

# TeamWorks 18.2.1

## Administrative User Interface Reference

March 2020

## Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.microfocus.com/about/legal/>.

**Copyright © 2017 – 2020 Micro Focus or one of its affiliates.**

---

# Contents

<b>About This Guide</b>	<b>5</b>
<b>1 Administrative Consoles</b>	<b>7</b>
<b>2 Administrative Access</b>	<b>9</b>
Assigning and Managing Port 8443 Designated Administrators . . . . .	9
Changing Passwords and SSH Access for vaadmin and root . . . . .	10
Logging In as an Administrator . . . . .	10
Port 8443 Console . . . . .	10
Port 9443 Console . . . . .	11
<b>3 Access to TeamWorks</b>	<b>13</b>
Reverse Proxy Configuration Settings . . . . .	13
<b>4 LDAP Servers and Synchronization</b>	<b>15</b>
<b>5 Licensing</b>	<b>25</b>
Installing/Updating the TeamWorks License . . . . .	25
Viewing TeamWorks License Details . . . . .	25
<b>6 Logging and Monitoring</b>	<b>27</b>
Accessing TeamWorks System Log Files . . . . .	27
Logging All HTTPS Traffic . . . . .	27
<b>7 Content Editor</b>	<b>29</b>
<b>8 Email Integration (Notifications)</b>	<b>31</b>
Configuring an Email Service for TeamWorks Notifications . . . . .	31
Email Notification Template Customization . . . . .	33
Email Notification Language Is User-specific . . . . .	34
<b>9 Memory and Performance Tuning</b>	<b>35</b>
Managing Memcached (Search Appliance Only) . . . . .	35
Changing Configuration Settings for Requests and Connections . . . . .	35
Changing the Memory Configuration Settings . . . . .	36
<b>10 Network Infrastructure</b>	<b>39</b>
Changing Network Settings . . . . .	39
Port Numbers . . . . .	40

<b>11 Product Improvement</b>	<b>43</b>
<b>12 Search and Indexing</b>	<b>45</b>
Search Index . . . . .	45
<b>13 Security</b>	<b>47</b>
Certificates . . . . .	47
Firewall Configuration . . . . .	47
Password Security (Local and External Users) . . . . .	48
<b>14 SQL Database Connection</b>	<b>49</b>
<b>15 Storage Management</b>	<b>51</b>
Managing the File Upload Size Limit . . . . .	51
Expanding the /vastorage Partition . . . . .	52
<b>16 Changing System Services Configurations</b>	<b>53</b>
Managing System Services . . . . .	53
Managing Search Appliance Services . . . . .	54
Shutting Down and Restarting the Micro Focus Appliance . . . . .	54
<b>17 Time and Locale</b>	<b>57</b>
Changing the Appliance's NTP Configuration . . . . .	57
Setting a Default Time and Locale for Non-LDAP and External Users . . . . .	57
<b>18 Updates, Patches, and Support Files</b>	<b>59</b>
Managing Field Test Patches . . . . .	59
Managing Online Updates, Including Service Packs . . . . .	59
Submitting Configuration Files to Micro Focus Support . . . . .	61
Upgrading TeamWorks to a Newer Version . . . . .	61
<b>19 Users and Groups</b>	<b>63</b>
Managing Users . . . . .	63
Viewing and Managing User Properties . . . . .	65
Managing Groups . . . . .	65

# About This Guide

This guide is for TeamWorks administrators and covers the administrative dialogs and screens for the following services and features:

- ♦ Chapter 1, “Administrative Consoles,” on page 7
- ♦ Chapter 2, “Administrative Access,” on page 9
- ♦ Chapter 3, “Access to TeamWorks,” on page 13
- ♦ Chapter 4, “LDAP Servers and Synchronization,” on page 15
- ♦ Chapter 5, “Licensing,” on page 25
- ♦ Chapter 6, “Logging and Monitoring,” on page 27
- ♦ Chapter 7, “Content Editor,” on page 29
- ♦ Chapter 8, “Email Integration (Notifications),” on page 31
- ♦ Chapter 9, “Memory and Performance Tuning,” on page 35
- ♦ Chapter 10, “Network Infrastructure,” on page 39
- ♦ Chapter 11, “Product Improvement,” on page 43
- ♦ Chapter 12, “Search and Indexing,” on page 45
- ♦ Chapter 13, “Security,” on page 47
- ♦ Chapter 14, “SQL Database Connection,” on page 49
- ♦ Chapter 15, “Storage Management,” on page 51
- ♦ Chapter 16, “Changing System Services Configurations,” on page 53
- ♦ Chapter 17, “Time and Locale,” on page 57
- ♦ Chapter 18, “Updates, Patches, and Support Files,” on page 59
- ♦ Chapter 19, “Users and Groups,” on page 63

## Audience

This guide is intended for TeamWorks administrators.

## Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the **comment on this topic** link at the bottom of each page of the online documentation.

## Documentation Updates

For the most recent version of the *Micro Focus TeamWorks Administration Guide* and other documentation, visit the [Micro Focus TeamWorks Documentation website \(http://www.novell.com/documentation/teamworks-18\)](http://www.novell.com/documentation/teamworks-18).

## **Additional Documentation**

You can find more information in the Micro Focus TeamWorks documentation, which is accessible from the [Micro Focus TeamWorks Documentation website \(http://www.novell.com/documentation/teamworks-18\)](http://www.novell.com/documentation/teamworks-18).

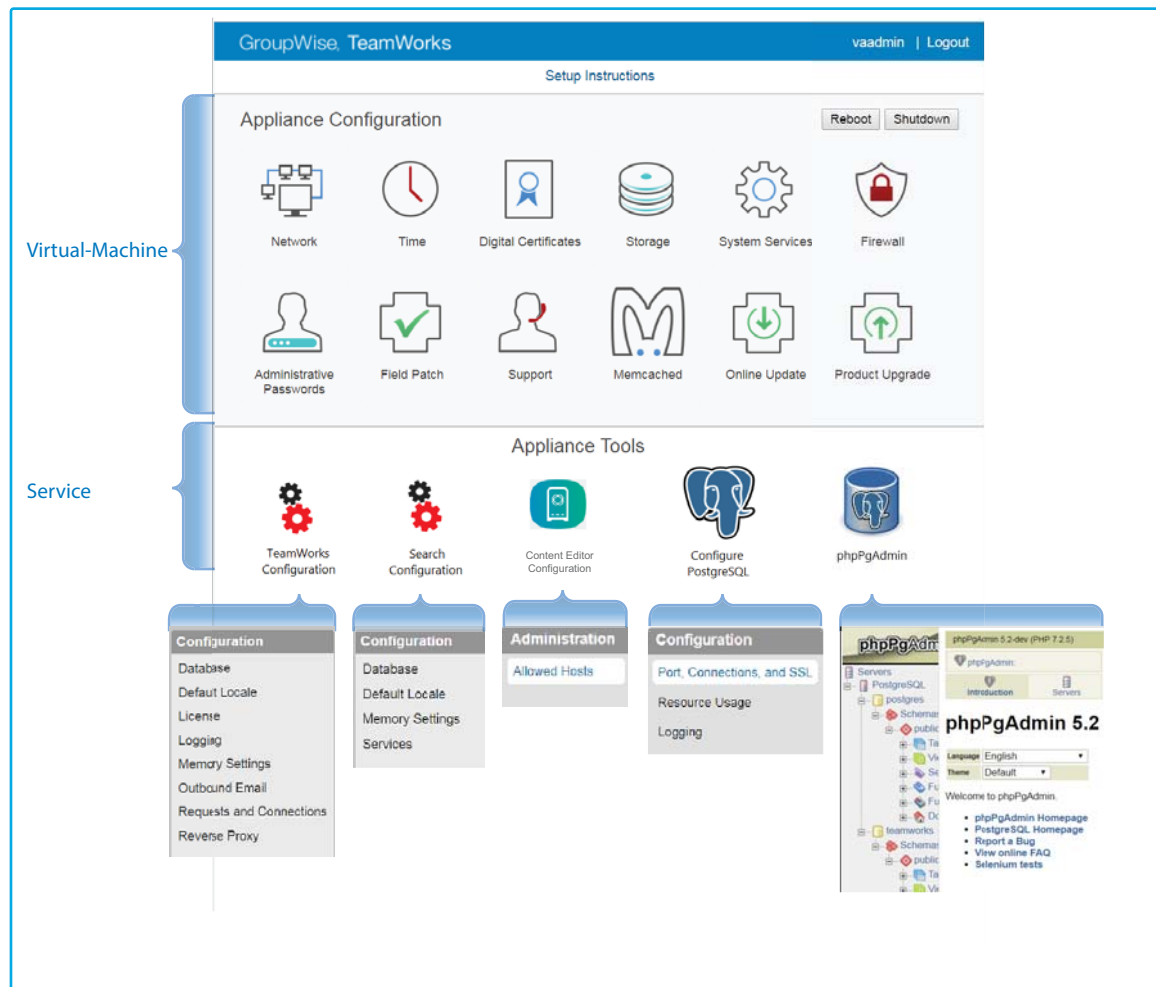
# 1 Administrative Consoles

## Port 9443 Appliance Console

**Path:** `https://appliance_ip_or_dns:9443`

- ♦ You and those with the `vaadmin` or `root` user password use this to manage virtual-machine-level settings and TeamWorks service configurations that affect an entire service and its interactions with other services.

**Figure 1-1** The Port 9443 Appliance Console (All Appliance Types Combined)

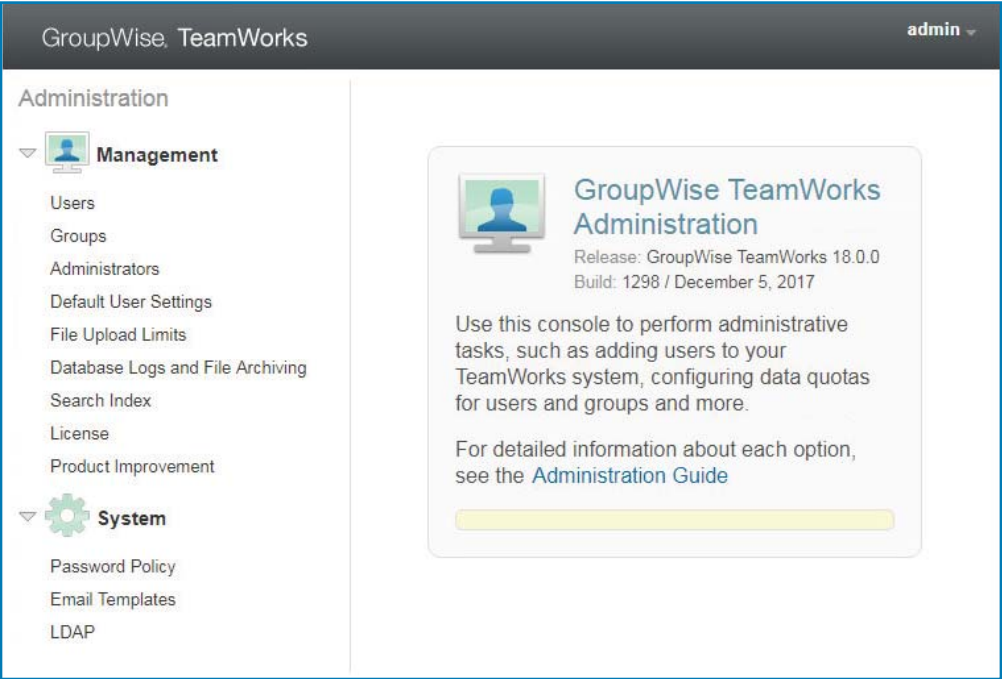


## Port 8443 TeamWorks Administration Console

**Path:** `https://appliance_ip_or_dns:8443` > **Username** > **Administration Console**

- ♦ You and other designated TeamWorks administrators use this console to manage all aspects of TeamWorks services.

