

TeamWorks 18.1

Administrative User Interface Reference

January 2019

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 Micro Focus Inc. All Rights Reserved.

Contents

About This Guide	5
1 Administrative Consoles	7
2 Administrative Access	9
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
3 Access to TeamWorks	13
Reverse Proxy Configuration Settings	13
4 LDAP Servers and Synchronization	15
5 Licensing	25
Installing/Updating the TeamWorks License	25
Viewing TeamWorks License Details	25
6 Logging and Monitoring	27
Accessing TeamWorks System Log Files	27
Changing the Ganglia Monitoring Configuration	27
Logging All HTTPS Traffic	28
7 Email Integration (Notifications)	31
Configuring an Email Service for TeamWorks Notifications	31
Email Notification Template Customization	33
Email Notification Language Is User-specific	34
8 Memory and Performance Tuning	35
Managing Memcached (Search Appliance Only)	35
Changing Configuration Settings for Requests and Connections	35
Changing the Memory Configuration Settings	36
9 Network Infrastructure	39
Changing Network Settings	39
Port Numbers	40

10 Product Improvement	43
11 Search and Indexing	45
Search Index	45
12 Security	47
Certificates	47
Firewall Configuration	47
Password Security (Local and External Users)	48
13 SQL Database Connection	49
14 Storage Management	51
Managing the File Upload Size Limit	51
Expanding Storage	52
15 Changing System Services Configurations	53
Managing System Services	53
Managing Search Appliance Services	54
Shutting Down and Restarting the Micro Focus Appliance	54
16 Time and Locale	57
Changing the Appliance's NTP Configuration	57
Setting a Default Time and Locale for Non-LDAP and External Users	57
17 Updates, Patches, and Support Files	59
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
18 Users and Groups	63
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, “Email Integration (Notifications),” on page 31
- ♦ Chapter 8, “Memory and Performance Tuning,” on page 35
- ♦ Chapter 9, “Network Infrastructure,” on page 39
- ♦ Chapter 10, “Product Improvement,” on page 43
- ♦ Chapter 11, “Search and Indexing,” on page 45
- ♦ Chapter 12, “Security,” on page 47
- ♦ Chapter 13, “SQL Database Connection,” on page 49
- ♦ Chapter 14, “Storage Management,” on page 51
- ♦ Chapter 15, “Changing System Services Configurations,” on page 53
- ♦ Chapter 16, “Time and Locale,” on page 57
- ♦ Chapter 17, “Updates, Patches, and Support Files,” on page 59
- ♦ Chapter 18, “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

