User Management

Working with User Roles

User roles define the following:

- what a user will see when they log in to the *up.time* 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 will apply. For example, a user who only needs to generate graphs and reports does not need to be able to view or add accounts for other *up.time* users.

Adding User Roles

To add user roles, do the following:

1. On the *up.time* tool bar, 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 will appear in the *up.time* Web interface.
4. Optionally, type a short description in the *Description of User Role* field.
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 checkbox 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*checkbox:
   - Administrator
     The user can perform all *up.time* 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 will appear in the *My Portal* panel, or the user can save reports to a local or network drive. Saving Reports 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 have been 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 *up.time* 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. Type a name for the user, which will be used to log into *up.time* , in the *Username* field.
   If you are using Active Directory or an LDAP directory to authenticate *up.time* 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 will be stored in the *up.time* DataStore.
   If using an AD or LDAP directory to authenicate users, *up.time* will refer 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 will be 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
   - 9am to 5pm weekdays
   - another Monitoring Period that you have previously created
9. If the user will receive alerts on their 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, *1234567890@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 will receive alerts via the Window messaging service, enter the name of the user’s computer in *User's Windows Desktop Hostname* field.
    Note - 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 Page on Login* .
15. If the user will receive alerts, select the *Should the user receive alerts?* option.
    Note - 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 step 14, select one of the following options:
    - Alert on Critical
      The user receives an alert when *up.time* detects a critical problem with one or more of monitored services.
    - Alert on Warning
      The user receives an alert when *up.time* detects a potential problem with one or more monitored services.
    - Alert on Unknown
      The user receives an alert when *up.time* detects an error in the configuration of the monitor, or if *up.time* 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.
17. Click the *Disable ActiveX Graphs* option to display graphs using a Java applet instead of in 3D.
    Note - ActiveX graphs are only available to users accessing up.time with Internet Explorer.
    Do not select this option if the user is working with Internet Explorer.
18. Click the *Show Tips* option to disable graphical tool tips on pages like *View Notification Groups* .
19. 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.
20. In the *Available User Groups* field, select the user group to which this user will belong and then click *Add* .
    For more information on user groups, see the section Working with User Groups.
21. Click *Save* .

Viewing Users

To view users, click *View Users* in the Tree panel.

A list of users appears in the *Users* subpanel.

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 section Adding Users.

Working with User Groups

User groups are sets of *up.time* users who have been assigned similar privileges. These privileges enable the members of a group to do the following:

- work with specific systems or network devices
- receive *up.time* 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. The following diagram illustrates how user groups work in *up.time* :

Each *up.time* user must belong to at least one user group. In a small installation of *up.time* 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. In the *Navigation* pane, click *Add New User Group* .
2. Enter a name for this group in the *User Group Name* field.
3. Optionally, type a short description in the *User Group Description* field.
4. Select the users to add to the group in the Available Users list, then click *Add* .
5. Optionally, select one of the systems or Elements from the *Available Elements* list, then click *Add* .
6. Optionally, select one of the groups from the *Available Element Groups* list, then click *Add* .
7. Optionally, select one of the views from the *Available Element Views* list, then click Add.
8. 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.
   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 *up.time* . Using a Distribution List is an easy way to broadcast to a large group of users without having to create and manage individual *up.time* 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 (e.g., only Critical-level and Recovery alerts).

Adding Distribution Lists

To add Distribution Lists, do the following:

1. Click *Users* on the *up.time* tool bar.
2. In the Tree panel, click *Add New Distribution List* .
3. Type a descriptive name in the *Display Name* field.
4. You will select this name when defining a Notification Group.
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 will receive by selecting one or more of the following check boxes:
   - Alert on Critical
     The user receives an alert when *up.time* detects a critical problem with one or more monitored services.
   - Alert on Warning
     The user receives an alert when *up.time* detects a potential problem with one or more monitored services.
   - Alert on Unknown
     The user receives an alert when *up.time* detects an error in the configuration of the monitor, or if *up.time* 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 will be sent.