Figure 1-2 The Port 8443 TeamWorks Console





# 2 Administrative Access

This section covers the following TeamWorks administrator-related tasks:

- ♦ “Assigning and Managing Port 8443 Designated Administrators” on page 9
- ♦ “Changing Passwords and SSH Access for vaadmin and root” on page 10
- ♦ “Logging In as an Administrator” on page 10

## Assigning and Managing Port 8443 Designated Administrators


**Path:** [Port 8443 TeamWorks Admin Console](#) > **Management** > **Administrators**



**Best Practice:** You can plan your Designated Administrators in advance or create them as needs develop. In either case, you should keep a record of those with administrative access on this worksheet:

- ♦ Worksheet 8 - Administrative Access

*Table 2-1 Using the Manage Administrators dialog*

Field, Option, or Button	Information and/or Action
<b>About Port 8443 Direct Administrators</b>	Port 8443 Designated Administrators can only administer the following: <ul style="list-style-type: none"><li>♦ Users</li><li>♦ Groups</li></ul>
 <b>Administrators</b>	
♦ <b>Add</b>	<ol style="list-style-type: none"><li>1. Click <b>Add</b> to add a new Designated Administrator.</li><li>2. Begin typing the user or group name you want to assign.</li><li>3. Click a user or group to add it to the list.</li></ol>
♦ <b>Remove</b>	<ol style="list-style-type: none"><li>1. Select one or more users or groups in the <b>Administrators</b> list.</li><li>2. Click <b>Remove</b>.</li></ol> <p>The selected items are removed.</p>
♦ <b>Filter</b> list	<ol style="list-style-type: none"><li>1. Type an alphanumeric string contained in the user or group names you want to display.</li><li>2. Press Enter.</li></ol> <p>The list displays only the names that contain the string you entered.</p>

Field, Option, or Button	Information and/or Action
◆ Gear icon	<ol style="list-style-type: none"> <li>1. Click the icon</li> <li>2. Select <b>Edit Column Sizes</b>.</li> <li>3. Follow the instructions in the Edit Column Sizes dialog to adjust column widths.</li> </ol> <p>Changes persist from session to session.</p>

## Changing Passwords and SSH Access for vaadmin and root

**NOTE:** If you log in as `vaadmin`, you can only change the `vaadmin` password.

**Path:** [Port 9443 Appliance Console](#) > **Administrative Passwords**

*Table 2-2 The Administrative Passwords dialog*

Field, Option, or Button	Information and/or Action
vaadmin	<ul style="list-style-type: none"> <li>◆ Acting as either <code>vaadmin</code> or <code>root</code>, type the current password, type and confirm the new password, and click <b>OK</b>.</li> </ul> <p><b>NOTE:</b> For Port 8443 console administrators, change this using the <b>Change Password</b> option in the admin user's drop-down list (upper-right corner).</p>
root SSH Access	<ul style="list-style-type: none"> <li>◆ Acting as <code>root</code>, select or deselect <b>Allow root access to SSH</b> and click <b>OK</b>.</li> </ul> <p>SSH is enabled by default. For information about how to start SSH on the appliance, see <a href="#">Chapter , "Managing System Services," on page 53</a>.</p>

## Logging In as an Administrator

### Port 8443 Console

**Path:** [Port 8443 TeamWorks Admin Console](#)

**Table 2-3** *Using the Sign In dialog*

Field, Option, or Button		Information and/or Action
♦ <b>User ID:</b>	♦	Admin
♦ <b>Password:</b>	♦	<b>First-time login:</b> Enter <code>admin</code> (case-insensitive)  You are then prompted to change the password.  ♦ <b>Subsequent login:</b> Administrative user password set above or changed in the Profile.
♦ <b>Change Password</b>	♦	<b>First-time login</b> <ol style="list-style-type: none"><li>1. Type <code>admin</code> (case-insensitive).</li><li>2. Type and confirm a new, more secure password.</li></ol> ♦ <b>Subsequent to the first-time login</b> <ol style="list-style-type: none"><li>1. Select the <b>Change Password</b> option in the admin user's drop-down list (upper-right corner).</li><li>2. Type the current password, then type and confirm a new, more secure password.</li></ol>

## Port 9443 Console

**Path:** [Port 9443 Appliance Console](#)

**Table 2-4** *Port 9443 Sign In dialog*

Field, Option, or Button		Information and/or Action
♦ <b>Username</b>	♦	Enter either <code>vaadmin</code> or <code>root</code> .
♦ <b>Password</b>	♦	Type the password for <code>vaadmin</code> or <code>root</code>



# 3 Access to TeamWorks

- ♦ “Reverse Proxy Configuration Settings” on page 13

## Reverse Proxy Configuration Settings

Use this when TeamWorks is fronted by a reverse proxy server or L4 switch that provides a single access point for TeamWorks users.

**Path:** [Port 9443 Appliance Console](#) > [Configuration icon](#) > [Reverse Proxy](#)

*Table 3-1 Using the Reverse Proxy dialog*

Field, Option, or Button	Information and/or Action
<b>Host Information</b>	<ul style="list-style-type: none"><li>♦ Specify the information for the server or switch through which internal and external users access TeamWorks.</li></ul> <p><b>IMPORTANT:</b> Two critical points:</p> <ul style="list-style-type: none"><li>♦ Configure each TeamWorks appliance that services user requests in a given deployment, with the same information.</li><li>♦ Do not configure synchronization and indexing on dedicated TeamWorks appliances with Reverse Proxy Configuration Settings.</li></ul>
♦ <b>Host:</b>	<ul style="list-style-type: none"><li>♦ For a reverse proxy server or a load balancer/L4 switch, specify the DNS hostname.</li><li>♦ For NetIQ Access Manager (NAM), enter the published DNS name. No further configuration is necessary, but the <a href="#">NAM documentation includes a few best practice points that might be useful to consider</a>.</li></ul>
♦ <b>Reverse Proxy Secure HTTP Port:</b>	<ul style="list-style-type: none"><li>♦ If you have enabled Port Redirection and secure HTTP Port access in the Network dialog, specify port 443.</li></ul>
<b>OK button</b>	<ul style="list-style-type: none"><li>♦ Click this to save your changes, then click <b>Reconfigure TeamWorks Server</b>.</li></ul> <p>This stops and restarts your TeamWorks server. Because this results in server downtime, you should restart the server during off-peak hours.</p> <p>Current user sessions are not affected. To see changes, users must log in to a new session.</p>
<b>Cancel button</b>	<ul style="list-style-type: none"><li>♦ Click this to cancel the changes you have made.</li></ul>



# 4 LDAP Servers and Synchronization

- ♦ “LDAP Configuration Dialog” on page 15
- ♦ “LDAP Server Configuration Dialog” on page 18
- ♦ “LDAP Search Dialog (User Version)” on page 22
- ♦ “LDAP Search Dialog (Group Version)” on page 23

## LDAP Configuration Dialog

**Path:** [Port 8443 TeamWorks Admin Console](#) > **System** > **LDAP**



Best Practice: Plan your LDAP Servers and use the following worksheets when working in this dialog:

- ♦ Worksheet 5 - LDAP Synchronization

*Table 4-1 Using the LDAP Configuration dialog*

Field, Option, or Button		Information and/or Action
LDAP Configuration dialog		
LDAP Servers tab		
♦ <b>Add</b> button	♦	Click this to begin the process of adding an LDAP server.  The <a href="#">LDAP Server Configuration dialog</a> opens.
♦ <b>Delete</b> button	♦	Click this to remove the selected LDAP server from the list.  <b>IMPORTANT:</b> Before you remove an LDAP server, make sure you consider the account options (Disable or Delete) that you have set for users and groups that are no longer in LDAP in the <b>User Settings tab</b> and the <b>Group Settings tab</b> .

Field, Option, or Button Information and/or Action	
♦ <b>Sync All</b> button	<p><b>TIP:</b> If you have just added or modified the LDAP Servers configuration, you must save it by clicking <b>OK</b> before running an LDAP synchronization.</p> <ul style="list-style-type: none"> <li>♦ After your users and groups are synchronized, you can click this to refresh the LDAP information in TeamWorks.</li> <li>♦ To synchronize only certain users or groups, filter the list by entering a string in the <b>Filter List</b>.</li> </ul> <p>Or</p> <ul style="list-style-type: none"> <li>♦ Click the drop-down arrow next to the Filter List and select the type of users or groups to synchronize.</li> </ul> <p>For example, Added users, Modified users, Modified groups, and so forth.</p> <ul style="list-style-type: none"> <li>♦ Users and groups that have been modified by running the LDAP sync are reported, along with information about how they have been modified.</li> </ul>
♦ <b>Preview Sync</b> button	<p><b>TIP:</b> If you have just added or modified the LDAP Servers configuration, you must save it by clicking <b>OK</b> before previewing an LDAP synchronization.</p> <ul style="list-style-type: none"> <li>♦ Use this to preview the synchronization results—users and groups that will be added or deleted, users that will be disabled, and so on—before you run the actual synchronization. <ul style="list-style-type: none"> <li>♦ To preview only certain users or groups, filter the list by entering a string in the <b>Filter List</b>.</li> </ul> </li> </ul> <p>Or</p> <ul style="list-style-type: none"> <li>♦ Click the drop-down arrow next to the Filter List and select the type of users or groups to synchronize.</li> </ul> <p>For example, Added users, Modified users, Modified groups, and so forth.</p> <ul style="list-style-type: none"> <li>♦ After you are satisfied with the results, use the <b>Sync All</b> option with the same filters to perform the actual synchronization.</li> </ul>
♦ <b>Show Sync Results</b> button	<ul style="list-style-type: none"> <li>♦ Use this to display the most recent synchronization results <i>for the current browser session</i>.</li> </ul> <p><b>NOTE:</b> If you run a synchronization, log out of TeamWorks, and then log in again, no previous synchronization results are available to view.</p>
<b>LDAP servers list</b>	
♦ <b>Server URL</b>	<ul style="list-style-type: none"> <li>♦ The URL that you specified when creating the LDAP server.</li> <li>♦ You can click this to access the <a href="#">LDAP Server Configuration dialog</a>.</li> </ul>
♦ <b>User DN</b>	<ul style="list-style-type: none"> <li>♦ This is the LDAP proxy user information for the LDAP server</li> </ul>
<b>User Settings tab</b>	
♦ <b>Register User Profiles Automatically</b>	<ul style="list-style-type: none"> <li>♦ Select this option to automatically add LDAP users to the TeamWorks site.</li> </ul>
♦ <b>Synchronize User Profiles</b>	<ul style="list-style-type: none"> <li>♦ Select this option to automatically update TeamWorks with user information changes following the initial LDAP synchronization.</li> <li>♦ The attributes that are synchronized are the attributes listed in the “mappings” box in the <b>Server Information tab</b>.</li> </ul>
<i>For user accounts provisioned from LDAP that are no longer in LDAP sub-section</i>	



---

**Field, Option, or Button    Information and/or Action**

---

- |  |  |
|--|--|
| <ul style="list-style-type: none"><li>◆ <b>Disable Account</b></li></ul> | <ul style="list-style-type: none"><li>◆ This is the default because deleting user accounts cannot be undone.<br/><br/>For more information about disabled users in TeamWorks, see <a href="#">Disabling TeamWorks User Accounts</a> in the <a href="#">TeamWorks 18.2.1: Maintenance Best Practices Guide</a>.</li></ul> |
|--|--|

- |   |   |
|---|---|
| <ul style="list-style-type: none"><li>◆ <b>Delete Account</b></li></ul> | <p><b>IMPORTANT:</b> A deleted user cannot be undeleted; this action is not reversible.</p> <ul style="list-style-type: none"><li>◆ Select this only if you have deleted users from your LDAP directory and you want the LDAP synchronization process to also remove them from TeamWorks.</li></ul> |
|---|---|

---

*Use the following when creating new users sub-section*

---

- |   |  |
|---|--|
| <ul style="list-style-type: none"><li>◆ <b>Time zone:</b></li></ul> | <ul style="list-style-type: none"><li>◆ Use this drop-down list to set the time zone for user accounts that are synchronized from the LDAP directory into your TeamWorks site.</li><li>◆ The time zone list is grouped first by continent or region, optionally by country or state, and lastly by city.</li></ul> |
| <ul style="list-style-type: none"><li>◆ <b>Locale:</b></li></ul>    | <ul style="list-style-type: none"><li>◆ Use this drop-down list to set the locale for user accounts that are synchronized from the LDAP directory into your TeamWorks site.</li><li>◆ The locale list is sorted alphabetically by language.</li></ul>  |

---

**Group Settings tab**

---

- |  |   |
|--|---|
| <ul style="list-style-type: none"><li>◆ <b>Register LDAP group profiles automatically</b></li></ul>                              | <ul style="list-style-type: none"><li>◆ Select this to automatically add new LDAP groups to the TeamWorks site.<br/><br/><b>NOTE:</b> LDAP groups are not included or supported in the TeamWorks apps for the initial release, but are currently planned to be supported in the future.<br/><br/>We recommend that you synchronize groups despite the initial limitation.</li></ul> |
| <ul style="list-style-type: none"><li>◆ <b>Synchronize group profiles</b></li></ul>  | <ul style="list-style-type: none"><li>◆ Select this to synchronize group information, such as the group description, to the TeamWorks site whenever this information changes in LDAP.</li></ul>   |
| <ul style="list-style-type: none"><li>◆ <b>Synchronize group membership</b></li></ul>  | <ul style="list-style-type: none"><li>◆ This option ensures that the TeamWorks group includes the same users (and possibly groups) as the corresponding LDAP group.<br/><br/>If this is not selected, then LDAP group changes are not reflected in TeamWorks.</li></ul>   |
| <ul style="list-style-type: none"><li>◆ <b>Delete groups that were provisioned from LDAP but are no longer in LDAP</b></li></ul> | <p><b>IMPORTANT:</b> A deleted group cannot be undeleted; this action is not reversible.</p> <ul style="list-style-type: none"><li>◆ Select this only if you have deleted groups from your LDAP directory and you want the LDAP synchronization process to also remove the groups from TeamWorks.</li></ul>   |

**Synchronization Schedule tab**

---

- |   |   |
|---|---|
| <ul style="list-style-type: none"><li>◆ <b>Enable schedule</b></li></ul>  | <ul style="list-style-type: none"><li>◆ This is selected by default so that LDAP synchronizations occur at regular intervals.</li><li>◆ You should not normally de-select this unless you are troubleshooting a problem or working with Micro Focus support to resolve a service request.</li></ul> |
| <ul style="list-style-type: none"><li>◆ <b>Every day</b></li></ul>        | <ul style="list-style-type: none"><li>◆ Select this to run an LDAP synchronization every day at the time or interval specified below.</li></ul>   |
| <ul style="list-style-type: none"><li>◆ <b>On selected days</b></li></ul> | <ul style="list-style-type: none"><li>◆ Select this if you want the LDAP synchronization to run only on specific days.</li></ul>  |
-

Field, Option, or Button	Information and/or Action
♦ <b>At HH:MM</b>	<ul style="list-style-type: none"> <li>♦ Using the drop-down lists, you can specify synchronizations to occur at a specific time.</li> <li>♦ Hours start at midnight (0) and continue through 11 p.m. (23).</li> <li>♦ Minutes can be specified using 5-minute increments.</li> </ul>
<b>Repeat every X hours</b>	<ul style="list-style-type: none"> <li>♦ As an alternative to synchronizing at a specific time, you can set a time interval and synchronize multiple times each day (for example, every four hours).</li> <li>♦ The smallest time interval you can set is .25 hours (every 15 minutes).</li> </ul>
<b>Local User Accounts tab</b>	
♦ <b>Allow log in for local user accounts (i.e user accounts not in LDAP)</b>	♦ Use this to enable or disable logging in by locally created and self-provisioned user accounts.

