notification Groups, do the following:

1. Click **Users**.
2. In the tree panel, click **View Notification Groups**.
   A list of Notification Groups appears in the **Notification Groups** subpanel.
3. Click the name of the Notification Group that you want to view.
   The details of the group appear in the **Notification Groups** subpanel.
4. To view the details of an Alert Profile, click the name of the profile.

Editing Notification Groups

If you find that a Notification Group is not properly configured, you can edit that group.

To edit Notification Groups, do the following:

1. Do one of the following:
   - Click the **Edit** icon beside the Notification Group.
   - Click the name of the notification whose information you want to edit, and then click **Edit Notification Group** on the **Notification Group Information *page***.

   The **Edit Notification Group** window appears.
2. Edit the group as described in Adding Notification Groups.

Changing How Users Are Authenticated

By default, user management and authentication is based entirely in Uptime Infrastructure Monitor: a profile for a User is created in Uptime Infrastructure Monitor, and all profile information is kept in the DataStore. Uptime Infrastructure Monitor user lists exist, and are maintained, separately from any other user management framework your organization may be using. In light of this, you can elect to use Active Directory or an LDAP-based service for authentication and user detail synchronization.

If you configure Uptime Infrastructure Monitor to authenticate users against a central AD or LDAP directory, password entry on login refers to that directory instead of the DataStore. Additionally, if you choose to synchronize specific user attributes (e.g., email address), the Uptime Infrastructure Monitor user profiles draw all information from the central directory instead of the DataStore. Both measures ensure Uptime Infrastructure Monitor access is automatically kept in sync with the current access levels in your organization: Uptime Infrastructure Monitor administrators do not have to manually update user access to match staffing changes.

If user detail synchronization with Active Directory or LDAP is enabled, you can no longer manually add users from within Uptime Infrastructure Monitor: the **Add New User** option on the **Users** panel is not available.

> Regardless of which authentication and synchronization method is selected, the Uptime Infrastructure Monitor “admin” user profile is always stored, and authenticated against the password found in, the DataStore.

Active Directory Authentication

To use Active Directory for user management, you need to provide Uptime Infrastructure Monitor with your organization’s AD information. You can also define whether, and how much, user information is synchronized between AD and Uptime Infrastructure Monitor’s user list.

Enabling Active Directory for Authentication

To configure Uptime Infrastructure Monitor to check an Active Directory listing for user passwords, do the following:

1. Click **Config**.
2. In the tree panel, click **User Authentication**.
3. Click **Edit Configuration**.

4. Select **Active Directory** as the authentication method.
   You now provide access details for the Active Directory server.
5. In the **Primary Domain Controller** field, enter the host name of the server acting as the domain controller, most likely enabled as the global catalog.
6. If applicable, in the **Backup Domain Controller** field, enter the name of the server acting as an additional domain controller on the same domain.
7. Enter the **Port** through which communication to the domain controller occurs.
8. If communication to the domain controller is secure, select the **SSL** check box.
9. In the **Domain Name** field, enter the domain that contains the domain controller.
10. Continue to the next section, Defining Active Directory Synchronization Mapping, to enable and configure synchronization from the Active Directory listing to Uptime Infrastructure Monitor user profiles. If you do not wish to synchronize users, click **Save**.

Clicking **Save** switches the authentication source to Active Directory. Administrators still need to create profiles for all Uptime Infrastructure Monitor users, but do not need to set a password for each one. See Adding Users for more information.

Defining Active Directory Synchronization Mapping

Before synchronizing user details, a populated “uptime” group must already exist in the Active Directory listing; you also need to know its distinguished group name, as it is required during configuration.

All DataStore-based user profiles are deleted when you switch to Active Directory for synchronization--a list of affected users is displayed during configuration. Before continuing, you should ensure your Uptime Infrastructure Monitor users are also in the AD listing.

To configure user detail synchronization from the Active Directory list, do the following:

1. Click **Edit Configuration** to open the **User Authentication Configuration** pop-up window.
2. Select the **Synchronization Enabled** check box.
   All user synchronization configuration options appear.
3. In the **Synchronize Users** field, enter the frequency at which Uptime Infrastructure Monitor user information is synchronized with the Active Directory listing.
   By default, synchronization occurs every hour.
4. In the **AD Group Distinguished Name** field, enter the name of the AD group of Uptime Infrastructure Monitor users (for example, CN=uptime users, CN=Groups, DC=yourdomain, DC=com).
5. If required, enter an appropriate administrative **AD Username** and **AD Password** required to access the directory.
6. In the **User Name** field, provide the name attribute used to retrieve the user name (for example, sAMAcountName).
   For AD synchronization, a user name is the minimum amount of directory information Uptime Infrastructure Monitor needs to map to a user profile.
7. For the remaining **Field Mappings**, provide attributes for other user details you would like to synchronize with the Uptime Infrastructure Monitor user profile:
   a. First Name (e.g., givenName)
   b. Last Name (e.g., sn)
   c. Location (e.g., physicalDeliveryOfficeName)
   d. Email Address (e.g., userPrincipalName)
   e. Pager/Cellphone
   f. User’s Windows Desktop Host Name
   g. User’s Windows Desktop Workgroup

   > Any user attributes selected to be synchronized with the directory are not editable in Uptime Infrastructure Monitor.