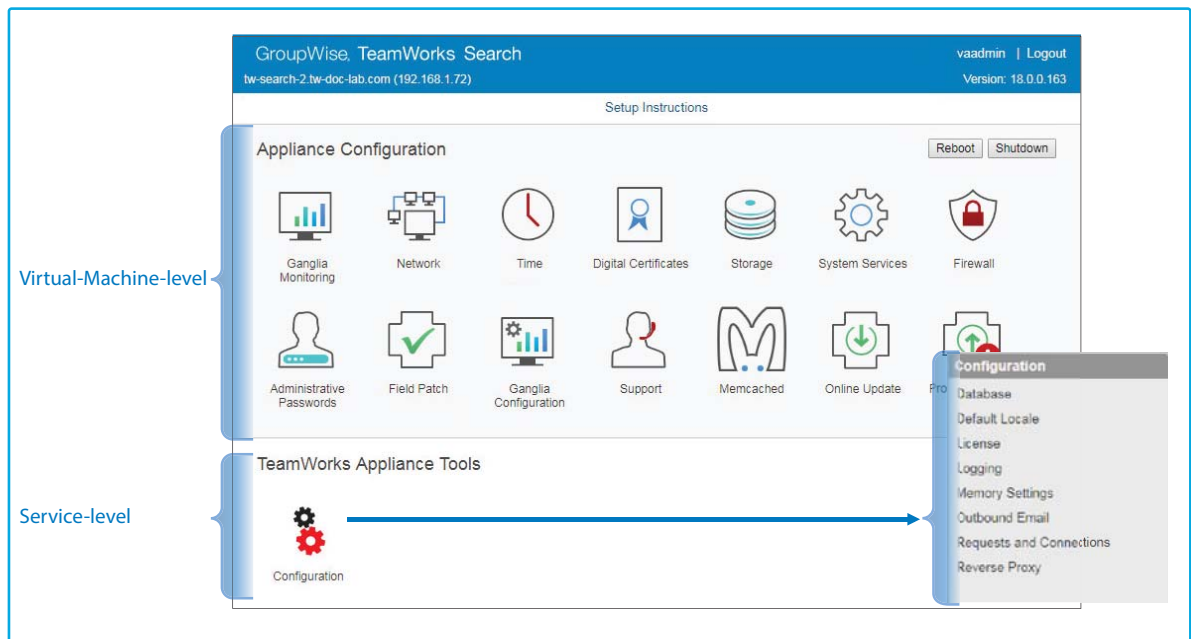
Administrative Consoles

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 TeamWorks Console

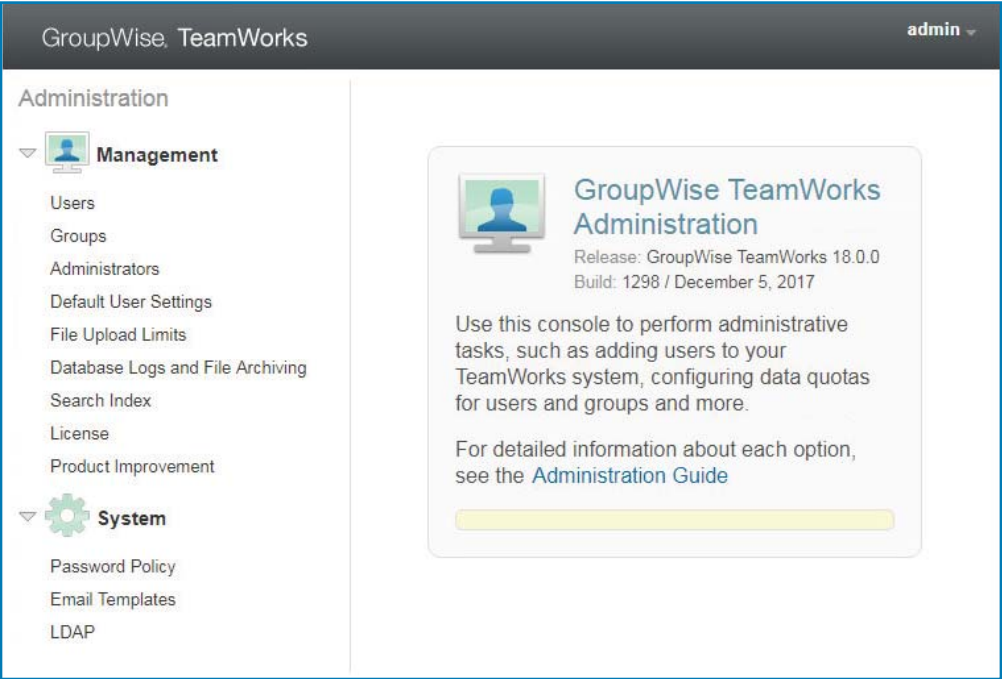


Port 8443 TeamWorks Administration Console

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
About Port 8443 Direct Administrators	Port 8443 Designated Administrators can only administer the following: <ul style="list-style-type: none">♦ Users♦ Groups
 Administrators	
♦ Add	<ol style="list-style-type: none">1. Click Add to add a new Designated Administrator.2. Begin typing the user or group name you want to assign.3. Click a user or group to add it to the list.
♦ Remove	<ol style="list-style-type: none">1. Select one or more users or groups in the Administrators list.2. Click Remove. <p>The selected items are removed.</p>
♦ Filter list	<ol style="list-style-type: none">1. Type an alphanumeric string contained in the user or group names you want to display.2. Press Enter. <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"> 1. Click the icon 2. Select Edit Column Sizes. 3. Follow the instructions in the Edit Column Sizes dialog to adjust column widths. <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"> ◆ Acting as either <code>vaadmin</code> or <code>root</code>, type the current password, type and confirm the new password, and click OK. <p>NOTE: For Port 8443 console administrators, change this using the Change Password option in the admin user's drop-down list (upper-right corner).</p>
root SSH Access	<ul style="list-style-type: none"> ◆ Acting as <code>root</code>, select or deselect Allow root access to SSH and click OK. <p>SSH is enabled by default. For information about how to start SSH on the appliance, see Chapter , "Managing System Services," on page 53.</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
♦ User ID:	♦	Admin
♦ Password:	♦	First-time login: Enter <code>admin</code> (case-insensitive) You are then prompted to change the password. ♦ Subsequent login: Administrative user password set above or changed in the Profile.
♦ Change Password	♦	First-time login <ol style="list-style-type: none">1. Type <code>admin</code> (case-insensitive).2. Type and confirm a new, more secure password. ♦ Subsequent to the first-time login <ol style="list-style-type: none">1. Select the Change Password option in the admin user's drop-down list (upper-right corner).2. Type the current password, then type and confirm a new, more secure password.

Port 9443 Console

Path: [Port 9443 Appliance Console](#)

Table 2-4 *Port 9443 Sign In dialog*

Field, Option, or Button		Information and/or Action
♦ Username	♦	Enter either <code>vaadmin</code> or <code>root</code> .
♦ Password	♦	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
Host Information	<ul style="list-style-type: none">♦ Specify the information for the server or switch through which internal and external users access TeamWorks. <p>IMPORTANT: Two critical points:</p> <ul style="list-style-type: none">♦ Configure each TeamWorks appliance that services user requests in a given deployment, with the same information.♦ Do not configure synchronization and indexing on dedicated TeamWorks appliances with Reverse Proxy Configuration Settings.
♦ Host:	<ul style="list-style-type: none">♦ For a reverse proxy server or a load balancer/L4 switch, specify the DNS hostname.♦ For NetIQ Access Manager, enter the published DNS name.
♦ Reverse Proxy Secure HTTP Port:	<ul style="list-style-type: none">♦ If you have enabled Port Redirection and secure HTTP Port access in the Network dialog, specify port 443.
♦ Logout URL:	<ul style="list-style-type: none">♦ The URL of the published DNS name of the reverse proxy that you have specified for the ESP, plus /AGLogout . <p>You can find the domain used for the ESP by editing the LAG/MAG cluster configuration and then clicking Reverse Proxy / Authentication.</p> <p>For example, if the published DNS name of the proxy service that you have specified for the ESP is <code>esp.yoursite.com</code>, specify the following URL:</p> <p><code>https://esp.yoursite.com/AGLogout</code></p> <ul style="list-style-type: none">♦ After clicking OK, you must click Reconfigure TeamWorks Server for your changes to take effect. <p>This stops and restarts your TeamWorks server. Because this results in server downtime, you should restart the server during off-peak hours.</p>

Field, Option, or Button	Information and/or Action
OK button	<ul style="list-style-type: none"> Click this to save your changes, then click Reconfigure TeamWorks Server. <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>
Cancel button	<ul style="list-style-type: none"> Click this to cancel the changes you have made.

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		
♦ Add button	♦	Click this to begin the process of adding an LDAP server. The LDAP Server Configuration dialog opens.
♦ Delete button	♦	Click this to remove the selected LDAP server from the list. IMPORTANT: 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 User Settings tab and the Group Settings tab .