## LDAP Server Configuration Dialog


**Path:** [Port 8443 TeamWorks Admin Console](#) > **System** > **LDAP** > **Add button**



Best Practice: Plan your LDAP Servers and use the following worksheets when working in this dialog:

- ♦ Worksheet 4 - Users and Groups

**Table 4-2** *Using the LDAP Server Configuration dialog*

Field, Option, or Button	Information and/or Action
<b>LDAP Server Configuration dialog</b>	
	<b>Server Information tab</b>

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> <li>♦ <b>LDAP Server URL</b></li> </ul>	<p><b>WARNING:</b> If you modify an existing LDAP connection, do not modify this LDAP server URL field. Doing so can cause synchronized users to be disabled or deleted.</p> <ul style="list-style-type: none"> <li>♦ This is the host name of the LDAP server where your directory service is running.</li> </ul> <p>Specify a URL with the format your server requires, as follows:</p> <ul style="list-style-type: none"> <li>♦ <b>Non-SSL:</b> <code>ldap://hostname</code> Assumes Port 389 is used</li> <li>♦ <b>SSL:</b> <code>ldaps://hostname</code> Assumes Port 636 is used</li> </ul> <p>This requires that you import the LDAP server's root certificate into the Java keystore before attempting an LDAP synchronization. See "LDAP Synchronization Security" in the <a href="#">TeamWorks 18.2.1: Maintenance Best Practices Guide</a>.</p> <ul style="list-style-type: none"> <li>♦ If the LDAP server uses a different port number from those above, you must include the port in the URL as follows: <ul style="list-style-type: none"> <li>♦ <code>ldap://hostname:port_number</code></li> <li>♦ <code>ldaps://hostname:port_number</code></li> </ul> </li> </ul>
<ul style="list-style-type: none"> <li>♦ <b>User DN:</b> (LDAP proxy user)</li> </ul>	<p><b>IMPORTANT:</b> If you are using GroupWise 18 as an LDAP directory source, make sure you have followed the instructions in "Configuring GroupWise LDAP Provisioning (<a href="https://www.novell.com/documentation/groupwise18/gwmob18_guide_admin/data/admin_con_config.html#b1inkuao">https://www.novell.com/documentation/groupwise18/gwmob18_guide_admin/data/admin_con_config.html#b1inkuao</a>)" in the <a href="https://www.novell.com/documentation/groupwise18/gwmob18_guide_admin/">GroupWise Mobility Service 18 Administration Guide</a> (<a href="https://www.novell.com/documentation/groupwise18/gwmob18_guide_admin/">https://www.novell.com/documentation/groupwise18/gwmob18_guide_admin/</a>).</p> <p>Specifically, you must create an Admin App in GroupWise to act as the LDAP proxy user for importing and synchronizing users and groups, and you must know the GroupWise system name to use it as the organization name when specifying the proxy user name.</p> <ul style="list-style-type: none"> <li>♦ This is the LDAP proxy user and it must have sufficient rights to access the user information stored there.</li> <li>♦ You must specify a fully qualified, comma-delimited user name, along with its context in your LDAP directory tree, in the format expected by your directory service. <ul style="list-style-type: none"> <li>♦ <b>GroupWise:</b> <code>cn=gw-admin-app-name,o=gw-system-name</code></li> <li>♦ <b>eDirectory:</b> <code>cn=username,ou=organizational_unit,o=organization</code></li> <li>♦ <b>Active Directory:</b> <code>cn=username,ou=organizational_unit,dc=domain_component</code></li> </ul> </li> </ul>
<ul style="list-style-type: none"> <li>♦ <b>Password:</b> (LDAP proxy user password)</li> </ul>	<ul style="list-style-type: none"> <li>♦ You must type the password for the <b>User DN</b>.</li> </ul>
<ul style="list-style-type: none"> <li>♦ <b>Directory Type:</b></li> </ul>	<ul style="list-style-type: none"> <li>♦ Select the directory type for the LDAP server that you are configuring (<b>GroupWise</b>, <b>eDirectory</b> or <b>Active Directory</b>)</li> </ul>

Field, Option, or Button	Information and/or Action
♦ <b>Guid attribute:</b>	<ul style="list-style-type: none"> <li>♦ Based on the directory type you have selected, TeamWorks selects the standard LDAP attribute used to identify a user.</li> <li>♦ <b>entryUUID, GUID, and objectGUID:</b> These are the default, binary attributes for GroupWise, eDirectory, and Active Directory, respectively They have unique values that do not change if you rename or move a user in the LDAP directory, thus ensuring that TeamWorks modifies the existing user rather than creating a new one.</li> <li>♦ <b>Other:</b> Selecting this option in the Guid attribute drop-down prompts you to map users to a different LDAP attribute by specifying the attribute name and then clicking <b>OK</b>. <ul style="list-style-type: none"> <li>♦ You must ensure that the attribute you specify is a binary attribute. For example, the cn attribute cannot be used because it is not a binary attribute.</li> <li>♦ If you cancel the prompt to specify an attribute or specify an attribute that is not binary, TeamWorks create new TeamWorks users when names or locations change. For example, if you have a TeamWorks user who is also an LDAP user named William Jones, and if William requests that you change his name to Bill in the LDAP directory, then the next time an LDAP synchronization occurs, TeamWorks creates a new user named Bill Jones.</li> </ul> </li> </ul>



Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> <li>♦ <b>TeamWorks account name attribute:</b></li> </ul>	<ul style="list-style-type: none"> <li>♦ TeamWorks uses this attribute <ul style="list-style-type: none"> <li>♦ To create TeamWorks account names</li> <li>♦ To locate users in the LDAP directory.</li> <li>♦ As the User ID for authentication purposes.</li> </ul> </li> <li>♦ The value of this attribute must be unique in LDAP.</li> <li>♦ Attribute options depend on the directory type selected in the <b>Directory type</b> drop-down list.</li> </ul> <p>Consult with your directory administrator to determine which attribute or attributes are used in your directory service.</p> <ul style="list-style-type: none"> <li>♦ For <b>GroupWise</b> and <b>eDirectory</b>, the default available options are <b>cn</b> and <b>Other</b>.</li> <li>♦ For <b>Active Directory</b>, the default available options are <b>sAMAccountName</b>, <b>cn</b>, and <b>Other</b>.</li> <li>♦ If you select <b>Other</b> as the value for this attribute, you are prompted to enter the name of an LDAP attribute to use instead of the default choices.</li> <li>♦ Based on your findings, you might need to set up two or more LDAP sources that point to the same LDAP server but use different values for the <b>LDAP Attribute Used for TeamWorks Name</b>.</li> </ul> <p>For example, if you use Active Directory, you might need to set up one LDAP source and use cn and another to <b>sAMAccountName</b> as the <b>TeamWorks account name attribute</b>.</p> <ul style="list-style-type: none"> <li>♦ In addition to the attributes already mentioned in this section, other LDAP attributes can be used for the <b>TeamWorks account name attribute</b>, as long as the attribute is unique for each User object.</li> </ul> <p>For example, the mail LDAP attribute could be used so that TeamWorks users can log in by using their email addresses.</p>
<ul style="list-style-type: none"> <li>♦ LDAP Attribute "Mappings" box</li> </ul>	<ul style="list-style-type: none"> <li>♦ This lists the mappings between TeamWorks user information and the LDAP attributes that correspond to them.</li> </ul> <p>It is populated automatically.</p> <ul style="list-style-type: none"> <li>♦ If <b>Synchronize User Profiles</b> is enabled in the <b>User Settings tab</b>, the information associated with the mappings that are configured here, is updated each time the user account is synchronized.</li> </ul>
<b>OK</b> button	<ul style="list-style-type: none"> <li>♦ If you are modifying previously configured LDAP server information, you can click <b>OK</b>. Otherwise, you must click the <b>Users tab</b></li> </ul>
<b>Cancel</b> button	<ul style="list-style-type: none"> <li>♦ Click this to discard any LDAP server configuration changes that you have made and exit the tab.</li> </ul>
<b>Users tab</b>	
<ul style="list-style-type: none"> <li>♦ <b>Add</b> button</li> </ul>	<ul style="list-style-type: none"> <li>♦ Click this to open the <b>"LDAP Search Dialog (User Version)" on page 22</b> wherein you can specify a context where TeamWorks searches for LDAP users.</li> </ul>
<ul style="list-style-type: none"> <li>♦ <b>Delete</b> button</li> </ul>	<ul style="list-style-type: none"> <li>♦ Click this after selecting one or more list entries. For example, when the context no longer exists or when it is covered by another entry.</li> </ul>

Field, Option, or Button	Information and/or Action
<b>OK</b> button	<ul style="list-style-type: none"> <li>♦ If you are modifying previously configured User information, you can click <b>OK</b>.</li> <li>♦ If this is a new configuration, you should click the <b>Groups tab</b> and add an LDAP search context. Otherwise, expected groupings of users will not be available in TeamWorks.</li> </ul>
<b>Cancel</b> button	<ul style="list-style-type: none"> <li>♦ Click this to discard your changes and exit.</li> </ul>
<b>Groups tab</b>	
♦ <b>Add</b> button	<ul style="list-style-type: none"> <li>♦ Click this to open the <a href="#">LDAP Search Dialog (Group Version)</a> wherein you can specify a context where TeamWorks searches for LDAP groups.</li> </ul>
♦ <b>Delete</b> button	<ul style="list-style-type: none"> <li>♦ Click this after selecting one or more group Base DN entries. For example, when the context no longer exists or when it is covered by another entry.</li> </ul>
<b>OK</b> button	<ul style="list-style-type: none"> <li>♦ Click <b>OK</b> to save the LDAP server configuration.</li> </ul>
<b>Cancel</b> button	<ul style="list-style-type: none"> <li>♦ Click this to discard your changes and exit.</li> </ul>

## LDAP Search Dialog (User Version)

**Path:** [Port 8443 TeamWorks Admin Console](#) > **System** > **LDAP** > **Add button** > **Users tab** > **Add button**

**Table 4-3** Using the LDAP Search dialog (User Version)



Field, Option, or Button	Information and/or Action
 <b>LDAP Search dialog (User Version)</b>	
♦ <b>Base DN:</b>	<p><b>Best Practice:</b> Use the <b>Browse</b> icon  next to the <b>Base DN</b> field to browse the LDAP directory for the base DN that you want to use. This eliminates the risk of typing the context incorrectly. Also, if browsing fails, that means the LDAP server configuration is not correct and must be changed.</p> <ul style="list-style-type: none"> <li>♦ This is the directory context or container under which LDAP User objects are located.</li> <li>♦ When specifying this you must use the syntax required by your directory service type. <ul style="list-style-type: none"> <li>♦ <b>GroupWise:</b> <code>ou=gw-domain-name,o=gw-system-name</code></li> <li>♦ <b>eDirectory:</b> <code>ou=organizational_unit,o=organization</code></li> <li>♦ <b>Active Directory:</b> <code>ou=organizational_unit,dc=domain_component</code> </li> </ul> </li> </ul> <p><b>IMPORTANT:</b> Container names cannot exceed 128 characters. If they do, users are not provisioned.</p>