To view Disbrituion Lists, do the following:

1. Click *Users* on the *up.time* tool bar.
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 *up.time* 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 will receive the notifications, as well as the Alert Profile that will be 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* on the *up.time* tool bar.
2. In the Tree panel, click *Add New Notification Group* .
3. Type a descriptive name in the *Name of Notification Group* field.
   You will 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 or not 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* on the *up.time* tool bar.
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 *up.time* : a profile for a User is created in *up.time* , and all profile information is kept in the DataStore. *up.time* 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 *up.time* to authenticate users against a central AD or LDAP directory, password entry on login will refer to that directory instead of the DataStore. Additionally, if you choose to synchronize specific user attributes (e.g., email address), the *up.time* user profiles will draw all information from the central directory instead of the DataStore. Both measures ensure *up.time* access is automatically kept in sync with the current access levels in your organization: *up.time* 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 will no longer be able to manually add users from within *up.time* : the *Add New User* option on the *Users* panel will not be available.

Note - Regardless of which authentication and synchronization method is selected, the up.time “admin” user profile will always be stored, and authenticated against the password found in, the DataStore.

Active Directory Authentication

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

Enabling Active Directory for Authentication

To configure *up.time* to check an Active Directory listing for user passwords, do the following:

1. On the *up.time* tool bar, click *Config* .
2. In the *Tree* panel, click *User Authentication* .
3. Click *Edit Configuration* .
4. Select *Active Directory* as the authentication method.

   You will next need to 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 Defining Active Directory Synchronization Mapping to enable and configure synchronization from the Active Directory listing to *up.time* 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 *up.time* users, but will 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 will also need to know its distinguished group name, as it will be required during configuration.

All DataStore-based user profiles will be deleted when you switch to Active Directory for synchronization--a list of affected users will be displayed during configuration. Before continuing, you should ensure your *up.time* 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 *up.time* user information will be 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 *up.time* users (e.g., 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 (e.g., sAMAcountName).

   For AD synchronization, a user name is the minimum amount of directory information *up.time* needs to map to a user profile.
7. For the remaining *Field Mappings* , provide attibutes for other user details you would like to synchronize with the *up.time* 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

   Note - Any user attributes selected to be synchronized with the directory will not be editable in up.time .
8. Select a *User Role* to which any newly detected users will be assigned.
9. Select a *User Group* to which any newly detected users will be assigned.
10. Click *Save* .

Once saved, *up.time* will synchronize its list of users with the *up.time* group in Active Directory at the specified interval.

LDAP Authentication

To use LDAP for user management, you need to provide *up.time* with your organization's LDAP information. You can also define whether, and how much, user information is synchronized between LDAP and *up.time* 's user list.

Enabling LDAP for User Authentication

To configure *up.time* to check an LDAP listing for user passwords, do the following:

1. On the *up.time* tool bar, click *Config* .
2. In the *Tree* panel, click *User Authentication* .
3. Click *Edit Configuration* .
4. Select *LDAP* as the authentication method.
   You will next 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 (e.g., " *ldaps://* " instead of " *ldap://* ").
6. Enter the *LDAP Query* that *up.time* will use on the LDAP server to look up a user's name.
7. Continue to Defining LDAP Synchronization Mapping to enable and configure synchronization from the Active Directory listing to *up.time* 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 *up.time* users, but will 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 will also need to know its distinguished group name, as it will be required during configuration.

Note that all DataStore-based user profiles will be deleted when you switch to an LDAP directory for synchronization--a list of affected users will be displayed during configuration. Before continuing, you should ensure your *up.time* 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 *up.time* user information will be 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 *up.time* 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 *up.time* needs to map to a user profile.
7. For the remaining *Field Mappings* , provide attibutes for other user details you would like to synchronize with the *up.time*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

   Note - Any user attributes selected to be synchronized with the directory will not be editable in up.time .
8. Select a *User Role* to which any newly detected users will be assigned.
9. Select a *User Group* to which any newly detected users will be assigned.
10. Click *Save* .

Once saved, *up.time* will synchronize its list of users with the *up.time* group in the LDAP listing at the specified interval.

up.time DataStore Authentication

By default, *up.time* 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 *up.time* users created while either was used as the authentication method will no longer have passwords. You will need to modify all existing user accounts to include passwords.

Enabling the DataStore for User Authentication

To use *up.time* DataStore to store passwords for user authentication, do the following:

1. On the *up.time* tool bar, click *Config* .
2. In the *Tree* panel, click *User Authentication* .
3. Click *Edit Configuration* .
4. Select *Database* as the authentication method.
5. Click Save.