Field, Option, or Button Information and/or Action	
♦ Sync All button	<p>TIP: If you have just added or modified the LDAP Servers configuration, you must save it by clicking OK before running an LDAP synchronization.</p> <ul style="list-style-type: none"> ♦ After your users and groups are synchronized, you can click this to refresh the LDAP information in TeamWorks. ♦ To synchronize only certain users or groups, filter the list by entering a string in the Filter List. <p>Or</p> <ul style="list-style-type: none"> ♦ Click the drop-down arrow next to the Filter List and select the type of users or groups to synchronize. <p>For example, Added users, Modified users, Modified groups, and so forth.</p> <ul style="list-style-type: none"> ♦ Users and groups that have been modified by running the LDAP sync are reported, along with information about how they have been modified.
♦ Preview Sync button	<p>TIP: If you have just added or modified the LDAP Servers configuration, you must save it by clicking OK before previewing an LDAP synchronization.</p> <ul style="list-style-type: none"> ♦ 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"> ♦ To preview only certain users or groups, filter the list by entering a string in the Filter List. <p>Or</p> <ul style="list-style-type: none"> ♦ Click the drop-down arrow next to the Filter List and select the type of users or groups to synchronize. <p>For example, Added users, Modified users, Modified groups, and so forth.</p> <ul style="list-style-type: none"> ♦ After you are satisfied with the results, use the Sync All option with the same filters to perform the actual synchronization.
♦ Show Sync Results button	<ul style="list-style-type: none"> ♦ Use this to display the most recent synchronization results <i>for the current browser session</i>. <p>NOTE: If you run a synchronization, log out of TeamWorks, and then log in again, no previous synchronization results are available to view.</p>
LDAP servers list	
♦ Server URL	<ul style="list-style-type: none"> ♦ The URL that you specified when creating the LDAP server. ♦ You can click this to access the LDAP Server Configuration dialog.
♦ User DN	<ul style="list-style-type: none"> ♦ This is the LDAP proxy user information for the LDAP server
User Settings tab	
♦ Register User Profiles Automatically	<ul style="list-style-type: none"> ♦ Select this option to automatically add LDAP users to the TeamWorks site.
♦ Synchronize User Profiles	<ul style="list-style-type: none"> ♦ Select this option to automatically update TeamWorks with user information changes following the initial LDAP synchronization. ♦ The attributes that are synchronized are the attributes listed in the “mappings” box in the Server Information tab.
<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">◆ Disable Account | <ul style="list-style-type: none">◆ This is the default because deleting user accounts cannot be undone.

For more information about disabled users in TeamWorks, see Disabling TeamWorks User Accounts in the TeamWorks 18.1: Maintenance Best Practices Guide. |
|--|--|

- | | |
|---|---|
| <ul style="list-style-type: none">◆ Delete Account | <p>IMPORTANT: A deleted user cannot be undeleted; this action is not reversible.</p> <ul style="list-style-type: none">◆ 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. |
|---|---|

Use the following when creating new users sub-section

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

Group Settings tab

- | | |
|--|---|
| <ul style="list-style-type: none">◆ Register LDAP group profiles automatically | <ul style="list-style-type: none">◆ Select this to automatically add new LDAP groups to the TeamWorks site.

NOTE: 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.

We recommend that you synchronize groups despite the initial limitation. |
| <ul style="list-style-type: none">◆ Synchronize group profiles | <ul style="list-style-type: none">◆ Select this to synchronize group information, such as the group description, to the TeamWorks site whenever this information changes in LDAP. |
| <ul style="list-style-type: none">◆ Synchronize group membership | <ul style="list-style-type: none">◆ This option ensures that the TeamWorks group includes the same users (and possibly groups) as the corresponding LDAP group.

If this is not selected, then LDAP group changes are not reflected in TeamWorks. |
| <ul style="list-style-type: none">◆ Delete groups that were provisioned from LDAP but are no longer in LDAP | <p>IMPORTANT: A deleted group cannot be undeleted; this action is not reversible.</p> <ul style="list-style-type: none">◆ 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. |

**Synchronization Schedule tab**

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

Field, Option, or Button	Information and/or Action
♦ At HH:MM	<ul style="list-style-type: none"> ♦ Using the drop-down lists, you can specify synchronizations to occur at a specific time. ♦ Hours start at midnight (0) and continue through 11 p.m. (23). ♦ Minutes can be specified using 5-minute increments.
Repeat every X hours	<ul style="list-style-type: none"> ♦ 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). ♦ The smallest time interval you can set is .25 hours (every 15 minutes).
Local User Accounts tab	
♦ Allow log in for local user accounts (i.e user accounts not in LDAP)	♦ 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
LDAP Server Configuration dialog	
	Server Information tab

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ♦ LDAP Server URL 	<p>WARNING: 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"> ♦ This is the host name of the LDAP server where your directory service is running. <p>Specify a URL with the format your server requires, as follows:</p> <ul style="list-style-type: none"> ♦ Non-SSL: <code>ldap://hostname</code> Assumes Port 389 is used ♦ SSL: <code>ldaps://hostname</code> Assumes Port 636 is used <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 TeamWorks 18.1: Maintenance Best Practices Guide.</p> <ul style="list-style-type: none"> ♦ 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"> ♦ <code>ldap://hostname:port_number</code> ♦ <code>ldaps://hostname:port_number</code>
<ul style="list-style-type: none"> ♦ User DN: (LDAP proxy user) 	<p>IMPORTANT: If you are using GroupWise 18 as an LDAP directory source, make sure you have followed the instructions in "Configuring GroupWise LDAP Provisioning (https://www.novell.com/documentation/groupwise18/gwmob18_guide_admin/data/admin_con_config.html#b1inkuao)" in the GroupWise Mobility Service 18 Administration Guide (https://www.novell.com/documentation/groupwise18/gwmob18_guide_admin/).</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"> ♦ This is the LDAP proxy user and it must have sufficient rights to access the user information stored there. ♦ 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"> ♦ GroupWise: <code>cn=gw-admin-app-name,o=gw-system-name</code> ♦ eDirectory: <code>cn=username,ou=organizational_unit,o=organization</code> ♦ Active Directory: <code>cn=username,ou=organizational_unit,dc=domain_component</code>
<ul style="list-style-type: none"> ♦ Password: (LDAP proxy user password) 	<ul style="list-style-type: none"> ♦ You must type the password for the User DN.
<ul style="list-style-type: none"> ♦ Directory Type: 	<ul style="list-style-type: none"> ♦ Select the directory type for the LDAP server that you are configuring (GroupWise, eDirectory or Active Directory)

Field, Option, or Button	Information and/or Action
♦ Guid attribute:	<ul style="list-style-type: none"> ♦ Based on the directory type you have selected, TeamWorks selects the standard LDAP attribute used to identify a user. ♦ entryUUID, GUID, and objectGUID: 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. ♦ Other: 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 OK. <ul style="list-style-type: none"> ♦ 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. ♦ 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.



Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none"> ♦ TeamWorks account name attribute: 	<ul style="list-style-type: none"> ♦ TeamWorks uses this attribute <ul style="list-style-type: none"> ♦ To create TeamWorks account names ♦ To locate users in the LDAP directory. ♦ As the User ID for authentication purposes. ♦ The value of this attribute must be unique in LDAP. ♦ Attribute options depend on the directory type selected in the Directory type drop-down list. <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"> ♦ For GroupWise and eDirectory, the default available options are cn and Other. ♦ For Active Directory, the default available options are sAMAccountName, cn, and Other. ♦ If you select Other as the value for this attribute, you are prompted to enter the name of an LDAP attribute to use instead of the default choices. ♦ 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 LDAP Attribute Used for TeamWorks Name. <p>For example, if you use Active Directory, you might need to set up one LDAP source and use cn and another to sAMAccountName as the TeamWorks account name attribute.</p> <ul style="list-style-type: none"> ♦ In addition to the attributes already mentioned in this section, other LDAP attributes can be used for the TeamWorks account name attribute, as long as the attribute is unique for each User object. <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"> ♦ LDAP Attribute "Mappings" box 	<ul style="list-style-type: none"> ♦ This lists the mappings between TeamWorks user information and the LDAP attributes that correspond to them. <p>It is populated automatically.</p> <ul style="list-style-type: none"> ♦ If Synchronize User Profiles is enabled in the User Settings tab, the information associated with the mappings that are configured here, is updated each time the user account is synchronized.
OK button	<ul style="list-style-type: none"> ♦ If you are modifying previously configured LDAP server information, you can click OK. Otherwise, you must click the Users tab
Cancel button	<ul style="list-style-type: none"> ♦ Click this to discard any LDAP server configuration changes that you have made and exit the tab.
Users tab	
<ul style="list-style-type: none"> ♦ Add button 	<ul style="list-style-type: none"> ♦ Click this to open the "LDAP Search Dialog (User Version)" on page 22 wherein you can specify a context where TeamWorks searches for LDAP users.
<ul style="list-style-type: none"> ♦ Delete button 	<ul style="list-style-type: none"> ♦ 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.

Field, Option, or Button	Information and/or Action
OK button	<ul style="list-style-type: none"> ♦ If you are modifying previously configured User information, you can click OK. ♦ If this is a new configuration, you should click the Groups tab and add an LDAP search context. Otherwise, expected groupings of users will not be available in TeamWorks.
Cancel button	<ul style="list-style-type: none"> ♦ Click this to discard your changes and exit.
Groups tab	
♦ Add button	<ul style="list-style-type: none"> ♦ Click this to open the LDAP Search Dialog (Group Version) wherein you can specify a context where TeamWorks searches for LDAP groups.
♦ Delete button	<ul style="list-style-type: none"> ♦ 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.
OK button	<ul style="list-style-type: none"> ♦ Click OK to save the LDAP server configuration.
Cancel button	<ul style="list-style-type: none"> ♦ Click this to discard your changes and exit.

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
 LDAP Search dialog (User Version)	
♦ Base DN:	<p>Best Practice: Use the Browse icon  next to the Base DN 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"> ♦ This is the directory context or container under which LDAP User objects are located. ♦ When specifying this you must use the syntax required by your directory service type. <ul style="list-style-type: none"> ♦ GroupWise: <code>ou=gw-domain-name,o=gw-system-name</code> ♦ eDirectory: <code>ou=organizational_unit,o=organization</code> ♦ Active Directory: <code>ou=organizational_unit,dc=domain_component</code> <p>IMPORTANT: Container names cannot exceed 128 characters. If they do, users are not provisioned.</p>

Field, Option, or Button	Information and/or Action
♦ Filter:	<p>♦ IMPORTANT: 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>♦ About User Filters:</p> <ul style="list-style-type: none"> ♦ By default, TeamWorks identifies potential users by filtering on the following LDAP directory object attributes: <ul style="list-style-type: none"> ♦ Person ♦ orgPerson ♦ inetOrgPerson <p>If needed, you can modify the filter by inserting the following operators:</p> <ul style="list-style-type: none"> ♦ OR (the default) ♦ & AND ♦ ! NOT <p>♦ A Group for TeamWorks Users:</p> <ul style="list-style-type: none"> ♦ You might want to create a group for only TeamWorks users, regardless of where they are located in your LDAP directory. ♦ After creating the group, use the following filters to search for User objects that have the group membership attribute shown below. <p>Make sure you include the parentheses in your filter.</p> <ul style="list-style-type: none"> ♦ GroupWise: <code>(groupMembership=cn=group_name,ou=gw-domain-name,o=gw-system-name)</code> ♦ eDirectory: <code>(groupMembership=cn=group_name,ou=organizational_unit,o=organization)</code> ♦ Active Directory: <code>(memberOf=cn=group_name,ou=organizational_unit,dc=domain_component)</code> <p>IMPORTANT: 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><attribute name>:<matching rule OID>:=<value></code></p>
♦ Search subtree	<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
 LDAP Search dialog (Group Version)	
<ul style="list-style-type: none"> ♦ Base DN: 	<p>Best Practice: Use the Browse icon  next to the Base DN 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"> ♦ This is the directory context or container under which LDAP Group objects are located. ♦ When specifying this you must use the syntax required by your directory service type. <ul style="list-style-type: none"> ♦ GroupWise: <code>ou=gw-domain-name,o=gw-system-name</code> ♦ eDirectory: <code>ou=organizational_unit,o=organization</code> ♦ Active Directory: <code>ou=organizational_unit,dc=domain_component</code> <p>IMPORTANT: Container names cannot exceed 128 characters. If they do, groups are not provisioned.</p>
<ul style="list-style-type: none"> ♦ Filter: 	<ul style="list-style-type: none"> ♦ IMPORTANT: TeamWorks sets up a standard group filter for the LDAP server type. <p>In almost all cases, this doesn't require modification.</p>
<ul style="list-style-type: none"> ♦ Search subtree 	<ul style="list-style-type: none"> ♦ Select this if you want TeamWorks to search for groups in containers underneath the base DN (that is, in subtrees).