Field, Option, or Button	Information and/or Action
♦ <b>Filter:</b>	<p>♦ <b>IMPORTANT:</b> TeamWorks sets up a standard user filter for the LDAP server type.</p> <p>In almost all cases, this doesn't require modification.</p> <p>♦ <b>About User Filters:</b></p> <ul style="list-style-type: none"> <li>♦ By default, TeamWorks identifies potential users by filtering on the following LDAP directory object attributes: <ul style="list-style-type: none"> <li>♦ Person</li> <li>♦ orgPerson</li> <li>♦ inetOrgPerson</li> </ul> </li> </ul> <p>If needed, you can modify the filter by inserting the following operators:</p> <ul style="list-style-type: none"> <li>♦   OR (the default)</li> <li>♦ &amp; AND</li> <li>♦ ! NOT</li> </ul> <p>♦ <b>A Group for TeamWorks Users:</b></p> <ul style="list-style-type: none"> <li>♦ You might want to create a group for only TeamWorks users, regardless of where they are located in your LDAP directory.</li> <li>♦ After creating the group, use the following filters to search for User objects that have the group membership attribute shown below.</li> </ul> <p>Make sure you include the parentheses in your filter.</p> <ul style="list-style-type: none"> <li>♦ <b>GroupWise:</b> <code>(groupMembership=cn=group_name,ou=gw-domain-name,o=gw-system-name)</code></li> <li>♦ <b>eDirectory:</b> <code>(groupMembership=cn=group_name,ou=organizational_unit,o=organization)</code></li> <li>♦ <b>Active Directory:</b> <code>(memberOf=cn=group_name,ou=organizational_unit,dc=domain_component)</code></li> </ul> <p><b>IMPORTANT:</b> Users in eDirectory sub-groups are not synchronized.</p> <p>However, for Active Directory you can create a filter that synchronizes users in sub-groups by using the following rule object identifier (OID):</p> <p><code>&lt;attribute name&gt;:&lt;matching rule OID&gt;:=&lt;value&gt;</code></p>
♦ <b>Search subtree</b>	<p>♦ Select this if you want TeamWorks to search for users in containers underneath the base DN (that is, in subtrees).</p>

## LDAP Search Dialog (Group Version)

**Path:** [Port 8443 TeamWorks Admin Console](#) > [System](#) > [LDAP](#) > [Add button](#) > [Groups](#) > [Add button](#)

**Table 4-4** Using the LDAP Search dialog (Group Version)

Field, Option, or Button	Information and/or Action
 <b>LDAP Search dialog (Group Version)</b>	
<ul style="list-style-type: none"> <li>♦ <b>Base DN:</b></li> </ul>	<p><b>Best Practice:</b> Use the <b>Browse</b> icon  next to the <b>Base DN</b> field to browse the LDAP directory for the base DN that you want to use. This eliminates the risk of typing the context incorrectly. Also, if browsing fails, that means the LDAP server configuration is not correct and must be changed.</p> <ul style="list-style-type: none"> <li>♦ This is the directory context or container under which LDAP Group objects are located.</li> <li>♦ When specifying this you must use the syntax required by your directory service type. <ul style="list-style-type: none"> <li>♦ <b>GroupWise:</b> <code>ou=gw-domain-name,o=gw-system-name</code></li> <li>♦ <b>eDirectory:</b> <code>ou=organizational_unit,o=organization</code></li> <li>♦ <b>Active Directory:</b>  <code>ou=organizational_unit,dc=domain_component</code></li> </ul> </li> </ul> <p><b>IMPORTANT:</b> Container names cannot exceed 128 characters. If they do, groups are not provisioned.</p>
<ul style="list-style-type: none"> <li>♦ <b>Filter:</b></li> </ul>	<ul style="list-style-type: none"> <li>♦ <b>IMPORTANT:</b> TeamWorks sets up a standard group filter for the LDAP server type.</li> </ul> <p>In almost all cases, this doesn't require modification.</p>
<ul style="list-style-type: none"> <li>♦ <b>Search subtree</b></li> </ul>	<ul style="list-style-type: none"> <li>♦ Select this if you want TeamWorks to search for groups in containers underneath the base DN (that is, in subtrees).</li> </ul>



# 5 Licensing

- ♦ “Installing/Updating the TeamWorks License” on page 25
- ♦ “Viewing TeamWorks License Details” on page 25

## Installing/Updating the TeamWorks License

---

**IMPORTANT:** If you have a multi-appliance deployment, you must update the license on each TeamWorks appliance in the deployment.

PostgreSQL and TeamWorks Search appliances do not require licenses.

---

**Path:** [Port 9443 Appliance Console](#) > **Configuration icon** > **License**

*Table 5-1 Using the License (port 9443) dialog*

---

Field, Option, or Button	Information and/or Action
♦ <b>Choose File</b> button	<ol style="list-style-type: none"><li>1. Download your XML license file (from the <a href="#">Novell Customer Center (NCC)</a>) to your management workstation.</li><li>2. Rename the downloaded file to <code>license-key.xml</code>.</li><li>3. Click <b>Choose File</b>.</li><li>4. Browse to and select the downloaded and renamed license file.</li><li>5. Click <b>Open</b>.</li><li>6. Click <b>Reconfigure TeamWorks Server</b> in the <b>Configuration</b> column.</li></ol>

---

## Viewing TeamWorks License Details

**Path:** [Port 8443 TeamWorks Admin Console](#) > **Management** > **License**

*Table 5-2 Using the License (port 8443) dialog*

---

Field, Option, or Button	Information and/or Action
♦ <b>Current License</b>	<p>This section displays information about the installed license, including:</p> <ul style="list-style-type: none"><li>♦ Information about the license key, when it was issued, and who issued it.</li><li>♦ Product and version information.</li><li>♦ The effective date range.</li><li>♦ Information about user allowances.</li></ul> <p>Your contract contains details. Internal users might or might not be restricted; external (TeamWorks administrator-created) users are not restricted.</p> <ul style="list-style-type: none"><li>♦ The options or features that the license enables for use.</li></ul>

---

---

Field, Option, or Button	Information and/or Action
--------------------------	---------------------------

---

♦ <b>Reload License File</b>	
------------------------------	--

- |  |  |
|--|--|
|  | <ul style="list-style-type: none"><li>♦ If the license information displayed doesn't seem correct, click this to reload the file and refresh the display.</li><li>♦ If you need to install a new license file, see "<a href="#">Installing/Updating the TeamWorks License</a>" on page 25.</li></ul> |
|--|--|
-

# 6 Logging and Monitoring

- ♦ “Accessing TeamWorks System Log Files” on page 27
- ♦ “Logging All HTTPS Traffic” on page 27

## Accessing TeamWorks System Log Files

Path: [Port 9443 Appliance Console](#) > **System Services icon**

*Table 6-1 List of System Log Files*

Field, Option, or Button	Information and/or Action
♦ <b>Log Files column</b>	<ul style="list-style-type: none"><li>♦ Click one of the <b>Download</b> links to download the log files for the following services.<ul style="list-style-type: none"><li>♦ <b>GroupWise TeamWorks:</b> catalina.out, appserver.log The catalina.out file reports all timestamps in UTC/GMT. (TeamWorks appliance)</li><li>♦ <b>Jetty:</b> jetty.stderrout.log (TeamWorks, Search, and PostgreSQL database appliances)</li><li>♦ <b>Postfix:</b> mail (TeamWorks appliance)</li><li>♦ <b>PostgreSQL:</b> Messages.log (PostgreSQL appliance)</li><li>♦ <b>Apache 2:</b> apache2.log (TeamWorks and Search appliance)</li></ul></li></ul>

## Logging All HTTPS Traffic

Path: [Port 9443 Appliance Console](#) > **Configuration icon** > **Logging**

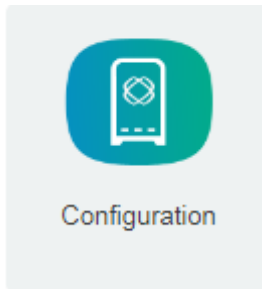
*Table 6-2 Using the Logging dialog*

Field, Option, or Button	Information and/or Action
♦ <b>Enable HTTPS traffic logging</b>	<ul style="list-style-type: none"><li>♦ Selecting this generates a single file that contains log information for all HTTPS traffic and can become large very quickly.</li><li>♦ If the file grows too large, you must disable this option.</li></ul>



# 7 Content Editor

After installing a Micro Focus Content Editor appliance, you must configure it with the DNS hostnames of each TeamWorks appliance that you want to be able to connect to it. For more information, see “[Setting Up a Content Editor Appliance](#)” in the [GroupWise TeamWorks 18.2.1: Installation and Deployment Guide](#).



**Path:** [Port 9443 Appliance Console](#) > **Content Editor Configuration icon**

*Table 7-1 Allowed Hosts dialog*

Field, Option, or Button Information and/or Action	
Allowed Hosts	<ol style="list-style-type: none"><li>1. To allow Filr and TeamWorks appliances to access the appliance's editing services, type their DNS hostnames, one per line.</li><li>2. Click <b>Submit</b>. The hostnames that you enter are listed in the left panel.</li></ol>
<b>Submit</b> button	<ol style="list-style-type: none"><li>1. Click this to add the typed DNS hostnames to the list of allowed hosts.</li></ol>
<b>Cancel</b> button	<ol style="list-style-type: none"><li>1. Click this to cancel any changes and return to the Home panel.</li></ol>



# 8 Email Integration (Notifications)

TeamWorks can send email notifications to users who request them.

- ♦ “Configuring an Email Service for TeamWorks Notifications” on page 31
- ♦ “Email Notification Template Customization” on page 33
- ♦ “Email Notification Language Is User-specific” on page 34

## Configuring an Email Service for TeamWorks Notifications

**Path:** [Port 9443 Appliance Console](#) > [Configuration icon](#) > [Outbound E-Mail](#)

---

### TIP

- ♦ If you make changes in this dialog, you must select **Reconfigure TeamWorks Server** for them to take effect.

Because reconfiguring TeamWorks causes a system restart, you should only change these settings during off-peak hours.



Best Practice: Plan the email service that will handle outgoing notifications in advance and use the following worksheet when working in this dialog:

- ♦ Worksheet 7 - Email Integration

**Table 8-1** Outbound Email dialog

---

Field, Option, or Button	Notes
--------------------------	-------

---



**Outbound  
Email dialog**

- |  |   |
|--|---|
| ♦ <b>Use Local Postfix Mail Server</b> | By default, TeamWorks is configured with an active Postfix mail server system. <ul style="list-style-type: none"><li>♦ To use another mail system (such as GroupWise), deselect this option, then specify the appropriate information for the system that TeamWorks will use instead.</li></ul> |
|--|---|

**IMPORTANT:** The TeamWorks Postfix server and GroupWise 18 servers cannot communicate by default because GroupWise 18 requires Secure SMTP (SMTPS). For more information about this issue and possible workarounds, see “[GroupWise, TeamWorks, and Secure SMTP](#)” in the [TeamWorks 18.2.1 Planning Your TeamWorks Deployment—Best Practices](#).

Field, Option, or Button	Notes
♦ <b>Protocol:</b>	<p>♦ Specify whether the email system that TeamWorks will leverage uses SMTP or SMTPS (secure SMTP).</p> <p>For GroupWise, check how the Internet Agent is configured.</p> <p>♦ If the email system requires SMTPS, see “<a href="#">Email Communications Security</a>” in the <i>TeamWorks 18.2.1: Maintenance Best Practices Guide</i>.</p>
♦ <b>Host:</b>	<p>♦ Specify the host name of the mail server that TeamWorks will leverage.</p> <p>If you are using GroupWise, this is the host name of a server where the Internet Agent is running.</p>
♦ <b>Port:</b>	<p>♦ Specify the port through which TeamWorks can connect to the SMTP mail server.</p> <p>GroupWise always uses port 25, even when SSL is enabled.</p> <p>Some mail servers require port 465 or 587 for SMTPS connections.</p>
♦ <b>Time zone:</b>	<p>♦ You can change the time zone if you want TeamWorks to use an email time stamp that is different from the time zone where the server is located.</p> <p>The time zone list is grouped first by continent or region, optionally by country or state, and lastly by city.</p>
♦ <b>User Name:</b>	<p>♦ Specify the email address that TeamWorks will use when sending emails.</p> <p>If the email server requires authentication, TeamWorks sends this username.</p> <p>Many SMTP mail hosts require a valid email address before they establish the SMTP connection.</p> <p>Although some email systems can construct a valid email address if you specify only a valid user name, you should provide a valid email address to ensure a successful connection.</p> <p>Email notifications from TeamWorks will show this email address in the <b>From</b> field.</p>
♦ <b>Password:</b>	<p>♦ If the email server requires passwords, specify the password for the user name.</p>
♦ <b>Authentication Required</b>	<p>♦ If the email server TeamWorks is leveraging requires authentication, select this option.</p> <p><b>GroupWise</b> The GroupWise Internet Agent does not require authentication for inbound messages. However, the <code>/forceinboundauth</code> startup switch in <code>gwia.cfg</code> will cause the Internet Agent to refuse SMTP connections unless a valid email user name and password are provided.</p> <p>The Internet Agent can accept just the user name or the full email address.</p> <p><b>Exchange</b> If you set up the outbound email server to require authentication (by selecting the option <b>Authentication Required</b>), Exchange must be configured to allow the From address to be different from the user who is configured for Exchange authentication. The Exchange permission that you need to add is <code>ms-Exch-SMTP-Accept-Any-Sender</code>.</p> <p>This is needed because Exchange, by default, requires that the From address of outbound emails match the exchange user who is configured for authentication, and many TeamWorks emails place the email address of the user performing an action in the From field.</p>



Field, Option, or Button	Notes
♦ <b>Allow sending e-mail to all users</b>	<ul style="list-style-type: none"> <li>♦ If you select this option, users can send email to the All Users group.</li> <li>This is disabled by default because of the potential for users to send large numbers of emails.</li> </ul>
♦ <b>Force HTTPS links</b>	<ul style="list-style-type: none"> <li>♦ Select this if all links in TeamWorks-generated email messages should be HTTPS instead of HTTP.</li> <li>Otherwise, TeamWorks uses its connection (HTTP or HTTPS) with the emailing user as the link protocol.</li> </ul>
♦ <b>Enable STARTTLS</b>	<ul style="list-style-type: none"> <li>♦ Select this option if the email service that TeamWorks is leveraging requires TLS over SMTP for secure email.</li> </ul>
♦ <b>From e-mail address override:</b>	<ul style="list-style-type: none"> <li>♦ If you don't want the <b>User Name</b> email address used in the <b>From</b> field in TeamWorks messages, specify a different address here.</li> </ul>
♦ <b>Connection Timeout:</b>	<ul style="list-style-type: none"> <li>♦ Specify the amount of time for TeamWorks to wait before timing out on a connection request to the email host.</li> </ul>
♦ <b>Test Connection</b>	<ul style="list-style-type: none"> <li>♦ Click this to test your Outbound E-Mail configuration.</li> </ul>

## Email Notification Template Customization

You can customize the email notifications that TeamWorks generates in order to provide localized messages, to comply with organizational policies, and so on.