8. Select a **User Role** to which any newly detected users are assigned.
9. Select a **User Group** to which any newly detected users are assigned.
10. Click **Save**.

Once saved, Uptime Infrastructure Monitor synchronizes its list of users with the Uptime Infrastructure Monitor group in Active Directory at the specified interval.

LDAP Authentication

To use LDAP for user management, you need to provide Uptime Infrastructure Monitor with your organization’s LDAP information. You can also define whether, and how much, user information is synchronized between LDAP and Uptime Infrastructure Monitor’s user list.

Enabling LDAP for User Authentication

To configure Uptime Infrastructure Monitor to check an LDAP listing for user passwords, do the following:

1. Click **Config**.
2. In the tree panel, click **User Authentication**.
3. Click **Edit Configuration**.
4. Select **LDAP** as the authentication method.
   You now need to provide access details for the Active Directory server.
5. In the **LDAP URL** field, enter the address for the LDAP server.
   If directory communication occurs through secure channels, such as TLS or SSL, ensure this is reflected in the server address (for example, `ldaps://` instead of `ldap://`).
6. Enter the **LDAP Query** that Uptime Infrastructure Monitor uses on the LDAP server to look up a user’s name.
7. Continue to the next section, Defining LDAP Synchronization Mapping, to enable and configure synchronization from the Active Directory listing to Uptime Infrastructure Monitor user profiles. If you do not wish to synchronize users, click **Save**.

Clicking *Save* switches the authentication source to the LDAP directory. Administrators still need to create profiles for all Uptime Infrastructure Monitor users, but do not need to set a password for each one. See Adding Users for more information.

Defining LDAP Synchronization Mapping

Before synchronizing user details, a populated “uptime” group must already exist in the LDAP directory. You also must know the group's distinguished name, as it is required during configuration.

Note that all DataStore-based user profiles are deleted when you switch to an LDAP directory for synchronization; a list of affected users is displayed during configuration. Before continuing, you should ensure your Uptime Infrastructure Monitor users are also in the LDAP directory.

To configure user detail synchronization from the Active Directory list, do the following:

1. Click **Edit Configuration** to open the **User Authentication Configuration** pop-up window.
2. Select the **Synchronization Enabled** check box.
   All user synchronization configuration options appear.
3. In the **Synchronize Users** field, enter the frequency at which Uptime Infrastructure Monitor user information is synchronized with the LDAP listing. By default, synchronization occurs every hour.
4. In the **LDAP Group Distinguished Name** field, enter the name of the LDAP group of Uptime Infrastructure Monitor users (e.g., CN=uptime users, CN=Groups, DC=yourdomain, DC=com).
5. If required, enter an appropriate administrative **LDAP Username** and **LDAP Password** required to access the directory.
6. In the **User Name** field, provide the attribute used to retrieve the user name.
   For LDAP synchronization, a user name is the minimum amount of directory information Uptime Infrastructure Monitor needs to map to a user profile.
7. For the remaining **Field Mappings**, provide attributes for other user details you would like to synchronize with the Uptime Infrastructure Monitor user profile:
   a. First Name
   b. Last Name
   c. Location
   d. Email Address
   e. Pager/Cellphone
   f. User’s Windows Desktop Host Name
   g. User’s Windows Desktop Workgroup

   > Any user attributes selected to be synchronized with the directory are not editable in Uptime Infrastructure Monitor.

8. Select a **User Role** to which any newly detected users are assigned.
9. Select a **User Group** to which any newly detected users are assigned.
10. Click **Save**.

Once saved, Uptime Infrastructure Monitor synchronizes its list of users with the Uptime Infrastructure Monitor group in the LDAP listing at the specified interval.

Uptime Infrastructure Monitor DataStore Authentication

By default, Uptime Infrastructure Monitor uses its own database for password storage and look-up.

If you are switching back to using the DataStore from a central AD or LDAP directory, all Uptime Infrastructure Monitor users created while either was used as the authentication method no longer have passwords. You must modify all existing user accounts to include passwords.

Enabling the DataStore for User Authentication

To use Uptime Infrastructure Monitor DataStore to store passwords for user authentication, do the following:

1. Click **Config**.
2. In the tree panel, click **User Authentication**.
3. Click **Edit Configuration**.
4. Select **Database** as the authentication method.
5. Click **Save**.