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
♦ Choose File button	<ol style="list-style-type: none">1. Download your <code>license-key.xml</code> file (from the Novell Customer Center (NCC)) to your management workstation.2. Click Choose File.3. Browse to and select the downloaded license file.4. Click Open.5. Click Reconfigure TeamWorks Server in the Configuration column.

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
♦ Current License	<p>This section displays information about the installed license, including:</p> <ul style="list-style-type: none">♦ Information about the license key, when it was issued, and who issued it.♦ Product and version information.♦ The effective date range.♦ Information about user allowances. <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">♦ The options or features that the license enables for use.

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

♦ Reload License File	
------------------------------	--

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

6 Logging and Monitoring

- ♦ “Accessing TeamWorks System Log Files” on page 27
- ♦ “Changing the Ganglia Monitoring Configuration” on page 27
- ♦ “Logging All HTTPS Traffic” on page 28

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

Changing the Ganglia Monitoring Configuration

Ganglia is a scalable, distributed monitoring system that lets you gather important information about your TeamWorks system.

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

Table 6-2 Using the Ganglia Monitoring Configuration dialog

Field, Option, or Button	Information and/or Action
Monitoring Services	

Field, Option, or Button	Information and/or Action
Enable Full Monitoring Services	<ul style="list-style-type: none"> Deselect this if: <ul style="list-style-type: none"> You already have a monitoring system that you plan to use for TeamWorks. You plan to configure a dedicated appliance for viewing monitoring information. You do this by selecting Unicast below and then specifying the DNS name or IP address of the appliance where monitoring information will be collected. (Default) Select this to have this appliance receive and store metrics from other appliances, and to allow the Ganglia Web Interface to run on the same machine as the TeamWorks appliance.
Monitoring Options	
Enable Monitoring on this appliance	<ul style="list-style-type: none"> (Default) Select this option to enable Ganglia monitoring on this appliance.
♦ Multicast	<ul style="list-style-type: none"> (Default) Send performance data to the other appliances on the network (default setting).
♦ Unicast	<ul style="list-style-type: none"> Send monitoring information to a single destination. This is a best practice recommendation for performance.
♦ Publish to:	<ul style="list-style-type: none"> The URL where you want Ganglia to send monitoring information when it is running in Unicast mode.
Monitoring Tool Options	
♦ Enable direct http port 9080 access	<ul style="list-style-type: none"> Select this to allow Ganglia to communicate using HTTP port 9080.
Panel Buttons	
♦ OK	<ul style="list-style-type: none"> Enable configuration changes.
♦ Reset Database button	<ul style="list-style-type: none"> Click this to remove all existing Ganglia metrics from this appliance. This option is not related to the TeamWorks database.
♦ Cancel	<ul style="list-style-type: none"> Cancel configuration changes and close dialog.

See Also

- “Monitoring with Ganglia” in the *TeamWorks 18.1: Maintenance Best Practices Guide*.
- The Ganglia Monitoring System web site (<http://ganglia.info/>).

Logging All HTTPS Traffic

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

Table 6-3 *Using the Logging dialog*

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

7 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 7-1 Outbound Email dialog

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



**Outbound
Email dialog**

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

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 18.1 Planning Your TeamWorks Deployment—Best Practices](#).

Field, Option, or Button	Notes
♦ Protocol:	<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 “Email Communications Security” in the <i>TeamWorks 18.1: Maintenance Best Practices Guide</i>.</p>
♦ Host:	<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>
♦ Port:	<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>
♦ Time zone:	<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>
♦ User Name:	<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 From field.</p>
♦ Password:	<p>♦ If the email server requires passwords, specify the password for the user name.</p>
♦ Authentication Required	<p>♦ If the email server TeamWorks is leveraging requires authentication, select this option.</p> <p>GroupWise 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>Exchange If you set up the outbound email server to require authentication (by selecting the option Authentication Required), 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
♦ Allow sending e-mail to all users	<ul style="list-style-type: none"> ♦ If you select this option, users can send email to the All Users group. This is disabled by default because of the potential for users to send large numbers of emails.
♦ Force HTTPS links	<ul style="list-style-type: none"> ♦ Select this if all links in TeamWorks-generated email messages should be HTTPS instead of HTTP. Otherwise, TeamWorks uses its connection (HTTP or HTTPS) with the emailing user as the link protocol.
♦ Enable STARTTLS	<ul style="list-style-type: none"> ♦ Select this option if the email service that TeamWorks is leveraging requires TLS over SMTP for secure email.
♦ From e-mail address override:	<ul style="list-style-type: none"> ♦ If you don't want the User Name email address used in the From field in TeamWorks messages, specify a different address here.
♦ Connection Timeout:	<ul style="list-style-type: none"> ♦ Specify the amount of time for TeamWorks to wait before timing out on a connection request to the email host.
♦ Test Connection	<ul style="list-style-type: none"> ♦ Click this to test your Outbound E-Mail configuration.

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 18.1: Maintenance Best Practices Guide* and “[Email Template Customization—A Video Walkthrough](#)” in *TeamWorks 18.1: Maintenance Best Practices Guide*.