For more information about email templates, see “[Customizing Email Notifications](#)” in the *TeamWorks 18.2.1: Maintenance Best Practices Guide* and “[Email Template Customization—A Video Walkthrough](#)” in *TeamWorks 18.2.1: Maintenance Best Practices Guide*.

**Path:** [Port 8443 TeamWorks Admin Console](#) > **System** > **Email Templates**

*Table 8-2 Using the Manage Email Templates dialog*

Field, Option, or Button	Information and/or Action
♦ <b>Delete</b> button	<ul style="list-style-type: none"> <li>♦ This button is activated when you select a template in the list that has been customized.</li> <li>♦ Use it to delete a customized template that you have uploaded to TeamWorks by using the <b>Add Files</b> button.</li> <li>Removing a customized template causes TeamWorks to revert to using the default template that ships with TeamWorks.</li> </ul>
♦ <b>Add Files</b> button	<ul style="list-style-type: none"> <li>♦ Use this to upload a customized template file to the TeamWorks system.</li> </ul>
♦ <b>Name</b>	<ul style="list-style-type: none"> <li>♦ The names of the email templates that TeamWorks uses.</li> </ul>
♦ <b>Type</b>	<ul style="list-style-type: none"> <li>♦ This indicates whether TeamWorks is using a customized or default template.</li> </ul>
♦ <b>Gear</b> icon	<ul style="list-style-type: none"> <li>♦ This lets you adjust column sizes on this page.</li> </ul>

# Email Notification Language Is User-specific

TeamWorks references a user’s Locale setting to determine which language to use for an email notification.

**Path:** [Port 9443 Appliance Console](#) > **Configuration icon** > **Default Locale**

*Table 8-3 Using the Default Locale dialog*

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"><li>◆ <b>Default Locale:</b></li></ul>	<ul style="list-style-type: none"><li>◆ This establishes the default language and locale for new user profiles that are imported through LDAP. Using this option, you can reset the language that you selected during the TeamWorks configuration process.</li></ul> <p>The following points explain more about the <b>Default Locale</b> setting.</p> <ul style="list-style-type: none"><li>◆ Micro Focus appliance installations run in English only.</li><li>◆ Locales consist of language and country code options, which provide customizations that reflect country differences. For example, in the United Kingdom, the day precedes the month while in the United States, the order is opposite.</li><li>◆ You can modify the Default Locale settings for new LDAP users in the LDAP Configuration dialog, <a href="#">User Settings tab</a>.</li></ul> <p>The default language for internal (non-LDAP) users is set in the <a href="#">Default User Settings</a> dialog. You can change this when creating individual users.</p>

# 9 Memory and Performance Tuning

- ♦ “Managing Memcached (Search Appliance Only)” on page 35
- ♦ “Changing Configuration Settings for Requests and Connections” on page 35
- ♦ “Changing the Memory Configuration Settings” on page 36

## Managing Memcached (Search Appliance Only)

**Path:** [Port 9443 Search Appliance Console](#) > **Memcached icon**

*Table 9-1 Memcached configuration*

Field, Option, or Button	Information and/or Action
♦ <b>Listen Interface:</b>	♦ The URL that Memcached listens on.
♦ <b>Number of Threads:</b>	♦ The number of threads to use when processing incoming requests.
♦ <b>Max Memory:</b>	♦ Max memory that can be used by Memcached.
♦ <b>Max Simultaneous Connections:</b>	♦ Specify the number of network connections that can be handled by memcached simultaneously.

## Changing Configuration Settings for Requests and Connections

Configure the number of client requests and database connections that TeamWorks supports.

**Path:** [Port 9443 Appliance Console](#) > **Configuration** > **Requests and Connections**

**Table 9-2** *Using the Requests and Connections dialog*

Field, Option, or Button	Information and/or Action
<b>Requests and Connections</b>	<ul style="list-style-type: none"> <li>♦ <b>Max Threads:</b> The maximum number of simultaneous client request threads that TeamWorks will support. Default: 250</li> <li>♦ <b>Max Active:</b> The maximum number of database connections that can be allocated simultaneously from this pool. Default: 300</li> <li>♦ <b>Max Idle:</b> The maximum number of database connections that can be simultaneously idle in this pool. Default: 300</li> <li>♦ <b>Scheduler Threads:</b> The size of the thread pool used for background execution of scheduled tasks. Default: 20</li> <li>♦ <b>Max REST Requests (upload/download):</b> The maximum number of concurrent desktop and mobile, upload and download requests that TeamWorks will handle simultaneously. Default: 50 Ensures that TeamWorks does not exceed capacity. Excess requests are cached so that TeamWorks can respond when it has bandwidth.</li> <li>♦ <b>Session Timeout:</b> The maximum number of concurrent desktop and mobile, upload and download requests that TeamWorks will handle simultaneously. Default: 240 By default, if a user's Micro Focus TeamWorks session is idle for four hours (240 minutes), TeamWorks logs the idle user out. For increased convenience to TeamWorks users, you can make the session timeout interval longer. For increased security for your TeamWorks site, you can make the session timeout shorter.</li> </ul>
<b>OK</b> button	<ul style="list-style-type: none"> <li>♦ After clicking this, you must click <b>Reconfigure TeamWorks Server</b> for the changes to take effect.</li> </ul>
<p><b>TIP:</b> Extremely large TeamWorks sites requesting numerous client requests and database connections might see improved performance by increasing these settings.</p>	

## Changing the Memory Configuration Settings

**Path:** [Port 9443 Appliance Console](#) > [Configuration icon](#) > [Memory Settings](#)

**Table 9-3** Using the Memory Settings dialog

Field, Option, or Button	Information and/or Action
<b>JVM Settings</b>	<p><b>Best practice recommendation:</b> Set both sizes to 66% of total RAM (see “Appliance Memory and CPU” in the <a href="#">GroupWise TeamWorks 18.2.1: Installation and Deployment Guide</a>).</p> <p><b>IMPORTANT:</b> Values must end with <code>g</code> or <code>m</code> and cannot contain fractional values. For example, to set the JVM min heap size to 1.5 GB, specify <code>1536m</code>.</p> <ul style="list-style-type: none"> <li>♦ <b>JVM Heap Size:</b> The upper limit that the system will allocate to the TeamWorks appliance’s JVM processes.</li> <li>♦ <b>Total System Memory:</b> The total RAM allocated to this appliance.</li> <li>♦ <b>Allow generation of a system dump on a user signal:</b> Causes generation of a system dump in addition to a heap dump and java core dump at the time a dump is triggered on a user signal.  This can be useful when troubleshooting issues with your TeamWorks system. However, a system dump takes more time and the files consume more disk space than a heap dump or java core dump.</li> <li>♦ <b>Java Home:</b> This location is shown for information only and cannot be changed.</li> </ul>
<b>Search Service Settings</b> (All-in-One appliance)	<ul style="list-style-type: none"> <li>♦ <b>JVM Heap Size:</b> The upper limit that the system will allocate to the Search service’s JVM processes on an all-in-one TeamWorks appliance.</li> </ul>
<b>Search Service Settings</b> (Search appliance)	<ul style="list-style-type: none"> <li>♦ <b>JVM Heap Size (MB):</b> The upper limit that the system will allocate to the Search service’s JVM processes on a TeamWorks Searchappliance.</li> </ul>
<b>Database Service Settings</b> (All-in-One appliance)	<ul style="list-style-type: none"> <li>♦ <b>Shared Buffers:</b></li> <li>♦ <b>Effective Cache Size:</b></li> </ul>
<b>Messaging Service Settings</b>	<ul style="list-style-type: none"> <li>♦ <b>Memory High Water Mark:</b> Increase or decrease as needed.</li> </ul>
<b>Memory Cache Service Settings</b>	<ul style="list-style-type: none"> <li>♦ <b>Memory Cache Max Heap:</b> Increase or decrease as needed.</li> </ul>
<b>OK</b> button	<ul style="list-style-type: none"> <li>♦ After clicking this, you must click <b>Reconfigure TeamWorks Server</b> for the changes to take effect.</li> </ul>



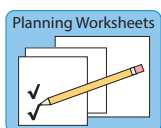
# 10 Network Infrastructure

- ♦ “Changing Network Settings” on page 39
- ♦ “Port Numbers” on page 40

## Changing Network Settings

The settings in this dialog are set during initial deployment.


**Path:** [Port 9443 Appliance Console](#) > **Network icon**



Best Practice: Be sure to update your record:

- ♦ Worksheet 9 - Network Support

**Table 10-1** Using the Network (DNS, NIC, Port 9443 Access restrictions) dialog

Field, Option, or Button		Information and/or Action
 <b>Network (IP Infrastructure)</b> dialog		Worksheet 20 - Network Support (IP Address Infrastructure Information and Appliance-Specific IP Configuration Settings)
<b>DNS Configuration</b> section		
♦ <b>Name Servers:</b>	♦	You can modify the name servers.
♦ <b>Search Domains:</b>	♦	If this field is left blank, it is auto-populated with the domain of the appliance hostname. For example, if the hostname of the appliance is <code>TeamWorks.mycompany.com</code> , the domain is auto-populated with <code>mycompany.com</code> .
♦ <b>Gateway:</b>	♦	Make sure that this matches any of the other changes you have made in this dialog.
<b>NIC Configuration</b> section		
	♦	In this section, you can modify the IP address, hostname, and network mask of any Network Interface Controller (NIC) associated with the appliance. (If you configured multiple NICs for the TeamWorks appliance, you can configure the additional NICs.)
	♦	In the <b>NIC Configuration</b> section, click the ID of the NIC.
	♦	Edit the IP address, hostname, or network mask.
		If you change the IP address, you must restart the appliance in order for the change to be reflected.
	♦	Click <b>OK</b> .

Field, Option, or Button Information and/or Action	
<b>Appliance Administration UI (Port 9443) Access Restrictions</b> section	
<ul style="list-style-type: none"> <li>♦ <b>Allowed Networks:</b></li> </ul>	<ul style="list-style-type: none"> <li>♦ To limit administrative access, specify the IP address of any networks from which you want administrators to access the TeamWorks site.</li> <li>♦ Leave this section blank to allow administrative access from any network.</li> </ul>
<b>Proxy Settings</b> section	
<b>Use a Proxy ...</b> checkbox	<ul style="list-style-type: none"> <li>♦ Select this if you want to configure a forward proxy server for the TeamWorks appliance.</li> </ul>
<ul style="list-style-type: none"> <li>♦ <b>Proxy URL:</b></li> </ul>	<ul style="list-style-type: none"> <li>♦ The URL address of the proxy server to be used, including the port.</li> </ul>
<ul style="list-style-type: none"> <li>♦ <b>Username:</b></li> </ul>	<ul style="list-style-type: none"> <li>♦ If required, the username for accessing the proxy server</li> </ul>
<ul style="list-style-type: none"> <li>♦ <b>Password:</b></li> </ul>	<ul style="list-style-type: none"> <li>♦ The password for the username.</li> </ul>
<b>OK</b> button	<ul style="list-style-type: none"> <li>♦ Click this to save your changes, then click <b>Reconfigure TeamWorks Server</b>.  This stops and restarts your TeamWorks server. Because this results in server downtime, you should restart the server during off-peak hours.  User sessions can be affected by the above changes.</li> </ul>
<b>Cancel</b> button	<ul style="list-style-type: none"> <li>♦ Click this to cancel the changes you have made.</li> </ul>

## Port Numbers

Table 10-2 lists the ports that you need to take into consideration when setting up TeamWorks.

As a best practice, do not change any port numbers from the default ports.

**Table 10-2** TeamWorks Port Numbers

Port Numbers	Description
80, 443	Standard Web server ports
8080, 8443	Default Tomcat ports for the TeamWorks appliance  When you install TeamWorks, Tomcat is installed along with the TeamWorks software. TeamWorks uses Tomcat as a stand-alone web server for delivering data to TeamWorks users in their web browsers. For more information about Tomcat, see the <a href="http://tomcat.apache.org">Apache Tomcat Web site (http://tomcat.apache.org)</a> .
9090, 9443	Jetty port for the appliance (Administrator Interface)
9080	Apache/HTTPD port
8005	Default shutdown port  For an explanation of the shutdown port, see <a href="http://www.wellho.net/mouth/837_Tomcat-Shutdown-port.html">Tomcat - Shutdown Port (http://www.wellho.net/mouth/837_Tomcat-Shutdown-port.html)</a> .



Port Numbers	Description
8009	Default AJP port  For an explanation of the Apache JServ Protocol port, see <i>The AJP Connector</i> ( <a href="http://tomcat.apache.org/tomcat-6.0-doc/config/ajp.html">http://tomcat.apache.org/tomcat-6.0-doc/config/ajp.html</a> ).
22	SSH port for the appliance
111	rpcbind utility
1099	Java RMI port
7380, 7443	Ganglia RRD-REST ports
8380, 8381	Default Jetty ports
8642, 8649, 8650, 8651, 8652	Ganglia web interface port
4369, 25672, 5671, and 15671	RabbitMQ messaging service port
9200, 9300	Elasticsearch server port
3306	PostgreSQL outbound port
1433	Microsoft SQL server port
25, 465	SMTP and SMTPS outbound ports
88	Kerberos port
11211	Used for memcached caching in an appliance cluster
636	Secure LDAP port
389	Non-secure LDAP port



# 11

## Product Improvement

The first time you log in to TeamWorks, after changing the admin user's password, a dialog displays that explains that the purpose of the TeamWorks data collection system is to help improve the TeamWorks product.

The data collection process runs for the first time when a TeamWorks appliance has been running for 24 hours. Thereafter, it runs weekly.

For additional information, see “[Helping Micro Focus Improve TeamWorks](#)” in the *TeamWorks 18.2.1: Maintenance Best Practices Guide*.

---

**IMPORTANT:** Micro Focus collects nothing that identifies your organization, your data, or your users.

---

**Path:** [Port 8443 TeamWorks Admin Console](#) > **Management** > **Product Improvement**

*Table 11-1 Using the Product Improvement dialog*

Field, Option, or Button	Information and/or Action
♦ <b>Collect and send the product name and version, and the number of LDAP users.</b>	♦ This option causes the TeamWorks system to send Micro Focus information about the product version and build, license type, and number of users.
♦ <b>Also collect and send information about the deployment size and configuration, and so on.</b>	♦ This option causes the TeamWorks system to send additional information about the installation, most of which is self-explanatory. <ul style="list-style-type: none"><li>♦ The <b>user</b> information doesn't include the LDAP user count because that is already available under the Tier1.</li><li>♦ The user count numbers do not include system user accounts, such as <code>admin</code>, and so on.</li><li>♦ The group count numbers do not include system groups, such as <code>www</code>, <code>admingroup</code>, and so on.</li></ul>
♦ <b>View the information collected.</b>	♦ After the system has been running 24 hours, this link displays so that you can download and review the <code>.json</code> file created by the collection process. This is the file that is sent to Micro Focus via FTP.



# 12 Search and Indexing

This section covers the following:

- ♦ [“Search Index” on page 45](#)

## Search Index

**Path:** [Port 8443 Search Appliance Console](#) > [Configuration Icon](#) > [Search Index](#)

*Table 12-1 Using the Search Appliance dialog*

Field, Option, or Button		Information and/or Action
Manage Search Index		
♦ <b>Use the Following Language for Stemming</b>	♦	Set this to the language used by most of your users for TeamWorks exchanges.  Words of other languages will still be indexed, but search results are optimized for the language specified.

Field, Option, or Button	Information and/or Action
♦ <b>Perform Full Reindex Now</b>	<p><b>IMPORTANT:</b> As a best practice, reindexing should be performed during times when TeamWorks activity is minimal, such as at night or on weekends. If it must be done during regular work hours, you can choose to allow or block access as explained below.</p> <ul style="list-style-type: none"> <li>♦ Selecting <b>Perform Full Reindex Now</b> and clicking <b>OK</b> launches the reindexing process. Status of the operation displays in the dialog until the process concludes, at which point any indexing errors are noted. <ul style="list-style-type: none"> <li>♦ Online (Allow user access during reindex) <p>Although users can continue to use TeamWorks there are costs in terms of additional time required to complete the reindexing operation as well as performance hits.</p> <p><b>WARNING:</b> You must have at least the amount of free disk space on /vastorage as the search index currently occupies.</p> <p>For example, if /vastorage is 100 GB and 25 GB are in use, then performing online reindexing is a viable option.</p> <p>On the other hand, if 55 GB are in use, there is insufficient free disk space.</p> <p>If disk space requirements are not met, the server will reach a disk full condition and go out of commission.</p> <p>You will then need to shut down TeamWorks and perform an offline full reindex to restore TeamWorks services.</p> </li> <li>♦ Offline (Block user access during reindex) <p>User access to TeamWorks is blocked and access attempts are answered with messages indicating that the system is undergoing maintenance.</p> <p>The advantage to this option is that reindexing is performed much more quickly and requires substantially fewer system resources. Therefore, this is generally preferred unless system access is critical and/or lack of TeamWorks access would have a detrimental effect on the organization.</p> </li> </ul> </li> </ul>
<b>OK</b> button	♦ Click this to save your changes and launch the reindexing process if so specified.
<b>Cancel</b> button	♦ Click this to cancel the changes you have made.

# 13 Security

Enterprise data is a critical resource that must be protected from unauthorized access, eavesdropping, corruption, unintended modification, or Trojan horses.

Generating, storing, and protecting enterprise data requires significant investments in time, money, and other resources.

TeamWorks is designed to enhance an organization's ability to use and leverage its data. It has been carefully engineered to guard against exposing data to additional vulnerabilities.

- ♦ [“Certificates” on page 47](#)
- ♦ [“Firewall Configuration” on page 47](#)
- ♦ [“Password Security \(Local and External Users\)” on page 48](#)

## Certificates

For certificate-maintenance procedures associated with this dialog, see [Certificate Maintenance](#) in the [TeamWorks 18.2.1: Maintenance Best Practices Guide](#)

**Path:** [Port 9443 Appliance Console](#) > **Digital Certificates icon**

*Table 13-1 Using the Digital Certificates Page*

Field, Option, or Button		Information and/or Action
<b>Certificates in the Selected Key Store</b>		
♦ <b>Key Store</b> drop-down	♦	Use this drop-down list to filter whether JVM or Web Application Certificates are listed.
♦ <b>File</b> drop-down	♦	This drop-down list lets you create a new key pair, import a trusted certificate or key pair, export a certificate you have selected in the list, or generate a CSR for a web application you have selected.
♦ <b>Edit</b> drop-down	♦	This exposes the option to delete a certificate you have selected.
♦ <b>View Info</b>	♦	This lets you view the information for a selected certificate
♦ <b>Reload</b>	♦	This lets you reload a selected certificate.

## Firewall Configuration

**Path:** [Port 9443 Appliance Console](#) > **Firewall icon**

Table 13-2 Using the Firewall Details page

Field, Option, or Button	Information and/or Action
Firewall Details	<p>This page is only informational, not editable.</p> <p>It lists the port numbers that TeamWorks expects to use on your network and the current status of each port.</p>

# Password Security (Local and External Users)

You can require that user passwords to the TeamWorks site meet certain criteria by enabling password complexity checking. Only locally created users and external users are affected by this setting; users whose accounts are synchronized to TeamWorks via LDAP are not affected.

Users' existing passwords are not forced to comply with the password policy; only when a user changes his or her password is the password policy put into effect.

Path [Port 8443 TeamWorks Admin Console](#) > [System](#) > [Password Policy](#)

Table 13-3 Using the Configure Password Policy dialog

Field, Option, or Button	Information and/or Action
<b>Password complexity changing requires that passwords:</b>	
<ul style="list-style-type: none"><li>◆ <a href="#">Enable Password Complexity Checking for Local and External Users</a></li></ul>	<ul style="list-style-type: none"><li>◆ When this is enabled, TeamWorks requires that passwords meet the criteria listed on the page:<ul style="list-style-type: none"><li>◆ Are at least 8 characters in length</li><li>◆ Do not contain the user's first name, last name, or user ID (these restrictions are not case-sensitive)</li><li>◆ Contain at least 3 of the following:<ul style="list-style-type: none"><li>◆ A lower-case character</li><li>◆ An upper-case character</li><li>◆ A number</li><li>◆ One of the following symbols: ~ @ # \$ % ^ &amp; * ( ) - + { } [ ]   \ ? / , . &lt; &gt;</li></ul></li></ul></li></ul>



# 14 SQL Database Connection

TeamWorks uses the SQL database for storing file and folder, and user and group metadata. You can change any of the fields in this dialog to match corresponding changes to the database server.

**Path:** [Port 9443 Appliance Console](#) > [Configuration icon](#) > [Database](#)



Best Practice: Plan your SQL database configuration in advance and use the following worksheets when working in this dialog:

- ♦ Worksheet 12 - SQL Database

**Table 14-1** Using the Database Connection dialog

Field, Option, or Button	Information and/or Action
<b>Database Connection</b> dialog	Worksheet 23 - SQL Database Connection
♦ <b>Database Type:</b>	♦ Select the appropriate option for the database server. <ul style="list-style-type: none"> <li>♦ <b>PostgreSQL:</b> Select <b>PostgreSQL</b></li> <li>♦ <b>Microsoft SQL Server:</b> Select <b>MS SQL Server</b></li> </ul>
♦ <b>Host Name or IP Address:</b>	♦ The DNS host name or IP address of your SQL server.
♦ <b>Port:</b>	♦ The port used for communications with TeamWorks.  The standard port for the database type is automatically selected.
♦ <b>Database Name:</b>	♦ The name of the database used by this TeamWorks deployment.
♦ <b>User Name:</b>	♦ The user id that TeamWorks uses to log in to the database server.
♦ <b>User Password:</b>	♦ The password for the User Name.
♦ <b>Encrypt Database Communication:</b>	♦ Select this option to encrypt data communication from the TeamWorks server to the database server.  For more information, see “ <a href="#">Database Communication Encryption</a> ” in the <a href="#">TeamWorks 18.2.1: Maintenance Best Practices Guide</a> .
<b>OK</b> button	♦ Click this to save your changes. Then click <b>Reconfigure TeamWorks Server</b> so that the changes are used by TeamWorks.
<b>Cancel</b> button	♦ Click this to cancel the changes you have made.



# 15 Storage Management

- ♦ “Managing the File Upload Size Limit” on page 51
- ♦ “Expanding the /vastorage Partition” on page 52

## Managing the File Upload Size Limit

The file upload size limit conserves disk space on your Micro Focus TeamWorks site because it prevents users from uploading large files to the TeamWorks site. There is no default upload limit.



Best Practice: Consider updating your records when working in this dialog:

- ♦ Worksheet 6 - User-Gen'd Storage & Limits

**Path:** [Port 8443 TeamWorks Admin Console](#) > [Management](#) > [File Upload Limits](#)

**Table 15-1** Using the TeamWorks Upload Limits dialog

Field, Option, or Button	Information and/or Action
Default File Upload Size Limit	<ul style="list-style-type: none"><li>♦ Unlike data quotas, there is no option to enable or disable file upload size checks.</li><li>♦ By default, file size is not limited, but if you planned your deployment using the planning worksheets, you were required to enter this as a sizing step for the /vashare mount point.</li><li>♦ You can also add different upload limits for individual users and groups as explained below.</li></ul>
♦ <a href="#">Add a Group</a> button	<p><b>IMPORTANT:</b> Group upload limits override the default limit. If users belong to more than one group, they are assigned the highest upload limit to which they are entitled through group membership.</p> <ol style="list-style-type: none"><li>1. Click this to add a group of users.</li><li>2. In the <b>Group</b> field, start typing the name of the group for which you want to set an upload limit, then click the group name when it appears in the drop-down list.  Repeat this process to add additional groups for which you want to assign the same upload limit.</li><li>3. In the <b>File Size Limit</b> field, specify the size limit for the group.</li><li>4. Click <b>OK</b>, then click <b>Apply</b> &gt; <b>Close</b> to save the group file size limit.</li></ol>

Field, Option, or Button	Information and/or Action
♦ <b>Add a User</b> button	<p><b>IMPORTANT:</b> User upload limits override default upload limits and the limits set for any groups to which users belong.</p> <ol style="list-style-type: none"> <li>1. Click this to add an individual user upload limit.</li> <li>2. In the <b>User</b> field, start typing the name of the user for which you want to set an upload limit, then click the user's name when it appears in the drop-down list.  Repeat this process to add additional users for which you want to assign the same upload limit.</li> <li>3. In the <b>File Size Limit</b> field, specify the file size limit for the user.</li> <li>4. Click <b>OK</b>, then click <b>Apply</b> &gt; <b>Close</b> to save the user file size limit.</li> </ol>

## Expanding the /vastorage Partition

**IMPORTANT:** If you need to expand the /var partition, see “[Expanding the /var Partition](#)” in the *TeamWorks 18.2.1: Maintenance Best Practices Guide*.