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

Table 7-2 Using the Manage Email Templates dialog

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

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 7-3 Using the Default Locale dialog

Field, Option, or Button	Information and/or Action
<ul style="list-style-type: none">◆ Default Locale:	<ul style="list-style-type: none">◆ 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. <p>The following points explain more about the Default Locale setting.</p> <ul style="list-style-type: none">◆ Micro Focus appliance installations run in English only.◆ 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.◆ You can modify the Default Locale settings for new LDAP users in the LDAP Configuration dialog, User Settings tab. <p>The default language for internal (non-LDAP) users is set in the Default User Settings dialog. You can change this when creating individual users.</p>

8 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 8-1 Memcached configuration

Field, Option, or Button	Information and/or Action
♦ Listen Interface:	♦ The URL that Memcached listens on.
♦ Number of Threads:	♦ The number of threads to use when processing incoming requests.
♦ Max Memory:	♦ Max memory that can be used by Memcached.
♦ Max Simultaneous Connections:	♦ 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 8-2 Using the Requests and Connections dialog

Field, Option, or Button	Information and/or Action
Requests and Connections	<ul style="list-style-type: none"> ♦ Max Threads: The maximum number of simultaneous client request threads that TeamWorks will support. Default: 250 ♦ Max Active: The maximum number of database connections that can be allocated simultaneously from this pool. Default: 300 ♦ Max Idle: The maximum number of database connections that can be simultaneously idle in this pool. Default: 300 ♦ Scheduler Threads: The size of the thread pool used for background execution of scheduled tasks. Default: 20 ♦ Max REST Requests (upload/download): 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. ♦ Session Timeout: 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.
OK button	<ul style="list-style-type: none"> ♦ After clicking this, you must click Reconfigure TeamWorks Server for the changes to take effect.
<p>TIP: 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 8-3 Using the Memory Settings dialog

Field, Option, or Button	Information and/or Action
JVM Settings	<p>Best practice recommendation: Set both sizes to 66% of total RAM (see “Appliance Memory and CPU” in the GroupWise TeamWorks 18.1: Installation and Deployment Guide).</p> <p>IMPORTANT: 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"> ♦ JVM Heap Size: The upper limit that the system will allocate to the TeamWorks appliance’s JVM processes. ♦ Total System Memory: The total RAM allocated to this appliance. ♦ Allow generation of a system dump on a user signal: 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. ♦ Java Home: This location is shown for information only and cannot be changed.
Search Service Settings (All-in-One appliance)	<ul style="list-style-type: none"> ♦ JVM Heap Size: The upper limit that the system will allocate to the Search service’s JVM processes on an all-in-one TeamWorks appliance.
Search Service Settings (Search appliance)	<ul style="list-style-type: none"> ♦ JVM Heap Size (MB): The upper limit that the system will allocate to the Search service’s JVM processes on a TeamWorks Searchappliance.
Database Service Settings (All-in-One appliance)	<ul style="list-style-type: none"> ♦ Shared Buffers: ♦ Effective Cache Size:
Messaging Service Settings	<ul style="list-style-type: none"> ♦ Memory High Water Mark: Increase or decrease as needed.
Memory Cache Service Settings	<ul style="list-style-type: none"> ♦ Memory Cache Max Heap: Increase or decrease as needed.
OK button	<ul style="list-style-type: none"> ♦ After clicking this, you must click Reconfigure TeamWorks Server for the changes to take effect.

9 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 9-1 Using the Network (DNS, NIC, Port 9443 Access restrictions) dialog

Field, Option, or Button		Information and/or Action
 Network (IP Infrastructure) dialog		Worksheet 20 - Network Support (IP Address Infrastructure Information and Appliance-Specific IP Configuration Settings)
DNS Configuration section		
♦ Name Servers:	♦ You can modify the name servers.	
♦ Search Domains:	♦ 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> .	
♦ Gateway:	♦ Make sure that this matches any of the other changes you have made in this dialog.	
NIC Configuration 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 NIC Configuration 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 OK .

Field, Option, or Button	Information and/or Action
Appliance Administration UI (Port 9443) Access Restrictions section	
<ul style="list-style-type: none"> ♦ Allowed Networks: 	<ul style="list-style-type: none"> ♦ To limit administrative access, specify the IP address of any networks from which you want administrators to access the TeamWorks site. ♦ Leave this section blank to allow administrative access from any network.
OK button	<ul style="list-style-type: none"> ♦ Click this to save your changes, then click Reconfigure TeamWorks Server. <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>User sessions can be affected by the above changes.</p>
Cancel button	<ul style="list-style-type: none"> ♦ Click this to cancel the changes you have made.

Port Numbers

Table 9-2 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 9-2 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 Apache Tomcat Web site (http://tomcat.apache.org) .
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 Tomcat - Shutdown Port (http://www.wellho.net/mouth/837_Tomcat-Shutdown-port.html) .
8009	Default AJP port
	For an explanation of the Apache JServ Protocol port, see The AJP Connector (http://tomcat.apache.org/tomcat-6.0-doc/config/ajp.html) .
22	SSH port for the appliance
111	rpcbind utility
1099	Java RMI port

Port Numbers	Description
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

10 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 18.1: 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 10-1 Using the Product Improvement dialog

Field, Option, or Button	Information and/or Action
♦ Collect and send the product name and version, and the number of LDAP users.	♦ This option causes the TeamWorks system to send Micro Focus information about the product version and build, license type, and number of users.
♦ Also collect and send information about the deployment size and configuration, and so on.	♦ 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">♦ The user information doesn't include the LDAP user count because that is already available under the Tier1.♦ The user count numbers do not include system user accounts, such as <code>admin</code>, and so on.♦ The group count numbers do not include system groups, such as <code>www</code>, <code>admingroup</code>, and so on.
♦ View the information collected.	♦ 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.

11 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 11-1 Using the Search Appliance dialog

Field, Option, or Button		Information and/or Action
Manage Search Index		
♦ Use the Following Language for Stemming	♦	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
♦ Perform Full Reindex Now	<p>IMPORTANT: 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"> ♦ Selecting Perform Full Reindex Now and clicking OK 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"> ♦ 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>WARNING: 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> ♦ 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>
OK button	♦ Click this to save your changes and launch the reindexing process if so specified.
Cancel button	♦ Click this to cancel the changes you have made.

12 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 18.1: Maintenance Best Practices Guide](#)

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

Table 12-1 Using the Digital Certificates Page

Field, Option, or Button		Information and/or Action
Certificates in the Selected Key Store		
♦ Key Store drop-down	♦	Use this drop-down list to filter whether JVM or Web Application Certificates are listed.
♦ File 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.
♦ Edit drop-down	♦	This exposes the option to delete a certificate you have selected.
♦ View Info	♦	This lets you view the information for a selected certificate
♦ Reload	♦	This lets you reload a selected certificate.