**Path:** [Port 9443 Appliance Console](#) > **Storage icon**

*Table 15-2 Using the Storage Expansion dialog to expand the /vastorage partition*

Field, Option, or Button	Information and/or Action
<b>Prerequisite</b>	<ul style="list-style-type: none"> <li>♦ Storage expansion requires unallocated free disk space associated with the /vastorage partition.</li> <li>♦ Shut down the appliance.</li> <li>♦ Use the tools and processes provided by your hypervisor vendor to expand the virtual disks that contain the partitions you want to expand.</li> <li>♦ Restart the appliance so that the operating system can detect the disks that have been expanded.</li> </ul>
<b>Appliance Disks Containing Unallocated Free Space:</b> If no disks are listed, nothing is available to be expanded.	
Expand partitions	<ul style="list-style-type: none"> <li>♦ After selecting the devices you want to expand, click this option.</li> <li>♦ Restart the appliance again so that the management software detects that the unallocated disk space has been used.</li> </ul>

# 16 Changing System Services Configurations

- ♦ “Managing System Services” on page 53
- ♦ “Managing Search Appliance Services” on page 54
- ♦ “Shutting Down and Restarting the Micro Focus Appliance” on page 54

## Managing System Services

**Path:** [Port 9443 Appliance Console](#) > **System Services icon**

*Table 16-1 Using the System Services dialog*

Field, Option, or Button		Information and/or Action
<b>Available System Services:</b> This varies by appliance type as listed below this table.		
♦ <b>Action</b> drop-down	♦	Use this to <b>start</b> , <b>stop</b> , or <b>restart</b> the selected service.  Before doing any of these, make sure you understand how your action will affect the appliance.
♦ <b>Options</b> drop-down	♦	Use this to set the selected service to start automatically or require a manual start.
♦ <b>Refresh List</b>	♦	Click this if the information displayed is outdated.

### TeamWorks Appliance

- ♦ **SSH:** This is the SSH service that is running on the appliance.
- ♦ **Micro Focus TeamWorks:** This is the TeamWorks service that is running on the appliance. Click **Download** to access the `appserver.log` and `catalina.out` files.
- ♦ **Jetty:** This is the Jetty service that is running on the appliance. Click **Download** to access the `jetty.stderrout.out` file.
- ♦ **PostgreSQL:** This is the PostgreSQL service that is running on the appliance. Click **Download** to access the `PostgreSQLId.log` file.

The PostgreSQL service runs on the TeamWorks appliance in a small deployment, and on the PostgreSQL appliance in a large deployment.

### Elasticsearch Search Index Appliance

- ♦ **SSH:** This is the SSH service that is running on the appliance.
- ♦ **Jetty:** This is the Jetty service that is running on the appliance. Click **Download** to access the `jetty.stderrout.out` file.
- ♦ **Search:** Click **Download** to access the `indexserver.log` file
- ♦ **Memcached:** Click **Download** to access the `jetty.stderrout.out` file.

## PostgreSQL Database Appliance

- ♦ **SSH:** This is the SSH service that is running on the appliance.
- ♦ **Jetty:** This is the Jetty service that is running on the appliance. Click [Download](#) to access the `jetty.stderrout.out` file.
- ♦ **PostgreSQL:** This is the PostgreSQL service that is running on the appliance. Click [Download](#) to access the `PostgreSQLId.log` file.

## Managing Search Appliance Services

Path: [Port 9443 Search Appliance Console](#) > [Configuration](#) > [Services](#)

*Table 16-2 Using the Services dialog to manage Search Appliance services*

Field, Option, or Button	Information and/or Action
♦ Messaging Service	<ul style="list-style-type: none"><li>♦ Displays the status of the Messaging service on this appliance (Enabled or Disabled).</li></ul> <p>You can change to the status indicated on the button by clicking it, provided that your action won't cause a state where none of the Search appliances is running the Messaging service.</p> <p>Best practice is to run the Messaging service on two of the appliances. The TeamWorks system enforces running the Messaging service on at least one Search appliance.</p>
♦ Search Services Health	<ul style="list-style-type: none"><li>♦ <b>Green:</b> Indicates that the Search system is healthy.</li><li>♦ <b>Yellow:</b> Indicates that the Search system is working to restore itself to a healthy state. For example, the system is reallocating Search Index Shards within the Search cluster.</li></ul> <p>Such operations should not normally require more than a few minutes to complete, at this point the health status should return to green.</p> <ul style="list-style-type: none"><li>♦ <b>Red:</b> Indicates that the Search system was unable to restore itself to a healthy state.</li></ul> <p>Resolving this requires that you contact Micro Focus Support.</p> <ul style="list-style-type: none"><li>♦ <b>Checking:</b> Indicates that the Search system is assessing its health status.</li></ul>
♦ Decommission Appliance	<ul style="list-style-type: none"><li>♦ Use this option when you are permanently removing a Search appliance from your TeamWorks deployment.</li></ul> <p>The option only works when <b>Search Cluster Health</b> is green.</p> <p>For more information, see “<a href="#">Permanently Removing (Decommissioning) a Search Appliance</a>” in the <i><a href="#">TeamWorks 18.2.1: Maintenance Best Practices Guide</a></i>.</p>

## Shutting Down and Restarting the Micro Focus Appliance

Path: [Port 9443 Appliance Console](#) > [Reboot](#) or [Shutdown](#)

- ♦ **Reboot:** Use this if you need to restart the Micro Focus appliance after performing maintenance.

- ♦ **Shutdown:** To ensure that appliance processes are properly terminated, you should always use this when you need to shut down a Micro Focus appliance.

Using the hypervisor's management features to power down or restart an appliance can result in system corruption.





# 17 Time and Locale

- ♦ “Changing the Appliance’s NTP Configuration” on page 57
- ♦ “Setting a Default Time and Locale for Non-LDAP and External Users” on page 57

## Changing the Appliance’s NTP Configuration

This dialog lets you adjust the NTP configuration settings that were established when the appliance was deployed.

**Path:** [Port 9443 Appliance Console](#) > **Time icon**

*Table 17-1 Using the Time dialog*

Field, Option, or Button	Information and/or Action
♦ <b>NTP Servers:</b>	♦ Type a new default NTP server.
♦ <b>Region:</b>	♦ Click the drop-down list and select a region for the appliance.
♦ <b>Time Zone:</b>	♦ Click the drop-down list and select a time zone for the appliance.
♦ <b>Hardware clock set to UTC</b>	♦ Use this option to change the hardware clock setting.

## Setting a Default Time and Locale for Non-LDAP and External Users

**NOTE:** You specify the default locale and time zone for LDAP users when you [configure LDAP synchronization](#).

On the other hand, when you create non-LDAP internal users and when external users self-provision, TeamWorks assigns `English (US)` as the default locale and `Greenwich Mean Time (GMT)` as the default time zone.

This dialog lets you change the non-LDAP internal user and external user defaults.

**Path:** [Port 8443 TeamWorks Admin Console](#) > **Management** > **Default User Settings**

**Table 17-2** *Using the Default User Settings dialog*

Field, Option, or Button		Information and/or Action
<i>Section: Settings for new internal (non-LDAP) users:</i>		
♦ <b>Time Zone:</b>	♦	Use the drop-down list to select a default time zone for TeamWorks to assign when you create Internal, non-LDAP users.
♦ <b>Locale:</b>	♦	Use the drop-down list to select a default locale for TeamWorks to assign when you create Internal, non-LDAP users.
<b>OK</b> or <b>Cancel</b>	♦	Click <b>OK</b> to apply the settings you have specified and exit this dialog, or <b>Cancel</b> to discard your changes and exit.

# 18 Updates, Patches, and Support Files

- ♦ “Managing Field Test Patches” on page 59
- ♦ “Managing Online Updates, Including Service Packs” on page 59
- ♦ “Submitting Configuration Files to Micro Focus Support” on page 61
- ♦ “Upgrading TeamWorks to a Newer Version” on page 61

## Managing Field Test Patches

You can manage field test patches for the TeamWorks appliance directly from the appliance. You can install new patches, view currently installed patches, and uninstall patches.

**Path:** [Port 9443 Appliance Console](#) > **Field Patch icon**

*Table 18-1 Using the Field Patch dialog*

Field, Option, or Button		Information and/or Action
<b>Field Test Patch</b>		
<i>Install a Downloaded Patch</i> sub-section		
♦ <b>Path to Field Patch:</b>	♦	Use the <b>Browse</b> button to navigate to a downloaded patch, then click <b>Install</b> to apply the patch.
<i>Manage Installed Patches</i> sub-section		
♦ <b>Uninstall Latest Patch</b> button	♦	Patches must be uninstalled in reverse order and only the latest patch can be uninstalled.  ♦ Select the latest installed patch, then click this button and confirm that you want the patch uninstalled.  You can then install the next patch until you have everything uninstalled as required.
♦ <b>Download Log File</b> button	♦	Click this to download the log file that tracks patch installations.

## Managing Online Updates, Including Service Packs

**Path:** [Port 9443 Appliance Console](#) > **Online Update icon**

**Table 18-2** Using the Online Update dialog

Field, Option, or Button	Information and/or Action
<b>Online Update (Automatic Update Schedule: X)</b>	<ul style="list-style-type: none"> <li>◆ This is the dialog title and it also shows which Schedule option is selected (represented by X).</li> </ul>
<b>Register Online Update Service dialog</b>	<ul style="list-style-type: none"> <li>◆ This dialog appears whenever the appliance is not registered with an update service. For example, the first time Online Update icon is clicked or when a service has been de-registered.</li> <li>◆ You must register the appliance for it to receive online updates.</li> </ul>
◆ <b>Service Type:</b>	<ul style="list-style-type: none"> <li>◆ Select the service type that the appliance will use to obtain online updates: a local Subscription Management Tool (SMT) or the Micro Focus Customer Center</li> </ul>
◆ <b>Local SMT</b>	<p>This is a server from where you can download the software updates and automatically install them to update the product.</p> <ul style="list-style-type: none"> <li>◆ <b>Hostname:</b> The hostname of the server from where you want the appliance to download software updates.</li> <li>◆ <b>SSL cert URL (optional):</b> The path to the SSL certificate for encrypting communications with the server.</li> <li>◆ <b>Namespace path (optional):</b> To enable the client to use the staging group, specify a value. Do not specify any value if you want to use the default production repositories.</li> </ul>
◆ <b>Micro Focus Customer Center</b>	<ul style="list-style-type: none"> <li>◆ <b>Email:</b> Your email address for registering the appliance to receive updates.</li> <li>◆ <b>Activation Key:</b> This is found in your NCC Portal in the same dialog as your product license.</li> <li>◆ <b>Allow Data send:</b> Select from the following options if you want to share information with the Micro Focus Customer Center: <ul style="list-style-type: none"> <li>◆ <b>Hardware Profile:</b> Shares the hardware information.</li> <li>◆ <b>Optional Information:</b> Shares information such as host type, productversion, release, architecture, timezone, and processor.</li> </ul> </li> </ul>
<b>Update service: X</b>	<ul style="list-style-type: none"> <li>◆ After you register the appliance for an update service, the service name appears in this field (represented by X).</li> </ul>
◆ Patches drop-down	<ul style="list-style-type: none"> <li>◆ <b>Needed Patches:</b> Selecting this option lists that patches that will be installed during the next manual or automatic update.</li> <li>◆ <b>Installed Patches:</b> Selecting this option lists all patches that have been previously installed.</li> </ul>
<b>Update Now tab</b>	<ul style="list-style-type: none"> <li>◆ This is selectable only when the Patches drop-down is set to <b>Needed Patches</b>.</li> <li>◆ After clicking the option, you must choose to apply either <b>All Needed Patches</b> or <b>Security Patches Only</b>.</li> <li>◆ Optionally, you can specify whether to <b>Automatically agree with all license agreements</b> and <b>Automatically install all interactive patches</b>.</li> </ul>

Field, Option, or Button	Information and/or Action
<b>View Info tab</b>	<ul style="list-style-type: none"> <li>Clicking this displays information such as a brief summary of the patch and the bug fixes in the patch.</li> </ul>
<b>Register tab</b>	<ul style="list-style-type: none"> <li>Clicking this displays the appliance's registration status, and an option to <b>Deregister</b> the appliance.</li> <li>If you deregister the appliance, the <a href="#">Register Online Update Service</a> dialog reappears.</li> </ul>
<b>Refresh tab</b>	<ul style="list-style-type: none"> <li>Clicking this refreshes the status of updates on the Appliance.</li> </ul>

## Submitting Configuration Files to Micro Focus Support

Sometimes Micro Focus Support needs to review your appliance's system configuration when processing a service request. This dialog facilitates the process and saves you time.

**Path:** [Port 9443 Appliance Console](#) > **Support icon**

*Table 18-3 Using the Support dialog*

Field, Option, or Button	Information and/or Action
<b>Support</b>	
<b>Automatically send the configuration to Micro Focus using FTP.</b>	<ul style="list-style-type: none"> <li>With this option selected, you can FTP your configuration to Micro Focus Support and include the <b>Service Request Number</b> if desired.</li> <li>The configuration is sent when you click <b>OK</b> and confirm your selection.</li> </ul>
<b>Download and save the configuration file locally, then send it to Micro Focus manually.</b>	<ul style="list-style-type: none"> <li>With this option selected, the configuration is downloaded when you click <b>OK</b> and confirm your selection.</li> <li>You must then send the file to Micro Focus through email or some other arrangement.</li> </ul>
<b>OK or Cancel</b>	<ul style="list-style-type: none"> <li>Click <b>OK</b> to send or download the file, or click <b>Cancel</b> to exit.</li> </ul>

## Upgrading TeamWorks to a Newer Version

**NOTE:** Upgrades are product releases that involve the installation of a new appliance and are indicated by a change to the major (X to X+1) or minor (X.X to X.X+1) versions of Micro Focus products.