Firewall Configuration

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

Table 12-2 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 12-3 Using the Configure Password Policy dialog

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

13 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 13-1 *Using the Database Connection dialog*

Field, Option, or Button	Information and/or Action
Database Connection dialog	Worksheet 23 - SQL Database Connection
♦ Database Type:	♦ Select the appropriate option for the database server. <ul style="list-style-type: none">♦ PostgreSQL: Select PostgreSQL♦ Microsoft SQL Server: Select MS SQL Server
♦ Host Name or IP Address:	♦ The DNS host name or IP address of your SQL server.
♦ Port:	♦ The port used for communications with TeamWorks. The standard port for the database type is automatically selected.
♦ Database Name:	♦ The name of the database used by this TeamWorks deployment.
♦ User Name:	♦ The user id that TeamWorks uses to log in to the database server.
♦ User Password:	♦ The password for the User Name.
♦ Encrypt Database Communication:	♦ Select this option to encrypt data communication from the TeamWorks server to the database server. For more information, see “ Database Communication Encryption ” in the TeamWorks 18.1: Maintenance Best Practices Guide .
OK button	♦ Click this to save your changes. Then click Reconfigure TeamWorks Server so that the changes are used by TeamWorks.
Cancel button	♦ Click this to cancel the changes you have made.

14 Storage Management

- ♦ “Managing the File Upload Size Limit” on page 51
- ♦ “Expanding Storage” 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 14-1 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">♦ Unlike data quotas, there is no option to enable or disable file upload size checks.♦ 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.♦ You can also add different upload limits for individual users and groups as explained below.
♦ Add a Group button	<p>IMPORTANT: 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">1. Click this to add a group of users.2. In the Group 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.3. In the File Size Limit field, specify the size limit for the group.4. Click OK, then click Apply > Close to save the group file size limit.

Field, Option, or Button	Information and/or Action
♦ Add a User button	<p>IMPORTANT: 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"> 1. Click this to add an individual user upload limit. 2. In the User 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. 3. In the File Size Limit field, specify the file size limit for the user. 4. Click OK, then click Apply > Close to save the user file size limit.

Expanding Storage

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

Table 14-2 Using the Storage Expansion dialog

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

15 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 15-1 Using the System Services dialog

Field, Option, or Button		Information and/or Action
Available System Services: This varies by appliance type as listed below this table.		
♦ Action drop-down	♦	Use this to start , stop , or restart the selected service. Before doing any of these, make sure you understand how your action will affect the appliance.
♦ Options drop-down	♦	Use this to set the selected service to start automatically or require a manual start.
♦ Refresh List	♦	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 15-2 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">♦ Displays the status of the Messaging service on this appliance (Enabled or Disabled). <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">♦ Green: Indicates that the Search system is healthy.♦ Yellow: 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. <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">♦ Red: Indicates that the Search system was unable to restore itself to a healthy state. <p>Resolving this requires that you contact Micro Focus Support.</p> <ul style="list-style-type: none">♦ Checking: Indicates that the Search system is assessing its health status.
♦ Decommission Appliance	<ul style="list-style-type: none">♦ Use this option when you are permanently removing a Search appliance from your TeamWorks deployment. <p>The option only works when Search Cluster Health is green.</p> <p>For more information, see “Permanently Removing (Decommissioning) a Search Appliance” in the <i>TeamWorks 18.1: Maintenance Best Practices Guide</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.

16 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 16-1 Using the Time dialog

Field, Option, or Button	Information and/or Action
♦ NTP Servers:	♦ Type a new default NTP server.
♦ Region:	♦ Click the drop-down list and select a region for the appliance.
♦ Time Zone:	♦ Click the drop-down list and select a time zone for the appliance.
♦ Hardware clock set to UTC	♦ 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 16-2 *Using the Default User Settings dialog*

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

17 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 17-1 Using the Field Patch dialog

Field, Option, or Button		Information and/or Action
Field Test Patch		
<i>Install a Downloaded Patch</i> sub-section		
♦ Path to Field Patch:	♦	Use the Browse button to navigate to a downloaded patch, then click Install to apply the patch.
<i>Manage Installed Patches</i> sub-section		
♦ Uninstall Latest Patch 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.
♦ Download Log File 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 17-2 Using the Online Update dialog

Field, Option, or Button	Information and/or Action
Online Update (Automatic Update Schedule: X)	<ul style="list-style-type: none"> ◆ This is the dialog title and it also shows which Schedule option is selected (represented by X).
Register Online Update Service dialog	<ul style="list-style-type: none"> ◆ 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. ◆ You must register the appliance for it to receive online updates.
◆ Service Type:	<ul style="list-style-type: none"> ◆ 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
◆ Local SMT	<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"> ◆ Hostname: The hostname of the server from where you want the appliance to download software updates. ◆ SSL cert URL (optional): The path to the SSL certificate for encrypting communications with the server. ◆ Namespace path (optional): 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.
◆ Micro Focus Customer Center	<ul style="list-style-type: none"> ◆ Email: Your email address for registering the appliance to receive updates. ◆ Activation Key: This is found in your NCC Portal in the same dialog as your product license. ◆ Allow Data send: Select from the following options if you want to share information with the Micro Focus Customer Center: <ul style="list-style-type: none"> ◆ Hardware Profile: Shares the hardware information. ◆ Optional Information: Shares information such as host type, productversion, release, architecture, timezone, and processor.
Update service: X	<ul style="list-style-type: none"> ◆ After you register the appliance for an update service, the service name appears in this field (represented by X).
◆ Patches drop-down	<ul style="list-style-type: none"> ◆ Needed Patches: Selecting this option lists that patches that will be installed during the next manual or automatic update. ◆ Installed Patches: Selecting this option lists all patches that have been previously installed.
◆ Schedule drop-down	<ul style="list-style-type: none"> ◆ Click this to set a schedule for when the appliance will download updates. ◆ If you select Manual, the appliance immediately downloads all available patches. ◆ If you select Daily, Weekly, or Monthly, you must then choose to apply either All Needed Patches or Security Patches Only. ◆ Optionally, you can specify whether to Automatically agree with all license agreements and Automatically install all interactive patches.

Field, Option, or Button	Information and/or Action
Update Now tab	<ul style="list-style-type: none"> ◆ This is selectable only when the Patches drop-down is set to Needed Patches. ◆ After clicking the option, you must choose to apply either All Needed Patches or Security Patches Only. ◆ Optionally, you can specify whether to Automatically agree with all license agreements and Automatically install all interactive patches.
View Info tab	<ul style="list-style-type: none"> ◆ Clicking this displays information such as a brief summary of the patch and the bug fixes in the patch.
Register tab	<ul style="list-style-type: none"> ◆ Clicking this displays the appliance's registration status, and an option to Deregister the appliance. ◆ If you deregister the appliance, the Register Online Update Service dialog reappears.
Refresh tab	<ul style="list-style-type: none"> ◆ Clicking this refreshes the status of updates on the Appliance.

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 17-3 Using the Support dialog

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

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 17-4 Using the Product Upgrade dialog

Field, Option, or Button	Information and/or Action

18 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 18-1 Using the Users dialog

Field, Option, or Button		Information and/or Action
Users dialog (header row)		
♦ New button	♦	Click this to begin creating a new non-LDAP internal user .
♦ Import Profiles... button	♦	<ul style="list-style-type: none">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.Click Choose File, then navigate to and select the file that contains user or group profile information in XML format.Click View a Sample File and make sure that the format of your file matches the format that is shown in the provided sample file.
♦ Delete 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 Deleting TeamWorks Users in the TeamWorks 18.1: Maintenance Best Practices Guide .
♦ More drop-down		<p>With one or more users selected, you can choose from the following options.</p> <ul style="list-style-type: none">♦ Disable User Account: Disabling TeamWorks User Accounts in the TeamWorks 18.1: Maintenance Best Practices Guide♦ Enable User Account: This restores access through a user account that was previously disabled.♦ Add Administrator Rights: Lets you assign selected users as Designated Administrators.♦ Remove Administrator Rights: Lets you remove Direct-administration rights from selected users.

Field, Option, or Button Information and/or Action	
♦ Filter List 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	♦ This lets you filter the displayed list of users using the following criteria: <ul style="list-style-type: none"> ♦ Internal Users ♦ External Users ♦ Disabled Users ♦ Enabled Users ♦ Administrators ♦ Non-administrators <p>By default, all of the above are selected for display.</p>
♦ Gear icon	♦ Click this to adjust column sizes.
Users List (below header row)	
♦ Full Name column	♦ Displays the user's first and last names combined
♦ Arrow drop-down column	♦ Provides access to the following settings for the user: <ul style="list-style-type: none"> ♦ User Properties dialog: Opens the User Properties dialog. ♦ Web Access 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.
♦ Type column	♦ Icons indicate whether users are LDAP, non-LDAP internal, External self-provisioned, System-created, and so on.
♦ Admin column	♦ This indicates whether users are assigned administrative responsibilities.
♦ Email column	♦ This displays the email address to which TeamWorks sends notifications
♦ User Id column	♦ The login name of each user
New User dialog	
♦ User ID	♦ You must assign a unique user ID for each non-LDAP internal user. See Worksheet 4—Duplicate User and Group Accounts in TeamWorks 18.1 Planning Your TeamWorks Deployment—Best Practices .
♦ Password	♦ You must assign (type and confirm) a password for the user to log in with.
♦ First Name	♦ You can include the user's first name
♦ Last Name	♦ You can also include the user's last name.
♦ Picture	♦ You can include a picture of the user, or the user can add it later.
♦ Time Zone	♦ Make sure the time zone setting is accurate.
♦ Locale	♦ Make sure the locale setting matches the user's language preference.
Personal Information	Users normally provide the following information for themselves.
♦ Job Title	
♦ About Me	

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

Viewing and Managing User Properties

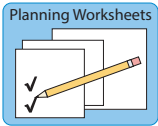
Path: [Port 8443 TeamWorks Administration Console](#) > **Management** > **Users** > drop-down arrow next to the user > **User Properties**

Table 18-2 Using the User Properties dialog

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

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 18-3 Using the Groups dialog

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

Field, Option, or Button Information and/or Action	
OK or Cancel	<ul style="list-style-type: none"> Click OK to save the changes you've made in this dialog or Cancel to discard your changes. Make sure you have edited the group membership. Otherwise your group will have no members.
Static Membership for Group dialog	
Allow external users and groups option	<ul style="list-style-type: none"> Select this to allow external users and groups to be added to the list.
Users tab	<ul style="list-style-type: none"> User field: Begin typing a user name, then select a listed user to add it to the Membership list.
Groups tab	<ul style="list-style-type: none"> Group field: Begin typing a group name, then select a listed group to add it to the Membership list.
<ul style="list-style-type: none"> Remove button 	<ul style="list-style-type: none"> Click this to remove a selected user or group (depending on which dialog you are in).
Membership list	<ul style="list-style-type: none"> A list of the users/groups in the static group.
OK or Cancel	<ul style="list-style-type: none"> Click OK to save the changes you've made in this dialog or Cancel to discard your changes.
Edit Dynamic Membership dialog	
Tips and Caveats	<ul style="list-style-type: none"> 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 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 "Guid attribute:" on page 20. 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 "LDAP Servers and Synchronization" on page 15. The Base DN set below must exist in each LDAP source. Otherwise, the membership of the dynamic group might not be updated correctly. 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.
<ul style="list-style-type: none"> Current Membership: button 	<ul style="list-style-type: none"> Click this to open the Dynamic Group Membership windows and view the users that are included in the group based on the current configuration.
<ul style="list-style-type: none"> Base DN: 	<ul style="list-style-type: none"> Use the LDAP browse button to locate the context where you want the search for users to begin.

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