Service Pack releases (version X.X.X. to X.X.X+1) are distributed through the Update channel (see [“Managing Online Updates, Including Service Packs” on page 59](#)) and do not involve the installation of a new appliance.

**Path:** [Port 9443 Appliance Console](#) > **Product Upgrade icon**

*Table 18-4 Using the Product Upgrade dialog*

Field, Option, or Button	Information and/or Action

# 19 Users and Groups

- ♦ “Managing Users” on page 63
- ♦ “Managing Groups” on page 65

## Managing Users

**Path:** [Port 8443 TeamWorks Admin Console](#) > **Users**



Best Practice: Plan users in advance and use the following worksheets when working in this dialog:

- ♦ Worksheet 4 - Users and Groups

*Table 19-1 Using the Users dialog*

Field, Option, or Button Information and/or Action	
<b>Users dialog (header row)</b>	
♦ <b>New</b> button	♦ Click this to begin creating a <a href="#">new non-LDAP internal user</a> .
♦ <b>Import Profiles...</b> button	<ul style="list-style-type: none"><li>♦ You can manage local users and groups by importing profile files that contain user or group information in XML format. This is a good way to simultaneously perform multiple actions on non-LDAP users and group, such as creating, modifying, or deleting users, and creating or modifying groups.</li><li>♦ Click <b>Choose File</b>, then navigate to and select the file that contains user or group profile information in XML format.</li><li>♦ Click <b>View a Sample File</b> and make sure that the format of your file matches the format that is shown in the provided sample file.</li></ul>
♦ <b>Delete</b> button	♦ The effects of this button on user accounts depends on whether the user is an LDAP, non-LDAP Internal, or External user. For more detail, see <a href="#">Deleting TeamWorks Users</a> in the <a href="#">TeamWorks 18.2.1: Maintenance Best Practices Guide</a> .
♦ <b>More</b> drop-down	<p>With one or more users selected, you can choose from the following options.</p> <ul style="list-style-type: none"><li>♦ <b>Disable User Account:</b> <a href="#">Disabling TeamWorks User Accounts</a> in the <a href="#">TeamWorks 18.2.1: Maintenance Best Practices Guide</a></li><li>♦ <b>Enable User Account:</b> This restores access through a user account that was previously disabled.</li><li>♦ <b>Add Administrator Rights:</b> Lets you assign selected users as Designated Administrators.</li><li>♦ <b>Remove Administrator Rights:</b> Lets you remove Direct-administration rights from selected users.</li></ul>

Field, Option, or Button		Information and/or Action
♦ <b>Filter List</b> field	♦	Begin typing a name and press enter to filter the list to only those users who match what you have entered.
♦ Filter Arrow drop-down	♦	<p>This lets you filter the displayed list of users using the following criteria:</p> <ul style="list-style-type: none"> <li>♦ Internal Users</li> <li>♦ External Users</li> <li>♦ Disabled Users</li> <li>♦ Enabled Users</li> <li>♦ Administrators</li> <li>♦ Non-administrators</li> </ul> <p>By default, all of the above are selected for display.</p>
♦ Gear icon	♦	Click this to adjust column sizes.
<b>Users List (below header row)</b>		
♦ <b>Full Name</b> column	♦	Displays the user's first and last names combined
♦ Arrow drop-down column	♦	<p>Provides access to the following settings for the user:</p> <ul style="list-style-type: none"> <li>♦ <b>User Properties</b> dialog: Opens the <a href="#">User Properties</a> dialog.</li> <li>♦ <b>Web Access</b> settings: Depending on what has already been configured, you can enable web access for the user, disable web access for the user, or specify that the default web access settings be used for the user.</li> </ul>
♦ <b>Type</b> column	♦	Icons indicate whether users are LDAP, non-LDAP internal, External self-provisioned, System-created, and so on.
♦ <b>Admin</b> column	♦	This indicates whether users are assigned administrative responsibilities.
♦ <b>Email</b> column	♦	This displays the email address to which TeamWorks sends notifications
♦ <b>User Id</b> column	♦	The login name of each user
<b>New User dialog</b>		
♦ <b>User ID</b>	♦	You must assign a unique user ID for each non-LDAP internal user. See <a href="#">Worksheet 4—Duplicate User and Group Accounts in TeamWorks 18.2.1 Planning Your TeamWorks Deployment—Best Practices</a> .
♦ <b>Password</b>	♦	You must assign (type and confirm) a password for the user to log in with.
♦ <b>First Name</b>	♦	You can include the user's first name
♦ <b>Last Name</b>	♦	You can also include the user's last name.
♦ <b>Picture</b>	♦	You can include a picture of the user, or the user can add it later.
♦ <b>Time Zone</b>	♦	Make sure the time zone setting is accurate.
♦ <b>Locale</b>	♦	Make sure the locale setting matches the user's language preference.
<i>Personal Information</i>		Users normally provide the following information for themselves.
♦ <b>Job Title</b>		
♦ <b>About Me</b>		



Field, Option, or Button		Information and/or Action
♦ Email		
♦ Phone		
♦ Text Messaging Email		
OK or Cancel	♦ Click <b>OK</b> to save the user information you have entered, or click <b>Cancel</b> to discard your entries.	

# Viewing and Managing User Properties

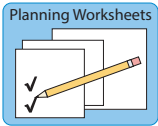
**Path:** [Port 8443 TeamWorks Administration Console](#) > **Management** > **Users** > drop-down arrow next to the user > **User Properties**

Table 19-2 Using the User Properties dialog

Field, Option, or Button		Information and/or Action
♦ <b>Profile</b> button	♦ You can change any of the following that is not synchronized from an LDAP source: <ul style="list-style-type: none"> <li>♦ User ID</li> <li>♦ Picture</li> <li>♦ Time Zone</li> <li>♦ Locale</li> <li>♦ Job Title</li> <li>♦ About Me</li> <li>♦ Email</li> <li>♦ Phone</li> <li>♦ Text Messaging Email</li> </ul>	

# Managing Groups

**Path:** [Port 8443 TeamWorks Admin Console](#) > **Groups**



Best Practice: Plan groups in advance and use the following worksheets when working in this dialog:

- ♦ Worksheet 4 - Users and Groups

**Table 19-3** *Using the Groups dialog*

Field, Option, or Button Information and/or Action	
<b>Manage Groups dialog (header row)</b>	
♦ <b>New</b> button	♦ Click this to begin <a href="#">adding a new non-LDAP internal group</a> .
♦ <b>Delete</b> button	♦ Click this to remove the selected groups from the list.
♦ <b>More</b> drop-down	With one or more groups selected, you can choose from the following options: <ul style="list-style-type: none"> <li>♦ <b>Add Administrator Rights:</b> Lets you assign selected group members as Designated Administrators.</li> <li>♦ <b>Remove Administrator Rights:</b> Lets you remove Direct-administration rights from selected groups.</li> </ul>
♦ <b>Filter List</b> field	♦ Begin typing a name and press enter to filter the list to only those users who match what you have entered.
<b>Manage Groups (below header row)</b>	
♦ <b>Type</b> column	♦ Icons indicate whether the groups are LDAP, non_LDAP internal, LDAP with Direct Admin rights, non-LDAP with Direct Admin rights.
♦ <b>Title</b> column	<ul style="list-style-type: none"> <li>♦ Displays group titles as defined in LDAP or specified when the group was created. LDAP titles cannot be changed in TeamWorks, non-LDAP titles can be changed.</li> <li>♦ Click this to edit the group, including changing the group title and the membership configuration.</li> </ul>
♦ Arrow drop-down column	<ul style="list-style-type: none"> <li>♦ Provides access to the following settings for the group: <ul style="list-style-type: none"> <li>♦ <b>Web Access</b> settings: Depending on what has already been configured, you can enable web access for all group members, disable web access for all group members, or specify that the default file downloading settings be used for all group members.</li> </ul> </li> </ul>
♦ <b>Name</b> column	♦ Displays group names as defined in LDAP or specified when the group was created. Group names cannot be changed.
♦ <b>Admin</b> column	♦ This indicates whether the group members are allowed Direct administrative responsibilities because of membership in the group.
<b>Add Group dialog</b>	
♦ <b>Description:</b> box	♦ If desired, include some text that describes the group, such as what the members of this group have in common.
♦ <b>Group membership is static</b> option	♦ Static groups are groups whose membership is directly specified and does not change based on LDAP queries.
♦ <b>Group membership is dynamic</b> option	♦ Dynamic groups are populated based on LDAP queries made by TeamWorks. Their membership changes as the meta data returned from TeamWorks's LDAP queries changes.
♦ <b>Edit group membership</b> button	♦ Click this to configure the type of group you have selected:

Field, Option, or Button Information and/or Action	
<b>OK or Cancel</b>	<ul style="list-style-type: none"> <li>Click <b>OK</b> to save the changes you've made in this dialog or <b>Cancel</b> to discard your changes.</li> <li>Make sure you have <a href="#">edited the group membership</a>. Otherwise your group will have no members.</li> </ul>
<b>Static Membership for Group dialog</b>	
<b>Allow external users and groups option</b>	<ul style="list-style-type: none"> <li>Select this to allow external users and groups to be added to the list.</li> </ul>
<b>Users tab</b>	<ul style="list-style-type: none"> <li><b>User field:</b> Begin typing a user name, then select a listed user to add it to the Membership list.</li> </ul>
<b>Groups tab</b>	<ul style="list-style-type: none"> <li><b>Group field:</b> Begin typing a group name, then select a listed group to add it to the Membership list.</li> </ul>
<ul style="list-style-type: none"> <li><b>Remove button</b></li> </ul>	<ul style="list-style-type: none"> <li>Click this to remove a selected user or group (depending on which dialog you are in).</li> </ul>
<b>Membership list</b>	<ul style="list-style-type: none"> <li>A list of the users/groups in the static group.</li> </ul>
<b>OK or Cancel</b>	<ul style="list-style-type: none"> <li>Click <b>OK</b> to save the changes you've made in this dialog or <b>Cancel</b> to discard your changes.</li> </ul>
<b>Edit Dynamic Membership dialog</b>	
Tips and Caveats	<ul style="list-style-type: none"> <li>Users must already have existing TeamWorks user accounts in order for them to be added to a TeamWorks group as described in this section. If your LDAP query includes users who are not already TeamWorks users, the users are not added to the TeamWorks group</li> <li>When you configure your LDAP connection, you must specify the name of the LDAP attribute that uniquely identifies the user (the value of this attribute never changes). For eDirectory, this value is <code>GUID</code>. For Active Directory, this value is <code>objectGUID</code>. For more information about this attribute, see <a href="#">"Guid attribute:" on page 20</a>.</li> <li>The TeamWorks process that creates a dynamic group uses the LDAP configuration settings in TeamWorks to authenticate to the LDAP directory server used to specify the Base DN (below). The credentials that are used are the LDAP server URL, user DN, and password. For more information on how to configure these and other LDAP configuration settings in TeamWorks, see <a href="#">"LDAP Servers and Synchronization" on page 15</a>.</li> <li>The Base DN set below must exist in each LDAP source. Otherwise, the membership of the dynamic group might not be updated correctly.</li> <li>If your TeamWorks site is configured with multiple LDAP sources and the base DN that you define for the dynamic group exists in each LDAP source, the membership of the dynamic group contains users from each LDAP source that match the dynamic group's filter.</li> </ul>
<ul style="list-style-type: none"> <li><b>Current Membership: button</b></li> </ul>	<ul style="list-style-type: none"> <li>Click this to open the Dynamic Group Membership windows and view the users that are included in the group based on the current configuration.</li> </ul>
<ul style="list-style-type: none"> <li><b>Base DN:</b></li> </ul>	<ul style="list-style-type: none"> <li>Use the LDAP browse button to locate the context where you want the search for users to begin.</li> </ul>

Field, Option, or Button Information and/or Action	
♦ <b>LDAP Filter:</b>	<ul style="list-style-type: none"> <li>♦ Specify the LDAP filter you want to use for the query. This is required for the search to return any results.</li> <li>♦ For an example and more information, see <a href="#">“Filter:” on page 23</a>.</li> </ul>
♦ <b>Search subtree</b> option	<ul style="list-style-type: none"> <li>♦ Select this to have the search extended into sub-containers.</li> </ul>
♦ <b>Update group membership during scheduled ldap synchronization</b> option	<ul style="list-style-type: none"> <li>♦ You must either select this or perform a manual ldap synchronization before any users are added to the group you are defining.</li> <li>♦ If you do not select this option, the group will not be automatically updated when changes occur in your LDAP directory.</li> </ul>
♦ <b>Test ldap query</b> button	<ul style="list-style-type: none"> <li>♦ Use this to see whether the configuration you have specified is working.</li> </ul>
<b>OK</b> or <b>Cancel</b>	<ul style="list-style-type: none"> <li>♦ Click <b>OK</b> to save the changes you’ve made in this dialog or <b>Cancel</b> to discard your changes.</li> </ul>
<b>Dynamic Group Membership window</b>	
<b>Users tab</b>	<ul style="list-style-type: none"> <li>♦ This displays a list of the users and groups that are members of the dynamic group.</li> </ul>
♦ <b>Close</b> button	<ul style="list-style-type: none"> <li>♦ Use this to return to the previous window.</li> </ul>